TRUST IN GERMAN SICHERHEIT

G DATA Business-Lösungen

Reference Guide

G DATA Software AG | Oktober 2017

Inhalt

Einleitung

G DATA bietet hochwertigen Malware-Schutz für KMU- und Konzernnetzwerke. Die zentral konfigurierten und verwalteten Lösungen werden in hohem Maß automatisch ausgeführt, lassen sich aber auch umfassend auf den Einzelfall anpassen. Alle Clients, egal ob Workstations, Notebooks, Dateiserver oder Mobilgeräte, werden zentral verwaltet. Die Client-Prozesse werden unsichtbar im Hintergrund ausgeführt und automatische Online-Updates ermöglichen extrem schnelle Reaktionszeiten. G DATA unterstützt verschiedene Verwaltungsoptionen. So können Sicherheitsfunktionen autonom ausgeführt werden, es ist aber auch möglich, volle Kontrolle über die Software-Aktionen zu behalten. Das vorliegende Dokument unterstützt die fundierte Entscheidungsfindung zur Installation von G DATA Unternehmenslösungen und enthält Empfehlungen sowie optimale Konfigurationen für den Schutz von KMU- und Konzernnetzwerken.

Die Installation der Netzwerk- und Client-Sicherheit kann in drei Teile gegliedert werden. Im Idealfall wird der Sicherheitsaspekt von Anfang an berücksichtigt, noch bevor Hard- und Software in Betrieb genommen werden. Doch selbst bereits vorhandene Netzwerke können und sollten von einer gut durchdachten Sicherheitsrichtlinie profitieren. In der Planungsphase müssen die Bedürfnisse und Wünsche der Endbenutzer, die physischen Möglichkeiten der Hardware, das optimale Layout des Unternehmensnetzwerks und die Sicherheitsebenen berücksichtigt werden, über die alle Netzwerkelemente verfügen müssen. Mit Blick auf das allgemeine Netzwerk-Layout kann dann eine fundierte Entscheidung über die zu installierende G DATA Sicherheitslösung getroffen werden.

Nach Festlegung der Grundlagen kann mit der eigentlichen Installation der ausgewählten G DATA Unternehmenslösung begonnen werden. Ob es sich nun um ein KMU-Netzwerk mit weniger als 50 Clients oder eine Konzernumgebung mit über 1.000 Clients handelt: die Installation der G DATA Software kann rationell an jede Situation angepasst werden. G DATA Lösungen verfügen über mehrere Client-Installationsszenarien, die von automatischer Ferninstallation mit Active Directory bis hin zur lokalen Client-Installation reichen. Dadurch wird der gesamte Vorgang beschleunigt.

Auf die Installation von Servern und Clients folgt die abschließende Phase. Mithilfe der neu eingerichteten Client-Server-Infrastruktur können Client-Schutz, Server-Sicherheit, Backups, Patch-Management, Sicherheitsrichtlinien und vieles mehr konfiguriert werden. Mithilfe des vorliegenden Dokuments kann die G DATA Software so konfiguriert werden, dass sie optimale Sicherheit ohne Leistungseinbußen bietet.

Abschnitt A: Planung und Installation

1. Netzwerk- und Client-Verwaltung

Ein sicheres Unternehmensnetzwerk einzurichten und zu verwalten, ist mit einer Reihe von Anforderungen verbunden. Hardware und Software von Netzwerk und Client müssen so konfiguriert werden, dass sie verschiedene Endbenutzer-Workflows unterstützen, dabei aber unbefugte Benutzer, Angreifer und andere Bedrohungen fernhalten. Anstatt G DATA Software sofort auf allen vorhandenen Servern und Clients im Netzwerk zu installieren, sollten zunächst Netzwerk-Layout und Client-Verwaltung überlegt werden. Die Unterteilung des Netzwerks in verschiedene Zonen und die Definition von Client-Rollen vereinfacht die nachfolgende Konfiguration erheblich. Ein unterteiltes Netzwerk und standardisierte Client-Profile sparen Zeit beim Installieren neuer Sicherheitsupdates, beim Vorbereiten von Scans und beim Planen von Backups. Außerdem können kritische Teile des Netzwerks definiert werden, um sich bei Bedarf auf den wichtigsten Teil der Infrastruktur zu konzentrieren.

1.1. Netzwerk-Layout

Beim Netzwerk-Layout geht es um die physische Anordnung der gesamten Netzwerk-Hardware wie Modems, Router, Switches, Server, Clients und andere vernetzte Geräte. Anstatt Netzwerkgeräte in der Reihenfolge hinzuzufügen, wie sie angeschafft und installiert wurden, behält man mit einem standardisierten Netzwerk-Layout einen Überblick über das Netzwerk als Ganzes. Durch die Arbeit mit Netzwerkzonen und Client-Rollen kann auf jedem neu hinzukommenden Gerät eine standardisierte Konfiguration installiert werden. Dies spart Zeit und sorgt für die Regeleinhaltung im gesamten Netzwerk. Dieses Konzept kann auf kleinere ebenso wie größere Netzwerke angewandt werden. Eine Standardkonfiguration erleichtert die Behebung von Client- und Serverproblemen bzw. Netzwerkunregelmäßigkeiten in einem kommerziellen Umfeld, sobald mehr als ein Client verwendet wird.

Zum Aufbau eines Netzwerks ist ein Netzwerkdiagramm hilfreich. Es sollte alle Netzwerkgeräte einschließlich Router, Switches und andere unterstützende Geräte enthalten und eine Übersicht über die verschiedenen physischen Sicherheitsebenen einschließlich Modems, Routern und Firewalls bieten. Diese Geräte müssen vor der Installation einer Software-Sicherheitslösung konfiguriert werden, da sie quasi als vorderste „Verteidigungslinie“ des Netzwerks fungieren. Wird beispielsweise ein Modem oder Router mit integrierter Firewall verwendet, ist es wichtig, die Firewall zu aktivieren und entsprechende Regeln zur Abwehr von schädlichem Datenverkehr festzulegen. Sind weitere Sicherheitsfunktionen integriert, so sollten sie beurteilt und gegebenenfalls aktiviert werden. Dabei ist zu beachten, dass alle diese Einstellungen nur den Ausgangspunkt der Netzwerksicherheit darstellen: Einfach eine Firewall zu aktivieren, bedeutet noch keinen Schutz für die Netzwerk-Clients. Sobald eine Sicherheitslösung auf den Client-Geräten installiert wurde, müssen frühere Einstellungen für die Hardware eventuell getestet werden, damit sie miteinander kompatibel sind.

Neben der Visualisierung der verschiedenen Hardware-Sicherheitsebenen können mit einem Netzwerkdiagramm auch Clients effektiv gruppiert werden. Hier kommen die Konzepte der Netzwerkzonen und Client-Rollen ins Spiel. In ihrer einfachsten Form ist eine Netzwerkzone ein konkretes Segment des Netzwerks, dem ein bestimmter Zweck zugewiesen wurde. Durch Netzwerkzonen

können Sicherheitsmaßnahmen nach IP-Bereich konfiguriert werden. Wird in einer bestimmten Zone ein neues Gerät installiert, so weiß der Administrator sofort, welche Richtlinien erforderlich sind. Nach Netzwerkzone zu gruppieren bedeutet, die Geräte nach Parametern wie physischer Standort, Zweck, Sicherheitsbeschränkungen und anderen Eigenschaften einzuordnen. Beispielsweise können die Geräte nach physischem Standort im Gebäude („Vertriebsabteilung“, „Front Office“) einer Netzwerkzone zugeordnet werden. Werden Geräte nach Sicherheitsbeschränkungen unterteilt, könnte eine Netzwerkzone aus Online-Servern (DMZ), lokalen Clients mit eingeschränktem Zugang oder anderen Geräten bestehen, für die gemeinsame Richtlinien konfiguriert werden. Die Konfiguration einer DMZ wird insbesondere Unternehmen mit eigenen Online-Servern (beispielsweise Website-Hosting, Mail- oder FTP-Server) empfohlen. Diese Computer als eigene Netzwerkzone mit strengen Firewall-Regeln, die sie vom internen Netzwerk abgrenzen, zu konfigurieren, macht es potenziellen Angreifern erheblich schwerer, sich bis auf Geräte im internen Netzwerk vorzuarbeiten. Jede Netzwerkzone kann als eigene Vertrauenszone mit eigenen Sicherheitsbeschränkungen angesehen werden. Der Datenfluss zu und von jeder Netzwerkzone kann auf Netzwerkebene eingeschränkt werden, damit kein unbefugter Zugriff auf wichtige Infrastruktur möglich ist. Selbst bei bereits bestehenden Netzwerken ist es hilfreich, wenigstens ein paar verschiedene Vertrauenszonen zu definieren, um die für das Unternehmen wichtigsten Computer zu ermitteln und entsprechend zu schützen.

Jedem Netzwerk-Client kann eine bestimmte Client-Rolle zugewiesen werden, die seiner Nutzung, Priorität, Sicherheitsgefährdung und anderen Parametern entspricht. Bei bestehenden Netzwerken, deren Clients im Active Directory (AD) organisiert sind, entspricht eine Client-Rolle im Groben einer AD-Organisationseinheit (OE). Einem Client, der hauptsächlich für grundlegende Bürotätigkeiten genutzt wird, könnte die Rolle „Büro“ zugewiesen werden. Bei prioritätsbasierten Rollen könnte einem generisch installierten Client für Bürotätigkeiten eine niedrigere Priorität als die des aufwendig konfigurierten Clients eines Entwicklers zugewiesen werden. Die Client-Rolle legt sowohl die lokalen Sicherheitsrichtlinien als auch die Softwareinstallation fest. Rolle und Netzwerkzone des Clients können sich auch überschneiden, beispielsweise wenn Netzwerkzonen nach physischer Nähe konfiguriert werden. Idealerweise ist die Überschneidung so groß wie möglich, damit pro Zone nur eine Richtlinie konfiguriert werden muss, die alle Clients abdeckt. So würde die nach physischer Nähe unterteilte Netzwerkzone „Vertriebsabteilung“ nur Geräte mit der Client-Rolle „Vertrieb“ enthalten und alle Clients dieser Netzwerkzone würden identische Softwarekonfigurationen und Sicherheitsrichtlinien erhalten. Es kann jedoch sein, dass nicht alle Clients innerhalb einer Netzwerkzone für den gleichen Zweck verwendet werden. Basiert eine Netzwerkzone auf Sicherheitsberechtigungen, besitzen die meisten Clients die gleichen Sicherheitseinstellungen, haben aber unterschiedliche Software installiert und verfügen somit über unterschiedliche Client-Rollen. Die folgenden Diagramme verdeutlichen das Konzept der Netzwerkzonen und Client-Rollen in einer Reihe gängiger Netzwerkumgebungen.

In einem kleinen Büronetzwerk müssen die meisten Sicherheitsmaßnahmen auf den Clients implementiert werden. Mit Ausnahme einer optionalen Hardware-Firewall gibt es keine weiteren Sicherheitsvorkehrungen auf Netzwerkebene. Auch wenn die einzelnen Netzwerkzonen nicht klar unterschieden werden, sollten die Client-Rollen dennoch durchgesetzt werden, selbst wenn es nur ein oder zwei Computer pro Rolle gibt. Maßgeschneiderte Sicherheit für jeden Client im Netzwerk wird durch zentral definierte Sicherheitsrichtlinien für die einzelnen Client-Rollen mithilfe von AD-Gruppenrichtlinienobjekten und vom G DATA ManagementServer bereitgestellt. Außerdem muss für eine angemessene Ausfallsicherheit des Servers gesorgt werden. Fällt der Server aufgrund von Hardware-

oder Verbindungsproblemen aus, müssen sich die Clients dennoch mit den Netzwerkressourcen verbinden können. Außerdem sollten die Server-Konfiguration und Datenbanken auf einem zweiten, separaten Gerät oder einem externen Speichermedium gesichert werden.

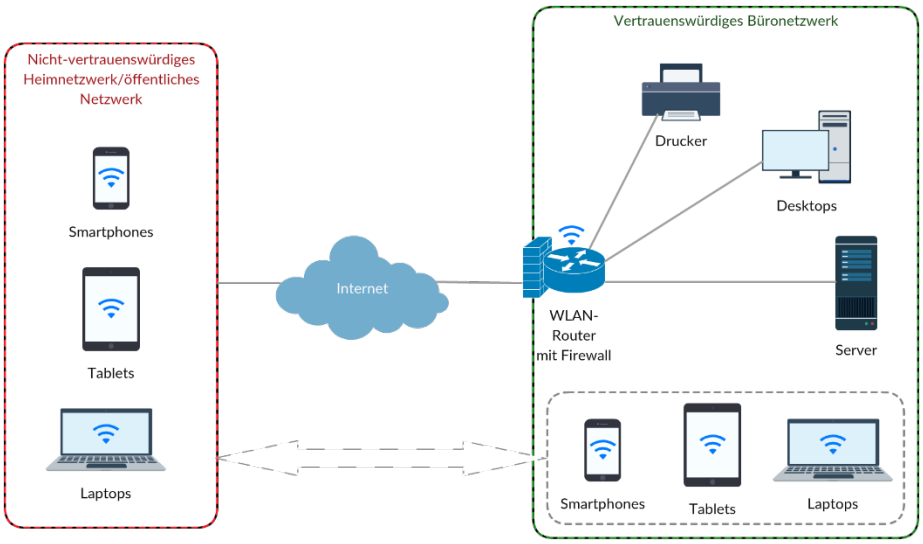

Abbildung 1: Kleines Büronetzwerk

Wenn sich das Netzwerk vergrößert, verhindert ein simples Layout effektive Installationen und Wartungsmaßnahmen. Mit einem formal definierten Netzwerk-Layout aus Zonen und Client-Rollen können Richtlinien für verschiedene Arten von Clients entwickelt werden. Dieser Netzwerktyp ist problemlos skalierbar und eignet sich für zehn Clients ebenso gut wie für mehrere Hundert. Ein typisches mittelgroßes bis großes Büronetzwerk beruht nicht auf einem einzelnen Gerät, das Modem, Router und Firewall in einem ist. Stattdessen werden mehrere Gateways installiert, die einen geschützten Internetzugang ermöglichen. Durch eine separate Firewall auf Netzwerkebene kann der Netzwerkverkehr leistungsstark gefiltert werden. Hinter der Firewall wird der Verkehr auf das interne Netzwerk verteilt. Die unterschiedlichen Netzwerkzonen werden physisch voneinander getrennt, indem sie jeweils einem Netzwerkgerät zugewiesen und in unterschiedliche Teilnetze aufgeteilt werden. Über Router und Switches wird kabelgebunden auf die einzelnen Netzwerkzonen zugegriffen. Sie verwalten und beschränken den Datenverkehr zwischen unterschiedlichen Vertrauenszonen. Wenn mobile Geräte installiert und für das Unternehmensnetzwerk eingerichtet wurden, können sie sich mit einem vertrauenswürdigen Netzwerk für drahtlose Geräte verbinden. Für unbekannte Geräte wird ein eigenes, nicht vertrauenswürdiges Gästenetzwerk konfiguriert.

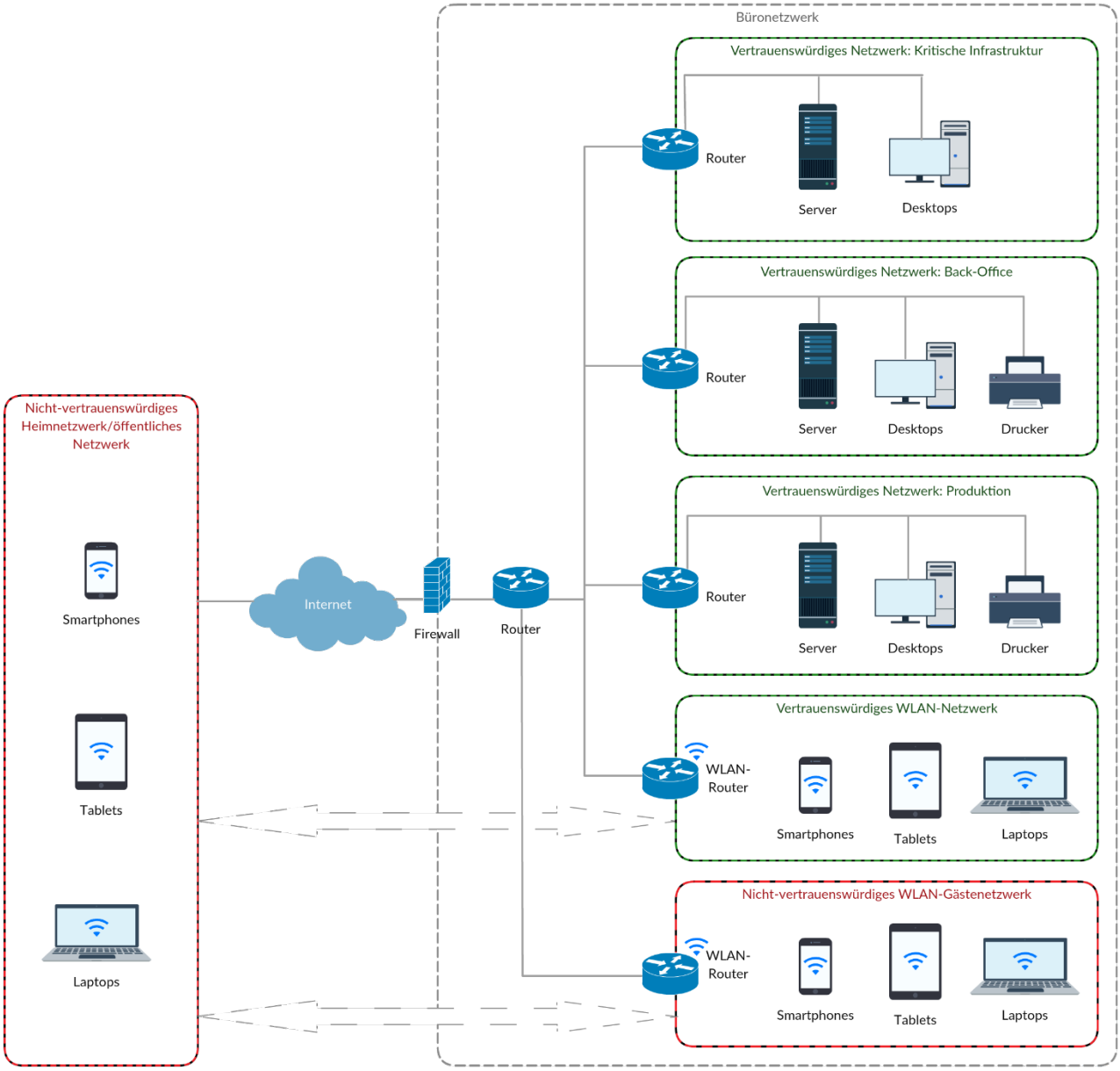

Abbildung 2: Mittelgroßes bis großes Büronetzwerk

Zwischen den verschiedenen Servern und den Clients, die sie versorgen, muss unterschieden werden. Diese Server können in einer eigenen Netzwerkzone gruppiert werden (müssen aber nicht) und stellen interne Client-Dienste wie Dateispeicherung, Druckdienste oder ERP bereit. Gleichzeitig dienen einer oder mehrere Server vielleicht als Mail-, Web- oder FTP-Server und versorgt Clients außerhalb des Netzwerks. Auch wenn es bei mittelgroßen und großen Netzwerken möglich ist, Offline- und Online-Server gemeinsam in einer internen Zone auszuführen, sollte eine zusätzliche Sicherheitsebene hinzugefügt werden, wenn das Netzwerk einen Online-Server enthält. Die demilitarisierte Zone (DMZ) ist ein logisches Teilnetz, das explizit nur die Dienste enthält, die Kommunikationsanfragen von außerhalb des Netzwerks erhalten. Unbefugter Zugriff auf das interne Netzwerk sollte dadurch verhindert werden, dass die Server in der DMZ und in internen Netzwerkzonen nur so viel Kontakt haben, wie zur ordnungsgemäßen Ausführung der Dienste (z. B. E-Mail) erforderlich ist. Sie müssen sicherstellen, dass quasi der gesamte externe Datenverkehr in der DMZ ankommt, es sei denn, die Anfrage stammt von

einem internen Client. Jeder Kontakt zwischen Diensten in der DMZ und internen Diensten sollte genau geprüft werden.

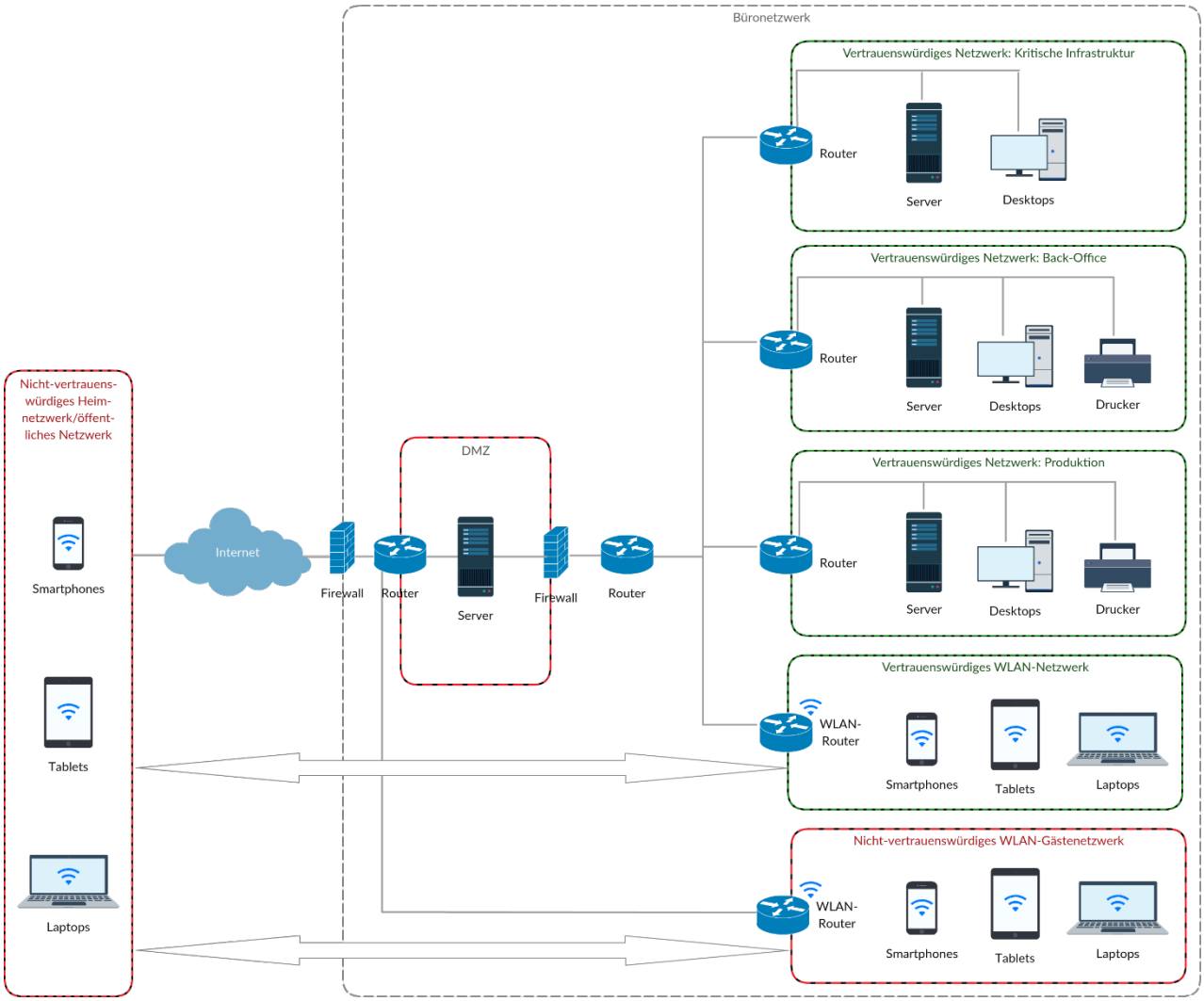

Abbildung 3: Mittelgroßes bis großes Büronetzwerk mit demilitarisierter Zone (DMZ)

Bei größeren Unternehmen mit mehreren Niederlassungen wird das Netzwerk-Layout etwas komplizierter. Lokale Dienste werden häufig für alle Standorte dupliziert, während Online-Server nicht unbedingt an allen Standorten installiert werden. Das Grundprinzip ist jedoch das gleiche wie für Unternehmen mit nur einer Niederlassung. Die Internetverbindung verläuft über verschiedene Hardware auf Netzwerkebene, die bösartigen Datenverkehr filtert und entweder an einen Server in der DMZ oder in einer internen Netzwerkzone weiterleitet.

Es gibt viele Geräte, die nicht in das herkömmliche Netzwerkparadigma passen. Mobile Geräte von Mitarbeitern könnten sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks verwendet werden. Unabhängig davon, ob es sich um unternehmenseigene Geräte handelt oder nicht: Bei der Verbindung mit dem Unternehmensnetzwerk müssen sie die geltenden Sicherheitsrichtlinien einhalten. Das Gleiche gilt für Geräte, die physisch zwar außerhalb des Netzwerks sind, aber auf Ressourcen innerhalb des Netzwerks zugreifen können (z. B. VPN-Clients). Die Sicherheit dieser Geräte hängt sowohl von den Hardware-Komponenten als auch davon ab, dass die Sicherheitsrichtlinien über Software durchgesetzt werden.

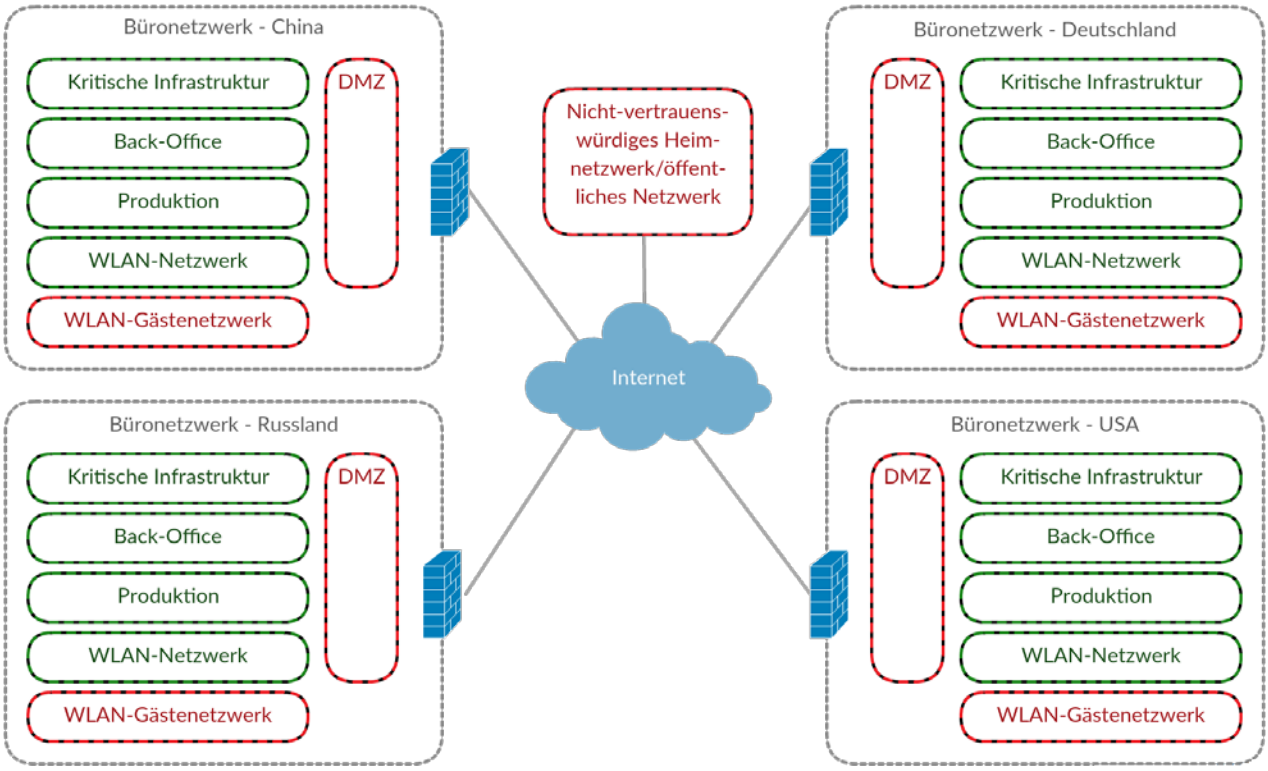

Abbildung 4: Mittelgroßes bis großes Büronetzwerk mit DMZ und mehreren Niederlassungen

Sobald das physische Netzwerk-Layout feststeht, ist es relativ einfach, logische Einheiten für die Netzwerk-Clients einzurichten. Idealerweise enthält jede Netzwerkzone eine einzelne Gruppe von Clients mit der gleichen Rolle. In manchen Netzwerkzonen gibt es Clients mit mehr als einer Rolle. Hier müssen also mehrere Gruppen erstellt werden. Diese Client-Struktur sollte sich in den Organisationseinheiten des Netzwerks widerspiegeln. Bei Netzwerken unter Windows ist dies normalerweise eine Active Directory-Struktur, in der jede Client-Rolle einer eigenen Organisationseinheit mit geltenden Richtlinien zugewiesen wird.

1.2. Sicherheitskomponenten

Einige Sicherheitsmaßnahmen werden auf Hardware-Ebene implementiert, wie es in den Netzwerkdiagrammen in Abschnitt 1.1 dargestellt ist. Ein Router mit integrierter Firewall oder ein eigenes Firewall-Gerät ist eine sehr gute Möglichkeit, um auf Hardware-Ebene einen Großteil des Datenverkehrs zu filtern, kann jedoch für sich genommen keine vollständige Betriebssicherheit bieten. Eine Netzwerksicherheitsrichtlinie muss aus verschiedenen Ebenen und Lösungen bestehen, die gemeinsam ein allumfassendes Sicherheitskonstrukt darstellen. Einige dieser Ebenen werden als Hardware umgesetzt, andere als Software. Manche Schutzeben bestehen in der Analyse des Netzwerkverkehrs, andere schränken gefährliche Aktivitäten auf den Clients ein. Da aber keine dieser Ebenen für sich allein ausreicht, müssen die Sicherheitskomponenten alle möglichen Zugangspunkte abdecken und effektiv zusammenarbeiten.

Das Netzwerkdiagramm ist ein guter Ausgangspunkt, um herauszufinden, welche Sicherheitskomponenten wo eingesetzt werden müssen. Neben der Installation von Hardware müssen auch einzelne Netzwerkgeräte geschützt werden. Für jedes Gerät bzw. jede Gerätekategorie im

Netzwerkdiagramm muss berücksichtigt werden, welche Art von Datenverkehr gesendet und empfangen wird, wozu er dient und wie wichtig er für das Unternehmen ist. Eine Möglichkeit ist es, Sicherheitssoftware lokal auf Clients und Servern zu installieren, um die Verbreitung von Malware zwischen den einzelnen Clients zu verhindern. Außerdem sollten sensible Server geschützt werden. Bei Mail-Servern sollten die ein- und ausgehenden E-Mails auf Malware gescannt werden (Spam-Filter bieten hier weitere Vorteile). In Kapitel 3 wird beschrieben, wie wichtige Netzwerkgeräte mithilfe von G DATA Software maximal geschützt werden.

2. Auswählen einer Lösung

Sobald das Netzwerk-Layout und die Client-Verwaltung festgelegt wurden, kann eine fundierte Entscheidung über die zu installierende G DATA Unternehmenslösung getroffen werden. Je nach Anforderungen des Unternehmens kann der Kunde die Lösung auswählen, die sich am besten für sein Netzwerk eignet. Seien es maximale Sicherheit, Flexibilität, Leistung oder alle genannten Eigenschaften: die Module der G DATA Unternehmenslösungen lassen sich so kombinieren, dass sie jedem Netzwerk gerecht werden. Um einen optimierten Schutz des Netzwerks zu gewährleisten, müssen die notwendigen Sicherheitsmodule ermittelt werden.

2.1. G DATA Unternehmenslösungen

Der Malware-Schutz bildet das Fundament des G DATA Unternehmensportfolios. Jede Lösung, beginnend mit dem Einstiegsmodell Antivirus Business, enthält das Virenschutzmodul mit signaturbasiertem Schutz und heuristischen Analysen, um Bedrohungen von Clients fernzuhalten. Durch den Einsatz zweier Engines liefert seine aktive Hybrid-Technologie optimale Erkennungsraten. Die G DATA CloseGap-Engine optimiert die Leistung und erkennt sogar lokal begrenzte Bedrohungen. Das BankGuard-Modul bietet zusätzlichen Schutz beim Online-Banking. Mit dem ReportManager erhält der Administrator einen Überblick über den Status des Netzwerks und der verbundenen Clients. Das Mobile Device Management zeigt Android- und iOS-Geräte im Verwaltungsbereich von G DATA an, um die Sicherheitslösung zu administrieren sowie Maßnahmen zu Daten- und Diebstahlschutz zu aktivieren.

Mit dem Modul Client Security Business kommt die G DATA Firewall hinzu, ein Host-basiertes Eindringschutzsystem (HIPS), das den Client-Netzwerkverkehr überwacht und unerwünschten Zugriff auf Client-Systeme verhindert. Das AntiSpam-Modul für Clients schützt vor unerwünschten und infizierten E-Mails, da es sie auf Netzwerkebene scannt und ein Plug-in für Microsoft Outlook bereitstellt. Endpoint Protection Business bietet Hilfestellung bei der zentralen Verwaltung von Sicherheitsrichtlinien, beispielsweise zur Gerätekontrolle und der im Internet verbrachten Zeit.

Einige Module sind separat erhältlich. Das Modul Exchange Mail Security bietet Spam- und Malware-Filterfunktionen für Mail-Server auf Protokollebene und kann als eigenständiger Gateway installiert werden. Das Plug-in für Microsoft Exchange fügt sich nahtlos in den Malware- und Spam-Schutz auf dem Microsoft Exchange Server ein. Die Mail-Sicherheit für Sendmail-/Postfix-Server steht über das optionale Modul Linux Mail Security Gateway zur Verfügung. Mit dem Backup-Modul können Dateisicherungen für alle Clients im Netzwerk geplant werden, um im Notfall einen Datenverlust zu verhindern. Das Patch Management spart Verwaltungskosten beim Testen und Installieren von Patches. Das Modul bezieht die neuesten Software-Patches von allen gängigen Anbietern und verteilt sie. Über Network Monitoring kann der Administrator den Status der gesamten Netzwerkinfrastruktur im Auge behalten. Das Modul Linux Web Security Gateway schließlich bietet Viren- und Spam-Schutzfunktionen für Squid-basierte Web-Proxys.

Welche Software installiert wird, hängt von den erforderlichen Modulen ab. Wichtig ist, dass die ausgewählte Lösung alle Netzwerkentitäten schützt: (Mail-)Server, Netzwerk-Clients und mobile Geräte. Die Module können beliebig miteinander kombiniert werden, um so die ideale Lösung für das Netzwerk zu finden. Einen vollständigen Überblick aller G DATA Unternehmenslösungen finden Sie auf unserer Website unter https://www.gdata.de/business.

2.2. Systemvoraussetzungen

Die Systemvoraussetzungen von G DATA sollten mit der momentan im Unternehmensnetzwerk genutzten Hardware abgeglichen werden, um eine reibungslose Installation zu gewährleisten. Alle zu schützenden Server und Clients müssen die Systemvoraussetzungen erfüllen. Hier muss unter Umständen die Hardware aktualisiert bzw. standardisiert werden. G DATA optimiert seine Software, damit sie auf einer Vielzahl von Betriebssystemen und Hardware für Server und Clients ausgeführt werden kann. Dadurch verläuft die Installation in den meisten Netzwerken ohne Zwischenfälle. Die Software erfordert keinen eigenen Server, er wird jedoch für größere Netzwerke empfohlen.

G DATA ManagementServer

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 und Windows Server 2003
- Arbeitsspeicher: 1 GB

G DATA Administrator/G DATA WebAdministrator/G DATA MailSecurity Administrator

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bit), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 und Windows Server 2003

G DATA MobileAdministrator

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 und Windows Server 2008 R2

G DATA Security Client

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista SP1, Windows XP SP3 (32-bit), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 und Windows Server 2003
- Arbeitsspeicher: 1 GB

G DATA Security Client für Linux

- Betriebssystem: 32- und 64-Bit-Editionen von Debian 7, 8, und 9, OpenSUSE Leap 42.1, (64 Bit) und Leap 42.2 (64 Bit), Suse Linux Enterprise Server 11 SP4[1] und 12 (64 Bit), Red Hat Enterprise Linux 5.11, 6.6 und 7.0 (64 Bit), Ubuntu 14.04.1 LTS und 16.04, CentOS 5.11, 6.6 und 7.0 (64 Bit), Fedora 24 und 25

G DATA Security Client für Mac

- Betriebssystem: Mac OS X 10.7 und höher

G DATA Mobile Device Management für Android

- Betriebssystem: Android 4.0 und höher

[1] Bei Verwendung des G DATA Security Clients für Linux 14.1 und höher auf einem Suse Linux Enterprise Server 11 SP4 muss zuerst das Suse Linux Enterprise 11 Security Module installiert werden.

G DATA Mobile Device Management für iOS

- Betriebssystem: iOS 7.0 und höher

G DATA Exchange Mail Security (64-Bit-Exchange-Plug-in)

- Mail-Server: Microsoft Exchange Server 2016, Microsoft Exchange Server 2013 und Microsoft Exchange Server 2010 und Exchange Server 2007 SP1

G DATA MailSecurity MailGateway

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bit), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 und Windows Server 2003
- Arbeitsspeicher: 1 GB

Der G DATA ManagementServer und der G DATA Administrator erfordern das Microsoft .NET Framework 4.0, das automatisch mit installiert wird. Auch der WebAdministrator und der MobileAdministrator benötigen das Microsoft .NET Framework. Da es sich um Webdienste handelt, sind zudem für die beide letzten Dienste die Microsoft-Internetinformationsdienste (IIS) erforderlich, die zuvor installiert werden müssen. Zur Anmeldung am WebAdministrator muss im lokalen Browser das Microsoft Silverlight-Plug-in installiert werden. Zur Speicherung verwendet der G DATA ManagementServer einen SQL-Server. Der Microsoft SQL Server 2014 Express wird installiert, es kann aber auch eine vorhandene Instanz vom Microsoft SQL Server (Express) verwendet werden[2]. Bei der Verwendung vom G DATA ManagementServer/G DATA MailSecurity MailGateway mit einer lokalen SQL-Datenbank oder anderen bandbreitenintensiven Anwendungen auf demselben Computer gelten folgende Systemvoraussetzungen:

- Arbeitsspeicher: 4 GB
- CPU: mehrere Kerne

2.3. Lizenzierung

Nachdem eine Lösung ausgewählt wurde, stehen Informationen über die Lizenzierung auf der G DATA Website[3] oder über einen offiziellen Vertriebspartner zur Verfügung. Im Allgemeinen sind Business-Lizenzen für Umgebungen von fünf oder mehr Clients erhältlich. Der Preis der einzelnen Lizenzen hängt von der gewählten Lösung, den möglichen Zusatzmodulen und der Anzahl der zu schützenden Clients ab.

[2] Microsoft SQL Server 2014 Express ist nicht mit Windows Vista bzw. Windows Server 2008/2003 kompatibel. Auf diesen Systemen wird Microsoft SQL Server 2008 Express manuell vor dem ManagementServer installiert oder eine vorhandene Datenbankinstanz verwendet.
[3] Siehe www.gdata.de.

3. Installationsszenarien

Nachdem die passende G DATA Lösung für das Netzwerk ausgewählt wurde, muss die Installation geplant werden. G DATA Lösungen beruhen auf dem Client-Server-Modell. Dabei verwaltet eine zentrale Serveranwendung alle Clients im Netzwerk und wird optional von einem Sekundärserver und einem oder mehreren Subnet-Servern unterstützt. Auf jedem Client-Computer gibt es eine Client-Software, welche die Sicherheitslösung, Backups, Patches und andere Prozesse verwaltet. Bei der Installation werden zunächst ein oder mehrere Server eingerichtet, mit denen dann die Client-Software auf den Netzwerkcomputern installiert wird. Ob ein oder mehrere Server benötigt werden, hängt vom Netzwerk-Layout ab. Kleine Netzwerke können durch einen lokalen ManagementServer verwaltet werden. In großen Netzwerken oder bei Niederlassungen bieten sich mehrere ManagementServer an, die per Fernzugriff durch einen zentralen MasterAdmin verwaltet werden.

G DATA Lösungen werden lokal installiert oder als verwalteter Dienst bereitgestellt. Eine lokale Installation bietet die Flexibilität, die Lösung jederzeit entsprechend den Anforderungen zu konfigurieren, erfordert aber einen gewissen Aufwand, um mit der Lösung vertraut zu werden und sie genau an die Netzwerkbedürfnisse anzupassen. Beim verwalteten Dienst übernimmt ein Managed-Service-Partner die oben genannten Aufgaben. Per Fernzugriff konfiguriert und administriert er die Lösung, sodass kein Eingreifen des lokalen Administrators erforderlich ist.

Die Konfiguration der G DATA Lösungen erfolgt mithilfe des G DATA Administrators, G DATA WebAdministrators bzw. G DATA MobileAdministrators, je nachdem, ob die Lösung lokal oder per Fernzugriff, über einen Browser oder über ein mobiles Gerät konfiguriert wird. Weitere Informationen über die Administrationstools samt Anwendungsfällen finden Sie in Kapitel 5.

3.1. Lokale Installation

Das Client-Server-Modell von G DATA ist mit jeder Netzwerkkonfiguration kompatibel. Zusammen mit einem oder mehreren Servern (G DATA ManagementServer und die Sekundär- oder Subnet-Server sowie G DATA MailSecurity) wird auf jedem Client eine Client-Software (G DATA Security Client und G DATA Internet Security für Android) installiert. Die verschiedenen Komponenten und Installationsoptionen für den zentralen ManagementServer werden gemäß den Netzwerk-Layout-Diagrammen in Abschnitt 1.1 erörtert.

3.1.1. Netzwerkkomponenten

G DATA Lösungen bestehen aus mehreren Netzwerkkomponenten. Je nach Layout und Anforderungen des Netzwerks können verschiedene Komponenten installiert werden. Der ManagementServer ist das zentrale Element des Client-Server-Schutzprinzips und spielt bei jeder Installation eine entscheidende Rolle. Es gibt verschiedene Installationsoptionen. Abschnitt 3.1.2 enthält Beispiele für Netzwerke in kleinen Büros und Szenarien für große Unternehmen.

Der G DATA Security Client wird auf den Netzwerkcomputern installiert. Der Security Client stellt Windows-, Mac- und Linux-Geräten mehrere Schutzschichten bereit. Android-Geräte können mit der G DATA Internet Security für Android geschützt werden. Für iOS-Geräte gibt es hierzu das iOS Mobile Device Management.

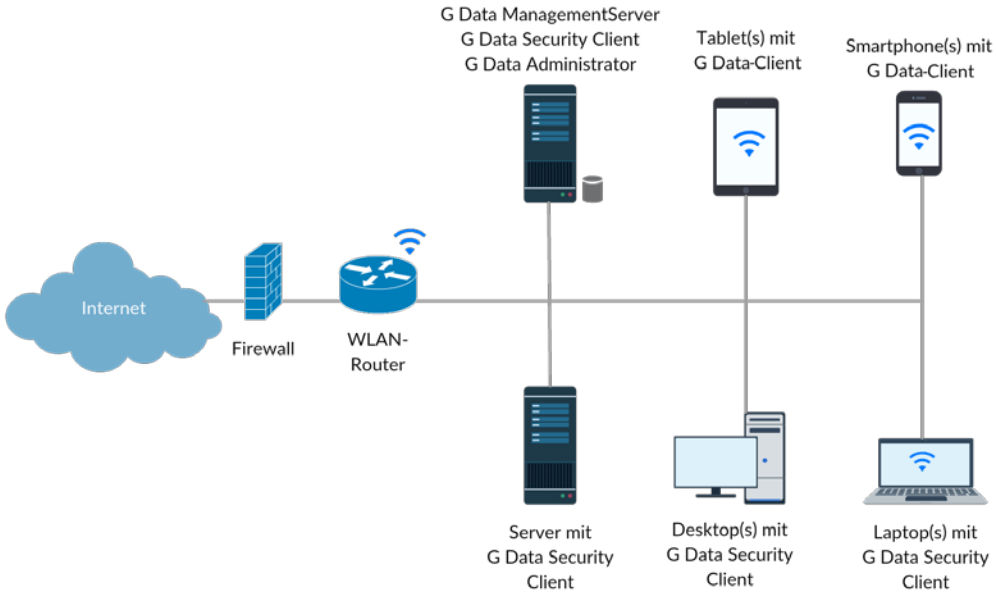

Abbildung 5: Installation in einem kleinen Büronetzwerk

Für Netzwerke mit eigenem Mail-Server ist die MailSecurity-Komponente für den Schutz des Mail-Servers als optionales Modul erhältlich, das E-Mails auf Malware und Spam scannt. Die MailSecurity kann als Plug-in für den Microsoft Exchange Server bzw. Sendmail/Postfix, aber auch als eigenständiges Produkt auf einem eigenen Server installiert werden, um den Datenverkehr bereits vor dem Mail-Server zu filtern.

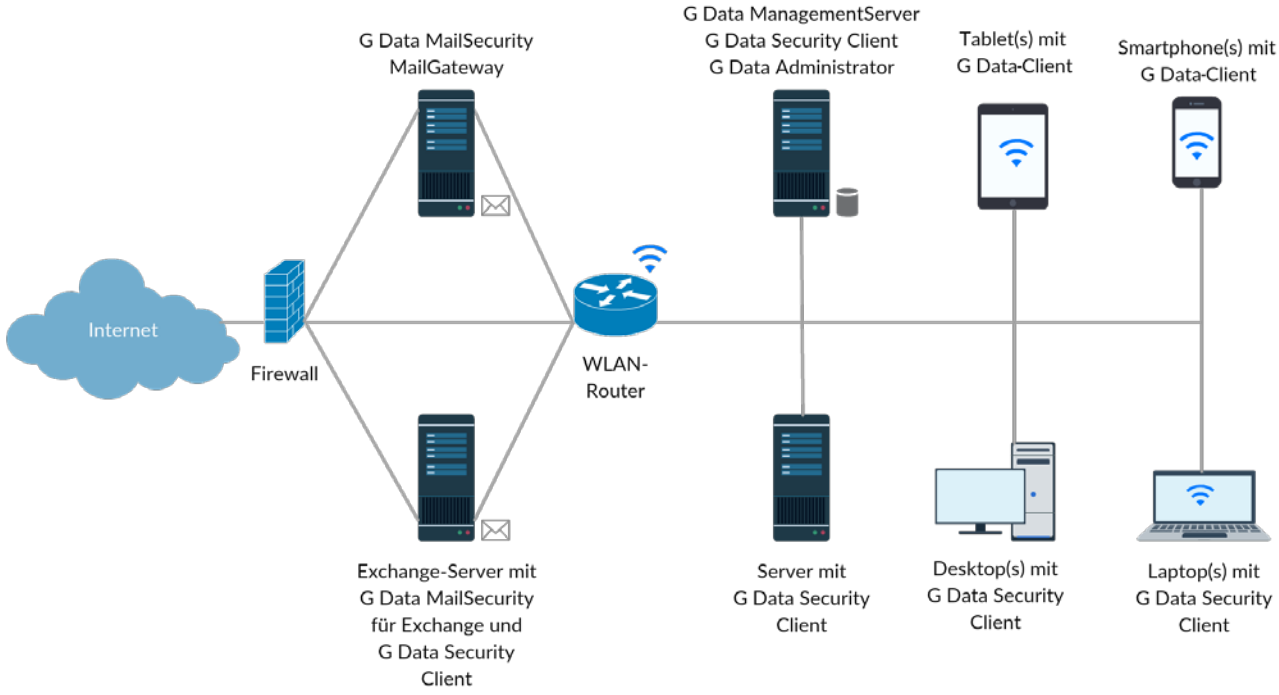

Abbildung 6: Installation in einem kleinen Büronetzwerk mit Mail-Server

3.1.2. ManagementServer-Installation

Wie der ManagementServer installiert wird, richtet sich ausschließlich nach der Art des Netzwerks. Aktuelle und zukünftige Merkmale des Netzwerks, wie Art der Infrastruktur, Anzahl der Clients und Art des Client-Zugriffs, müssen dabei berücksichtigt werden. Die unten aufgeführten Szenarien zeigen beispielhaft, wie eine G DATA Lösung in verschiedenen Netzwerken installiert werden kann. Aufgrund der Modularität der Lösungen kann die Installationsvariante ganz an die Erfordernisse des Netzwerks angepasst werden. Die Entscheidung für ein bestimmtes Szenario bedeutet jedoch nicht, dass später keine Änderungen an der Installation mehr möglich sind. Wenn das Netzwerk eine bestimmte Anzahl von Clients übersteigt, können die Komponenten im Netzwerk verschoben und zusätzliche (Subnet-)Server bereitgestellt werden.

Die wichtigste Komponente bei der Installation von G DATA Lösungen ist der G DATA ManagementServer. Aus Leistungsgründen wird zwar davon abgeraten, den ManagementServer auf einem Client in der Produktivumgebung zu installieren, die Möglichkeit besteht jedoch: Der ManagementServer benötigt kein Server-Betriebssystem, kann also problemlos unter Windows XP, Windows 10 oder einem anderen unterstützen Windows-Desktop-Betriebssystem installiert werden – eine wertvolle Alternative für kleine Büronetzwerke. Wird ein eigener Server verwendet, ist hierfür weder ein Server-Betriebssystem noch eine spezielle Hardware erforderlich. Der Computer sollte jedoch ausschließlich als Host für den ManagementServer genutzt werden. Werden auf diesem Server weitere Dienste installiert, insbesondere Datenbanken, E-Mail-Sicherheitslösungen, Domänen-Controller und Web-Server-Dienste, muss mit Bedacht vorgegangen werden: Je mehr Dienste auf einem Computer ausgeführt werden, desto mehr beeinträchtigen sich diese Dienste gegenseitig, was in Stoßzeiten zu Verzögerungen führt. Auch die Anzahl der installierten Clients wirkt sich unmittelbar auf die Serverleistung aus. In Netzwerken mit wenigen Clients ist diese Last relativ klein, sodass mehr Dienste auf demselben Server ausgeführt werden können. In größeren Netzwerken kann die Grenze der Serverleistung schon früher erreicht sein, sodass Dienste auf einen anderen Server verschoben oder auf mehrere Server verteilt werden müssen.

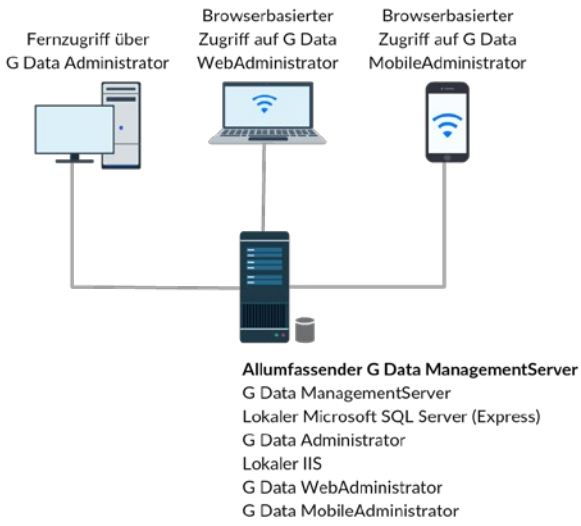

Abbildung 7: ManagementServer-Komplettinstallation

Die einfachste Variante beim Server ist die Komplettinstallation. Für Netzwerke mit relativ wenigen Clients oder ohne dedizierten Server können alle ManagementServer-Komponenten, also der

ManagementServer, eine lokale Installation des Microsoft SQL Servers oder der im Lieferumfang enthaltene Microsoft SQL Server 2014 Express und der G DATA Administrator, auf einem gemeinsamen Computer installiert werden. Ist Fernadministration erforderlich, können auch die Microsoft-Internetinformationsdienste (IIS) und der G DATA WebAdministrator oder der MobileAdministrator auf demselben Computer bereitgestellt werden.

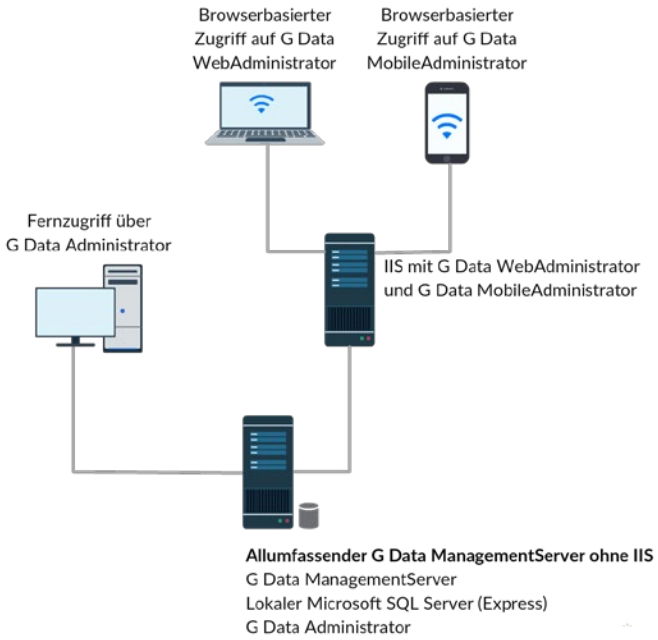

Abbildung 8: ManagementServer-Installation mit eigenem Webserver

Der ManagementServer, die dazugehörige Datenbank und die Administrationskomponenten auf einem gemeinsamen Computer zu installieren, ergibt einen leicht verwaltbaren Server, der bei wachsendem Netzwerk jedoch anfällig für Leistungsprobleme wird. Optional können die IIS und Administrationskomponenten auf einem eigenen Webserver untergebracht werden. Netzwerke mit IIS-Server benötigen keine weitere IIS-Installation auf dem ManagementServer. Der WebAdministrator und der MobileAdministrator können einfach auf einem vorhandenen IIS-Server (ab IIS 7 für Windows XP und WebAdministrator bzw. ab IIS 7.5 für Windows 7 und MobileAdministrator) bereitgestellt werden. Wie im Kapitel zu Netzwerk-Layouts beschrieben (siehe Abschnitt 1.1), kann der Webserver entweder Teil des allgemeinen Netzwerks oder der DMZ sein.

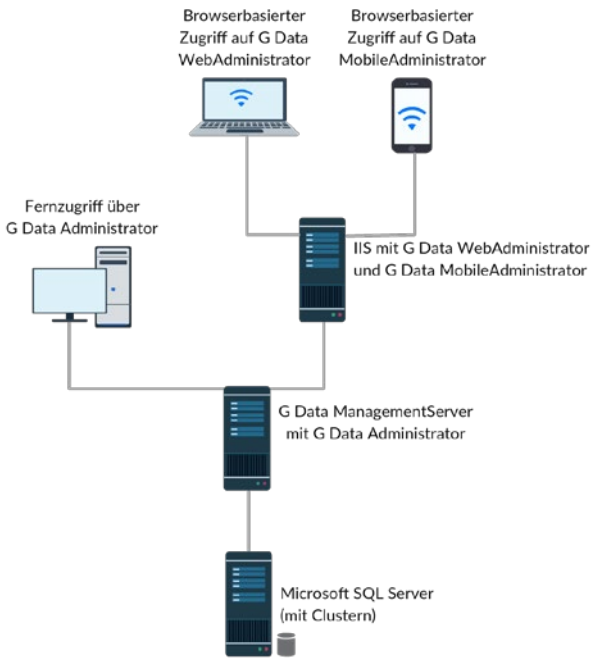

Abbildung 9: ManagementServer-Installation mit eigenem SQL-Server(verbund)

Trotz der integrierten Lastbegrenzungsfunktionen (siehe Abschnitt 7.5) vom ManagementServer bietet es sich bei großen Netzwerken an, etwas anders vorzugehen. Die Serverlast kann durch einen Microsoft SQL Server(verbund) reduziert werden. Wird die ManagementServer-Datenbank von einem eigenen SQL-Server gehostet, die Datenbanktransaktionen also ausgelagert, steigt die Leistung des ManagementServers. Zwar kann direkt von Anfang an ein eigener SQL-Server verwendet werden, doch ist der Migrationsfall in der Praxis deutlich häufiger: Nämlich dann, wenn es so viele Clients gibt, dass sie nicht mehr effizient durch eine Datenbank auf dem ManagementServer verwaltet werden können. Nach der Installation und Konfiguration vom Microsoft SQL Server auf einem eigenen Server wird die Datenbank mithilfe des Tools GdmmsConfig.exe-Tools migriert (siehe Abschnitt 4.7).

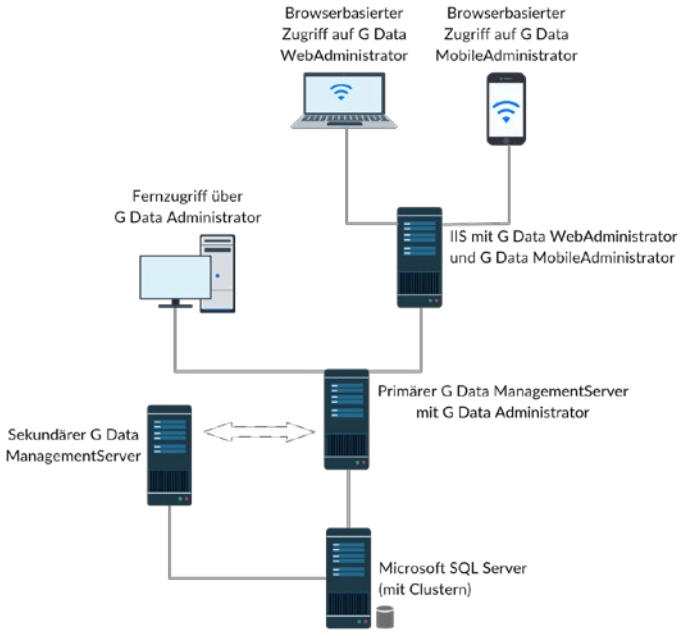

Abbildung 10: ManagementServer-Installation mit sekundärem ManagementServer

Ein mittelgroßes bis großes Büronetzwerk kann von einem sekundären ManagementServer zur Ausfallsicherung profitieren. Der sekundäre ManagementServer wird auf einem anderen Server installiert und läuft parallel zum primären ManagementServer. Ist der primäre ManagementServer länger als eine Stunde nicht verfügbar, verbinden sich die Clients mit dem Sekundärserver, um Updates zu beziehen. Der primäre und der sekundäre ManagementServer greifen auf dieselbe Datenbank zu. Deshalb eignet sich diese Variante nur für Umgebungen mit einer extern gehosteten Datenbank. Obwohl beide Server dieselbe Datenbank nutzen, beziehen sie ihre Updates vom G DATA Update-Server unabhängig voneinander. Dies bietet zusätzliche Redundanz, falls die Internetverbindung eines der Server getrennt wird. In Kombination mit einem eigenen SQL-Server(verbund) ist die Installation eines Sekundärservers sehr zuverlässig und umgeht Schwierigkeiten, wenn es zu Hardware-Problemen kommt.

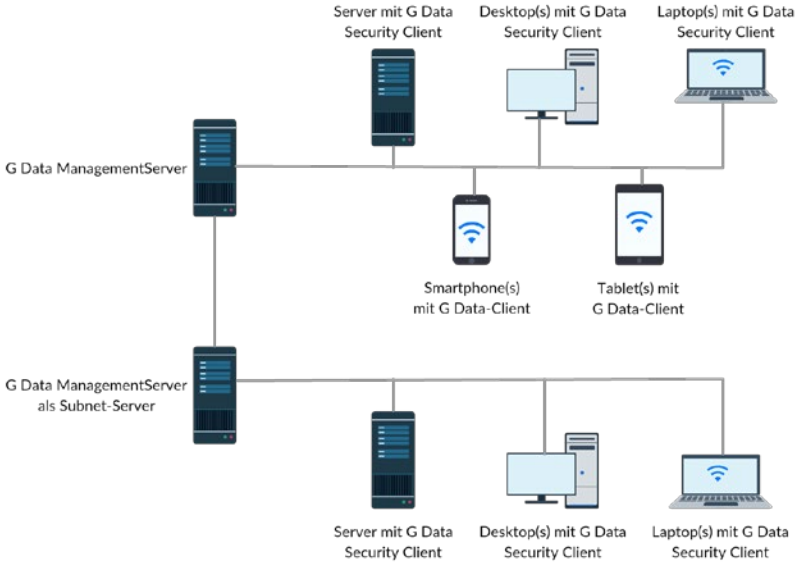

Abbildung 11: ManagementServer-Installation mit Subnet-Server

Der G DATA ManagementServer unterstützt die Installation eines oder mehrerer Server, die Client-Teilnetze verwalten, um den primären ManagementServer zu entlasten. Das ist besonders hilfreich für große Netzwerke bzw. solche mit mehreren Niederlassungen. Ein Subnet-Server ist ein ManagementServer für eine bestimmte Gruppe von Clients. Dadurch verringert sich die Netzwerklast, da der ManagementServer nur den Subnet-Server kontaktieren muss, der anschließend automatisch seine Clients versorgt. Mit Subnet-Servern können einem einzelnen ManagementServer mühelos tausende Clients zugeordnet werden. Die Subnet-Server werden je nach Sachverhalt normalerweise nach dem Haupt- bzw. Sekundärserver und seinen Clients installiert. Der primäre ManagementServer muss sich nicht im selben physischen Netzwerk wie der Subnet-Server befinden (beispielsweise können Niederlassungen von Subnet-Servern verwaltet werden, die sich mit einem zentralen ManagementServer verbinden).

Ein großes Unternehmen kann seine Clients auf mehrere ManagementServer verteilen. In diesem Fall kann die Verwaltung zentralisiert werden, indem alle ManagementServer zu einer MasterAdmin-Installation hinzufügt werden. Die ManagementServer sind unabhängig voneinander, werden jedoch zentral von einem MasterAdmin verwaltet. Hierfür muss die Portweiterleitung richtig eingestellt werden, damit die Server über das Internet erreichbar sind. Ansonsten unterscheidet sich diese Installation nicht

von anderen. Mit dem MasterAdmin kann der Administrator auf alle Module und Einstellungen zugreifen. Weitere Informationen zur Verwaltung von Servern mit dem MasterAdmin finden Sie in Abschnitt 5.4.

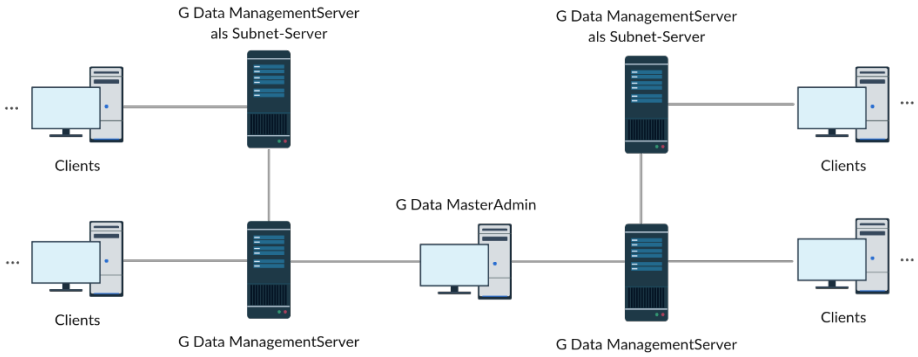

Abbildung 12: ManagementServer-Installation mit MasterAdmin

Sobald die G DATA Lösung im Einsatz ist, macht sich der Aufwand zur Organisation des Netzwerks bezahlt, und zwar ungeachtet seiner Größe. Die Sicherheitsmodule sind speziell auf das Konzept der Client-Gruppen abgestimmt. Sicherheitseinstellungen, Scan- und Backup-Aufgaben sowie jeder andere Sicherheitsaspekt können auf einzelne Clients oder ganze Client-Gruppen angewendet werden. Gruppen können manuell erstellt werden und beliebig viele Clients enthalten, die entweder durch Spiegelung einer Netzwerkzone bzw. Client-Rolle oder durch die Gruppierung gemäß anderen Attributen erzeugt werden. Bei Netzwerken mit Clients in Active Directory-Organisationseinheiten (OE) verringert sich der Aufwand weiter, da Client-Gruppen mit OE verknüpft werden können und automatisch ihre Client-Liste vererben.

3.2. Managed Endpoint Security und Managed Endpoint Security Powered by Microsoft Azure

Als Alternative zur lokalen Installation und Verwaltung können Sie auch die verwalteten Service-Lösungen von G DATA einsetzen. G DATA Partner, die diesen Service bieten, nehmen ihren Kunden auf diese Weise alle Arbeit ab. Der Partner kümmert sich sowohl um die Installation als auch die Verwaltung der gesamten Lösung und der Kunde profitiert von enormer Zeitersparnis. Es müssen keine Mitarbeiter geschult werden, um die Sicherheitslösung zu verwalten, und die Administratoren können sich auf andere Aufgaben konzentrieren. Mit der Managed Endpoint Security können Partner auch die Kunden erreichen, die keine lokal installierte G DATA Lösung verwenden würden. Bei der Entscheidung für Managed Endpoint Security Powered by Microsoft Azure profitieren Partner von weiteren Vorteilen wie Skalierbarkeit, Verfügbarkeit und Kostenplanbarkeit.

Die Verwaltung erfolgt per Fernzugriff ohne jegliches Eingreifen durch den lokalen Administrator. Das Produkt vereinfacht nicht nur die Installation, sondern stellt auch ein transparentes Lizenzmodell dar. Der Partner berechnet dem Unternehmen monatlich exakt die verwalteten Clients, sodass der Preis je nach Anzahl der Clients schwanken kann.

Für den Client funktioniert die Managed Endpoint Security wie eine lokale Installation, die im weiteren Verlauf dieses Handbuchs beschrieben ist. Für die Verwaltung fällt keinerlei Aufwand an. Alle Aufgaben werden per Fernzugriff vom Partner erledigt, der den Dienst bereitstellt. Die Partner verwalten die Managed Endpoint Security Netzwerke per Fernzugriff über den MasterAdmin (siehe Abschnitt 5.4).

4. Installation

Hier sind verschiedene Szenarien möglich, je nachdem, ob ein lokaler Administrator oder ein Managed Service-Partner die Installation durchführt bzw. ob es sich um ein Upgrade oder eine Erstinstallation handelt. In jedem Fall empfiehlt sich eine Testinstallation vorab, um das physische Netzwerk nicht zu beeinträchtigen. Die G DATA Lösung kann auf Servern und Clients eines virtuellen Netzwerks oder eines Teilnetzes des physischen Netzwerks installiert werden, um eventuell auftretende Probleme zu erkennen. Die Testinstallation muss auf einer Gruppe mit allen Client-Rollen (IT, Back-Office, F&E usw.) durchgeführt werden, damit die Ergebnisse der Testinstallation auf das ganze Netzwerk übertragbar sind. Der Testlauf und die eigentliche Installation einer G DATA Sicherheitslösung sollten, falls vorhanden, gemäß den Installationsrichtlinien des Unternehmens durchgeführt werden. In kleinen Unternehmen ist dies vermutlich relativ unkompliziert, während größere Unternehmen unter Umständen einen Projektplan entwickeln müssen, um Installationsplanung, Risikobewertung usw. zu dokumentieren.

Jede Installation besteht aus mehreren Phasen. Da G DATA Lösungen nach dem Server-Client-Prinzip funktionieren, wird zuerst der Server installiert und eingerichtet. Danach sollten die Server-Einstellungen (z. B. Update-Zeitplan und -Verteilung) und die Client-Standardeinstellungen konfiguriert werden, damit die Clients nach dem Rollout nach Bedarf geschützt sind. Nach der eigentlichen Installation müssen die Clients auf Funktionstüchtigkeit hinsichtlich der Sicherheitslösung geprüft werden. Da sich alle Clients regelmäßig mit dem primären ManagementServer verbinden, können die Einstellungen für jeden Client angepasst werden.

Das Zusatzmodul G DATA MailSecurity ist eine eigenständige Lösung. Es gibt also ein eigenes Installationsprogramm und die Konfiguration unterscheidet sich ein wenig von der Konfiguration anderer Sicherheitslösungen. Bei der Installation wird die MailSecurity gemäß der Position im Netzwerk konfiguriert (siehe Abschnitt 3.1.1). Anschließend können die Viren- und Spam-Schutzmaßnahmen umfassend angepasst werden.

4.1. Vorbereitung

Vor der Installation von Servern und Clients müssen die Systeme bestimmte Grundvoraussetzungen erfüllen. Auf den Servern, auf denen G DATA ManagementServer installiert werden soll, muss Windows Update ausgeführt und es müssen alle verfügbaren Sicherheitsupdates installiert werden. Frameworks wie Microsoft .NET Framework müssen ebenfalls aktualisiert werden. Und schließlich müssen Clients, die per Fernzugriff installiert werden sollen, mit den entsprechenden Zugriffsrechten ausgestattet werden (siehe Abschnitt 4.8).

Vor der Installation einer Sicherheitslösung muss sichergestellt werden, dass der Computer frei von Malware ist, um den Vorgang nicht zu beeinträchtigen und die Systemsicherheit zu erhalten. Aus diesem Grund ist jedes Installationsmedium einer G DATA Unternehmenslösung auch bootfähig und besitzt ein eigenes Linux-Betriebssystem[4]. Bei Ausführung des bootfähigen Datenträgers kann über die G DATA Startumgebung ein vollständiger Malware-Scan aller lokalen Festplatten durchgeführt werden, um eventuelle Malware-Überreste zu beseitigen. Bei kleineren Netzwerken sollte der bootfähige Datenträger

[4] Ist das Originalinstallationsmedium nicht verfügbar, kann der G DATA Bootmedium Wizard installiert und ausgeführt werden, um ein bootfähiges G DATA Bootmedium (CD, DVD oder USB-Stick) zu erstellen.

zuerst für alle Server und Clients verwendet werden. Bei größeren Netzwerken ist dies jedoch nicht immer durchführbar: Jeder Client muss manuell über den bootfähigen Datenträger gestartet werden und ein Komplett-Scan dauert einige Zeit. Der Server würde also lange Zeit ausfallen. Hier bietet es sich an, nur eine begrenzte Anzahl von Systemen zu scannen, wie z. B. Clients mit hoher Priorität oder hohem Risikopotential, und Servern, bei denen ein Malware-Verdacht besteht.

4.2. Erstinstallation

Ist dies die erste G DATA Lösung im Netzwerk, werden alle Komponenten erstmalig installiert. Das heißt, dass der Hauptserver, die potentiellen sekundären oder Subnet-Server, die lokale Datenbankinstanz und die Clients vollständig eingerichtet werden. Mit den Standardeinstellungen ist dies ein unkomplizierter Vorgang. Die Server-Komponenten werden zuerst installiert, gefolgt von den Verwaltungstools, Clients und der Mail-Server-Sicherheitslösung. Eine Erstinstallation erfordert minimalen Konfigurationsaufwand und ist in wenigen Stunden abgeschlossen. Wichtig ist jedoch die Kenntnis des Netzwerkaufbaus. Die Komponenten sollten auf den entsprechenden Geräten installiert und grundlegend konfiguriert werden. Die Kapitel 1, 2 und 3 enthalten Informationen zum Netzwerkaufbau.

4.2.1. Server

Während der Installation des ManagementServers müssen mehrere Optionen eingerichtet werden, wie der Servermodus (primärer oder sekundärer ManagementServer bzw. Subnet-Server) und die Datenbankkonfiguration. Diese Entscheidungen hängen vollständig vom Netzwerkaufbau und der ausgewählten Installation ab.

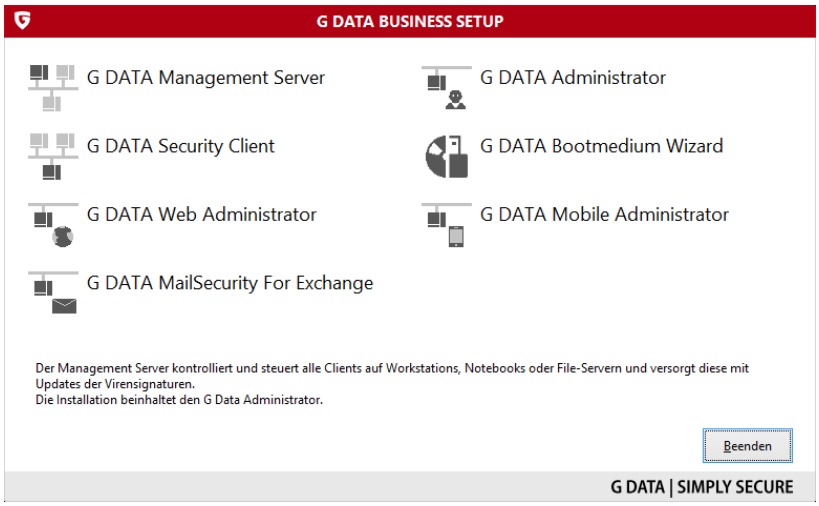

Abbildung 13: G DATA Installationsmedium – Produktauswahl

Der primäre ManagementServer muss als erste Komponente installiert werden. Er ist der zentrale Server, der alle Clients koordiniert, und wird möglicherweise von einem Sekundärserver bzw. einem oder mehreren Subnet-Servern unterstützt. Die ManagementServer-Komponente wird auf dem G DATA Installationsmedium über die Option G DATA MANAGEMENT SERVER im entsprechenden Fenster ausgewählt. Der Installationsassistent ist zwar unkompliziert, doch zwei Schritte erfordern besondere Aufmerksamkeit.

Der ManagementServer kann als Haupt-, Sekundär- oder Subnet-Server installiert werden. Die erste Installationsvariante bezieht sich auf den Hauptserver. Wenn das Netzwerk-Layout einen sekundären oder Subnet-Server erfordert (siehe Abschnitt 3.1.2 mit weiteren Informationen über typische Szenarien mit sekundären oder Subnet-Servern), müssen diese nach der Installation und Erstkonfiguration des Hauptservers auf den entsprechenden Computern bereitgestellt werden. In Abschnitt 4.10 wird der Installationsvorgang für einen Subnet-Server beschrieben.

Nach dem Servertyp muss der Datenbanktyp ausgewählt werden. In Netzwerken mit bis zu 1.000 Clients ist eine lokale Installation vom Microsoft SQL Server 2014 Express ausreichend. Bei Auswahl der Expressoption installiert und konfiguriert der Installationsassistent automatisch die lokale Datenbankserverinstanz und die erforderliche Datenbank. In Netzwerken mit mehr als 1.000 Clients oder Szenarien mit einem Sekundärserver sollte der ManagementServer auf einem eigenen Server ausgeführt werden und eine vorhandene Microsoft SQL Server-Instanz nutzen. Bei Verwendung einer vorhandenen Microsoft SQL-Server-Instanz muss der Datenbankserver über die Ports UDP 1434 und TCP 1433 (Standardwerte) erreichbar sein. Wird der ManagementServer erneut auf einem Computer installiert, auf dem sich bereits eine SQL Server Express- oder ManagementServer-Datenbank befindet, sollte die Option zur Verwendung einer vorhandenen Instanz ausgewählt werden. Die Verbindung mit der SQL Server (Express)-Instanz kann über den Einrichtungsassistenten konfiguriert werden, sobald Installation und Aktivierung abgeschlossen sind.

Die Installation von Microsoft SQL Server 2014 Express ist nur auf Systemen unter Windows 7/Windows Server 2008 R2 und höher möglich, da keine älteren Systeme unterstützt werden. Auf diesen Systemen wird Microsoft SQL Server 2008 R2 Express manuell vor dem ManagementServer installiert oder eine Datenbankinstanz auf einem anderen Computer verwendet. Microsoft SQL Server 2008 R2 Express steht auf der Microsoft-Website zum Download bereit[5]. Starten Sie die heruntergeladene Datei und wählen Sie INSTALLATION > NEUINSTALLATION ODER HINZUFÜGEN VON FUNKTIONEN ZU EINER VORHANDENEN INSTALLATION aus. Nun werden die Systemvoraussetzungen überprüft und die Dateien vorbereitet, die den Einrichtungsvorgang unterstützen. Danach wird der Installationsassistent gestartet. Die Standardeinstellungen der Installation können unverändert bleiben: Der Assistent installiert die Datenbank-Engine mit einer benannten Datenbankinstanz. Nach der Installation des SQL-Servers muss der ManagementServer installiert und die Option zur Nutzung einer vorhandenen Datenbankinstanz ausgewählt werden. Nach Abschluss des Setupvorgangs zeigt der ManagementServer-Installationsassistent die Konfigurationseinstellungen für die Datenbank an. Wählen Sie die Datenbankinstanz, die durch die Installation von Microsoft SQL Server 2008 R2 Express konfiguriert wurde, und geben Sie Ihr einen Namen.

Nach Abschluss der Installation fragt der Installationsassistent nach Informationen über die Lösungsaktivierung. Wenn die Lösung bisher noch nicht aktiviert wurde, wird nun der Lizenzschlüssel eingegeben, um die Software automatisch zu aktivieren und die Eingabe von Benutzernamen und Kennwort anzufordern. Benutzername und Kennwort werden anschließend in der Lösungskonfiguration gespeichert, damit Updates automatisch heruntergeladen werden können. Falls die Lösung bereits einmal aktiviert wurde und die Lizenz noch gültig ist, können Benutzername und Kennwort manuell eingegeben werden. Alternativ kann die Aktivierung verschoben werden. Eine Aktivierung zu einem späteren Zeitpunkt wird unterstützt (siehe Abschnitt 4.6), jedoch nicht empfohlen. Ohne Aktivierung

[5] Siehe https://www.microsoft.com/en-us/download/details.aspx?id=30438.

bietet die Lösung nur elementarste Funktionalität. Selbst wenn die Lösung als Endpoint Protection Business- oder Client Security Business-Edition gekauft wurde, sind bis zur Aktivierung der Software nur die Funktionen der Antivirus Business-Edition verfügbar. Des Weiteren können ohne eine Aktivierung keine Updates von Programmdateien oder Virensignaturen heruntergeladen werden. Dies beeinträchtigt die Effektivität der verschiedenen Schutzebenen erheblich.

Während der ManagementServer-Installation wird auch Microsoft .NET Framework 4.0 bereitgestellt, falls es noch nicht auf dem Server vorhanden war. Nach der Installation vom ManagementServer sollte mit Windows Update geprüft werden, ob sich Microsoft .NET Framework 4.0 auf dem neuesten Stand befindet. Nach der Installation wird unbedingt ein Neustart empfohlen.

Sobald der Hauptserver installiert wurde, hängt der nächste Schritt vom gewünschten Szenario ab. Zunächst sollte der Hauptserver konfiguriert werden (siehe Abschnitt 4.5). Erfordert das Netzwerk einen Sekundärserver, muss der ManagementServer-Installationsassistent hierzu auf dem entsprechenden Server ausgeführt werden. Sind Subnet-Server erforderlich, werden sie nach den Clients installiert (siehe Abschnitt 4.10). Alle Server müssen über entsprechende TCP-Kommunikationsports verfügen. Wird eine Netzwerk- oder Software-Firewall verwendet, müssen einige Ports offen bleiben. Weitere Informationen über TCP-Ports für G DATA Server und Clients finden Sie in Abschnitt 4.4.

4.2.2. Administration

Sobald der Haupt- und gegebenenfalls der Sekundärserver funktionsfähig sind, sollten die Administrationsanforderungen betrachtet werden. Jeder ManagementServer beinhaltet eine lokale Installation des G DATA Administrator-Tools, um den ManagementServer zu konfigurieren. Soll der Server per Fernzugriff konfiguriert werden (was dringend empfohlen wird), gibt es verschiedene Optionen: den G DATA Administrator auf einem anderen Client installieren, den G DATA WebAdministrator installieren, um den ManagementServer über einen Browser per Fernzugriff zu konfigurieren, oder den G DATA MobileAdministrator installieren, um den Server über ein Smartphone oder Tablet per Fernzugriff zu administrieren. Die Optionen für die Administration per Fernzugriff werden in Kapitel 5 beschrieben.

4.2.3. Clients

Nach der Installation vom ManagementServer und Administrator muss der G DATA Security Client auf alle Windows-, Linux- und Mac-Clients verteilt werden. Die Installation des G DATA Security Clients auf dem Server wird empfohlen, um auch den Server selbst vor Malware zu schützen. Wie auch bei anderen Netzwerk-Clients ist die Installation per Fernzugriff die einfachste Option. Android- und iOS-Clients können ebenfalls bereitgestellt werden, sobald der ManagementServer und der Administrator installiert wurden. Weitere Informationen über die Client-Installation finden Sie in Abschnitt 4.8.

4.2.4. Mail-Server-Sicherheit

Sollen auch G DATA MailSecurity MailGateway, Exchange Mail Security oder Linux Mail Security Gateway installiert werden, so erfolgt dies nach dem ManagementServer. Das MailGateway dient als zusätzliche Schutzebene vor dem eigentlichen Mail-Server und verarbeitet alle ein- und ausgehenden E-Mails. Dies kann auf zwei Arten erfolgen: durch die Installation von MailGateway auf dem Mail-Server oder indem es

auf einem anderen Server als Gateway eingerichtet wird. Exchange- und Linux-Server (Sendmail/Postfix) können mithilfe der entsprechenden Plug-ins geschützt werden.

4.2.4.1. G DATA Exchange Mail Security

Das Exchange-Plug-in der G DATA MailSecurity sollte auf allen Exchange-Servern installiert werden, auf denen Postfach- oder Hub-Transportrollen ausgeführt werden. Wird die Exchange Mail Security in einem Netzwerk mit mehreren Active Directory-Domänencontrollern installiert, benötigt der Einrichtungsassistent das Tool Repadmin.exe. Repadmin.exe ist im Rahmen der Active Directory Domain Services-Rolle, der Active Directory Lightweight Directory Services-Rolle und der Active Directory Domain Services Tools (Remote Server Administration Tools) verfügbar. Vor dem Start des Installationsassistenten von Exchange Mail Security müssen also eine oder mehrere dieser Komponenten bereitstehen.

Da das Exchange-Plug-in dem G DATA ManagementServer untergeordnet ist, muss dieser zuerst installiert werden. Nach der Installation des Exchange-Plug-ins registriert es sich beim ManagementServer. Lokal installierte Clients sind erst nach der Autorisierung über das Modul CLIENTS des G DATA Administrators voll funktionstüchtig, um unbefugten Zugriff auf den ManagementServer zu verhindern.

Durch die Anmeldung am ManagementServer können alle Einstellungen des Exchange-Plug-ins verwaltet werden. Es wird empfohlen, sofort einen On-Demand-Scan zu planen, der den gesamten Exchange-Speicher abdeckt (siehe Abschnitt 17.1.1.2), um jegliche Viren zu finden, die eventuell vor der Installation vorhanden waren.

4.2.4.2. G DATA Linux Mail Security Gateway

Antiviren- und Antispam-Funktionalität für Sendmail- und Postfix-Server werden über das Modul Linux Mail Security Gateway bereitgestellt. Es kann im Rahmen des G DATA Security Clients für Linux installiert werden (siehe Abschnitt 4.8.3) und benötigt das Amavis-Plug-in-Framework.

4.2.4.3. G DATA ManagementServer/G DATA MailSecurity MailGateway

Ist der vorhandene Mail-Server auf die CPU- und RAM-Last ausgelegt, kann das MailGateway auf demselben Computer installiert werden. Das hat den Vorteil, dass die IP-Adresse des Mail-Servers nicht geändert werden muss. Die Software des Mail-Servers muss jedoch anschließend neu konfiguriert werden, um andere Ports für ein- und ausgehende E-Mails zu verwenden. Alternativ kann das MailGateway auf einem eigenen Gateway-Server installiert werden, der die E-Mails vor dem Mail-Server filtert. Weitere Informationen über Installationsarten und Porteinstellungen für das MailGateway finden Sie in Abschnitt 17.3.1.

Ungeachtet der Art Server, auf dem das MailGateway installiert ist, sollte der G DATA Security Client zunächst auf diesem Server bereitgestellt werden. Dadurch wird nicht nur das lokale Dateisystem des Servers vor Malware geschützt, sondern das MailGateway bezieht auch automatisch die Virensignaturen von Security Client in den Malware-Scan ein.

Der Installationsassistent des MailGateways ist sehr benutzerfreundlich. Er kann optional einen lokalen Datenbankserver (Microsoft SQL Server 2008 SP3 Express) installieren, um E-Mails statistisch auszuwerten (siehe Abschnitt 17.3.1) und Greylists zu führen (siehe Abschnitt 17.3.4.4). Diese Funktionen sind jedoch nicht zwingend notwendig.

Die Einstellungen des MailGateways werden mit dem G DATA MailSecurity Administrator konfiguriert, der automatisch mit dem MailGateway installiert wird. Wie der G DATA Administrator, der den G DATA ManagementServer per Fernzugriff konfiguriert, muss der MailSecurity Administrator nicht auf demselben Server wie das MailGateway installiert werden. Der MailSecurity Administrator kann über das Installationsmedium auf jedem Netzwerk-Client installiert werden, der Zugriff auf den MailGateway-Server hat. Damit der MailSecurity Administrator den MailGateway-Server kontaktieren kann, muss der Zugriff auf den TCP-Port 7182 zugelassen werden.

4.3. Updates

4.3.1. G DATA ManagementServer

Sind der G DATA ManagementServer und seine Clients bereits installiert, ist ein Update normalerweise völlig unkompliziert. Es gibt zwei Möglichkeiten, um einen primären ManagementServer upzugraden. Am einfachsten wird die neue Version mit dem Internet Update-Tool heruntergeladen und installiert (siehe Abschnitt 4.6). Ist ein Sekundärserver vorhanden, wird er automatisch vom Hauptserver benachrichtigt, wenn dessen Upgrade installiert wurde, und führt das Upgrade dann selbst durch.

Bei Versions-Upgrades, wenn also kein direktes Upgrade möglich ist, muss zunächst der primäre ManagementServer deinstalliert werden, bevor die neue Version bereitgestellt werden kann. Die vorhandene Datenbank sollte nicht entfernt werden, da sie in der neuen Version verwendet und gegebenenfalls konvertiert werden kann. Wurden Konfigurationsdateien manuell geändert (z. B. mithilfe von Config.xml; siehe Abschnitt 18.2), müssen diese Änderungen nach der Neuinstallation erneut erfolgen. Während der Installation der neuen Version muss die Option zur Nutzung einer vorhandenen Datenbankinstanz ausgewählt werden. Nach der Installation kann die vorhandene Datenbank über die Schnittstelle des Einrichtungsassistenten ausgewählt werden. Das Gleiche gilt für den Sekundärserver. Beim nächsten Start zeigt der G DATA Administrator alle Clients und Einstellungen, wie zuvor konfiguriert. Zusätzlichen Schutz bietet ein Backup der alten Datenbank vor der Entfernung des ManagementServers (siehe Abschnitt 4.7). Treten bei der Installation der neuen Version Probleme auf, kann vor der Wiederherstellung der Originaldatenbank ein Downgrade oder eine Neuinstallation durchgeführt werden.

Meistens werden Subnet-Server automatisch nach dem Upgrade des primären ManagementServers upgegradet. Nur bei Subnet-Servern mit der ManagementServer-Version 12 muss Datenbankserver manuell installiert werden, bevor sie auf Version 14 aktualisiert werden können. Auf solchen Systemen muss Microsoft SQL Server 2014 Express (Windows Server 2008 R2/Windows 7 und höher) oder Microsoft SQL Server 2008 R2 Express (Windows Server 2003/2008/Windows Vista) manuell installiert werden (siehe Abschnitt 4.2.1). Nach der Installation des SQL-Servers kann mit der Option PROGRAMMAKTUALISIERUNG FREIGEBEN im Bereich ÜBERSICHT des SERVER-Moduls die Programmaktualisierung freigegeben werden. Nach

der Aktualisierung wird auf dem Subnet-Server mit GdmmsConfig.exe die Verbindung zur Datenbank konfiguriert (siehe Abschnitt 18.1).

4.3.2. G DATA Administrator/G DATA WebAdministrator/G DATA MobileAdministrator

Die Version des G DATA Administrators, die in der Installation des G DATA ManagementServers enthalten ist, wird automatisch mit dem ManagementServer selbst upgegradet. Wurde jedoch zuvor eine eigenständige Version des G DATA Administrators, der G DATA WebAdministrator oder der G DATA MobileAdministrator installiert, muss er manuell über den Installationsassistenten der neuen Version aktualisiert werden. Beim Versuch, sich mit einer veralteten Version des G DATA Administrators an einer neueren Version des ManagementServers anzumelden, muss der G DATA Administrator sofort aktualisiert werden.

4.3.3. G DATA Security Client

Nach dem Upgrade der Server erhalten auch alle Clients ein Software-Upgrade. Nach dem Server-Update wird die aktualisierte Software auf die Clients verteilt, und zwar gemäß dem normalen Ablauf: automatische Programmdatei-Updates oder manuelle Verteilung (siehe Abschnitt 7.3.2). Bei größeren Netzwerken wird für Updates die Peer-to-Peer-Verteilung empfohlen, damit der hohe Datenverkehr nicht die Serverleistung beeinträchtigt. Wie bei allen Software-Verteilungen muss auch hier auf Kompatibilität geachtet werden. Durch eine stufenweise Softwareverteilung kann der aktualisierte Client zunächst auf eine kleine Gruppe verteilt werden, bevor er im gesamten Netzwerk bereitgestellt wird. Alternativ kann eine manuelle Verteilung in einer kleinen, repräsentativen Testgruppe Hinweise auf mögliche Probleme geben.

4.3.4. G DATA MailSecurity MailGateway

Über den MailSecurity Administrator kann das MailSecurity MailGateway aktualisiert werden. Unter UPDATE wird die aktuell installierte Version des MailGateways und des Administrators angezeigt. Durch Klicken auf PROGRAMM-UPDATE wird das Update gestartet, das, ähnlich wie das Update vom ManagementServer, nahtlos über das Internet Update-Tool ausgeführt wird.

4.3.5. G DATA Exchange Mail Security

Wie auch der G DATA Security Client führt die Exchange Mail Security ein automatisches Upgrade durch, sobald auf dem ManagementServer eine neue Version verfügbar ist. Um sicherzustellen, dass die neueste Version des Exchange-Plug-in verwendet wird, verfügt das Internet Update-Tool des ManagementServer über die Funktion PROGRAMMDATEIEN (CLIENT) AKTUALISIEREN. Aktualisiert das Exchange-Plug-in seine Programmdateien laut Konfiguration selbsttätig, wird dies beim nächsten Verbindungsaufbau mit dem ManagementServer ausgeführt. Alternativ kann ein Upgrade manuell mit dem G DATA Administrator ausgeführt werden.

Aufgrund von Änderungen am Installationsvorgang können Versionen von Exchange Mail Security unter Version 12 nicht direkt upgegradet werden. In diesem Fall muss die Vorgängerversion der Exchange Mail

Security vor der Installation der neuen Version deinstalliert werden. Bei einem Upgrade auf die neueste Version sollte die Exchange Mail Security auf allen Exchange Servern installiert werden, auf denen Postfach- oder Hub-Transportrollen ausgeführt werden.

4.4. Netzwerkkonfiguration

Die Server und Clients der verschiedenen Komponenten von G DATA Lösungen kommunizieren über das TCP/IP-Protokoll miteinander. Hierfür müssen auf den Servern und Clients bestimmte Ports verfügbar sein, um die Kommunikation und Update-Verteilung zu ermöglichen. Software zur Netzwerküberwachung und Firewalls müssen so konfiguriert werden, dass sie Datenverkehr über diese Ports zulassen. Bei Portkonflikten können einige Portnummern neu konfiguriert werden (siehe Abschnitt 18.2).

Primärer/sekundärer ManagementServer

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)
- Port 7182 (TCP)
- Port 7183 (TCP)

Subnet-Server

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)

Clients

- Port 7169 (TCP)

MailSecurity MailGateway Server

- Port 7182 (TCP)

MailSecurity-Exchange-Plug-in

- Port 7171 (TCP)
- Ports 7185–7195 (TCP)

Wird Port 80 bzw. 443 bereits ausschließlich von einem anderen Prozess genutzt, wählt der G DATA ManagementServer beim Start einen zufälligen Port aus und speichert die Portnummer in der Config.xml (siehe Abschnitt 18.2).

Bei Verwendung des Moduls PatchManager (siehe Kapitel 15) muss neben den Ports auch die Firewall konfiguriert werden. Der Datenverkehr zwischen dem G DATA ManagementServer und dem folgenden URL muss immer zugelassen werden:

URLs
gdata.cdn.heatsoftware.com

Je nach Software, für die Patches bereitgestellt werden, muss der Datenverkehr zwischen G DATA ManagementServer und den folgenden URLs zugelassen werden:

Anbieter	URLs
7-Zip	http://downloads.sourceforge.net
Adobe	ardownload.adobe.com
	armdl.adobe.com
	download.adobe.com
	swupdl.adobe.com
	www.adobe.com
Microsoft	go.microsoft.com
	download.windowsupdate.com
	www.download.windowsupdate.com
	download.skype.com
	download.microsoft.com
Mozilla	http://ftp.mozilla.org
UltraVNC	http://support1.uvnc.com
VideoLAN	http://download.videolan.org

4.5. Anfangskonfiguration

Nach der Installation des G DATA ManagementServers und der anderen Komponenten werden Server und Clients erstmalig konfiguriert. Hierfür kann der G DATA Administrator verwendet werden, der automatisch auf demselben Computer wie der G DATA ManagementServer installiert wurde. Soll der Server per Fernzugriff konfiguriert werden, muss zunächst der G DATA WebAdministrator eingerichtet oder der G DATA Administrator auf einem Netzwerk-Client mit Zugriff auf den primären ManagementServer installiert werden (siehe Kapitel 5). Ungeachtet der jeweiligen Anwendung kann sich der Administrator mit einem lokalen oder einem Domänenadministratorkonto anmelden.

4.5.1. Server-Einrichtungsassistent

Einige Einstellungen müssen vor der Installation der Clients konfiguriert werden. Der SERVER-EINRICHTUNGSASSISTENT, der bei der ersten Anmeldung am G DATA Administrator gestartet wird, unterstützt die Konfiguration der elementaren Einstellungen und kann sowohl im G DATA Administrator als auch im G DATA WebAdministrator ausgeführt werden. Auch nach der Ersteinrichtung kann der Assistent weiterhin über das Menü SERVER > ÜBERSICHT gestartet werden. Zusätzlich sind die meisten Optionen separat über die verschiedenen Konfigurationsmodule vom G DATA Administrator verfügbar.

Der erste Schritt des SERVER-EINRICHTUNGSASSISTENTEN ist die Client-Installation. Bei der Ersteinrichtung kann dieser Schritt übersprungen werden (in Abschnitt 4.8 sind die verschiedenen Methoden der Client-Installation beschrieben). Wichtig ist die Konfiguration der automatischen Internet-Updates. Diese Einstellungen beziehen sich auf den Download von Virensignatur- und Programmdatei-Updates vom G DATA Update-Server auf den ManagementServer. Die anschließende Verteilung der Updates auf die Netzwerk-Clients kann später konfiguriert werden. Wurde die Lösung während der Einrichtung registriert, sind Benutzername und Kennwort bereits gespeichert. Anderenfalls kann die Lösung mit dem Internet Update-Tool registriert werden, um Benutzernamen und Kennwort zu erhalten (siehe Abschnitt 4.6). Der Update-Plan für Client-Virensignaturen und -Programmdateien muss so konfiguriert werden, dass er den Anforderungen des Netzwerks entspricht. Die beiden Zeitpläne können bei Bedarf angepasst werden. Für Server mit permanenter Internetverbindung werden stündliche Update-Anfragen empfohlen. Die genaue Update-Zeit kann durch eine Minutenangabe festgelegt werden. Die beiden

Update-Anfragen sollten nicht für die gleiche Uhrzeit geplant werden, um Leistungsprobleme zu vermeiden. Updates für Programmdateien können beispielsweise 15 Minuten nach der vollen Stunde, Updates für Signaturdateien 15 Minuten vor der vollen Stunde angefragt werden.

Im nächsten Schritt werden die E-Mail-Berichte konfiguriert. Dies ist im Rahmen des Server-Einrichtungsassistenten zwar nicht erforderlich, wird aber empfohlen. Weitere Informationen über die Konfiguration von E-Mail-Berichten finden Sie in Abschnitt 6.2. Auch wenn zu diesem Zeitpunkt keine E-Mail-Berichte konfiguriert werden, sollten jetzt die Mail-Server-Einstellungen eingegeben und Empfängergruppen definiert werden. Durch Klicken auf das Zahnradsymbol wird das Fenster E-MAIL-EINSTELLUNGEN geöffnet, um einen SMTP-Server zu definieren. Dazu müssen ein gültiger SMTP-Server und -Port (normalerweise 25) sowie eine Absender-E-Mail-Adresse eingegeben werden. Diese E-Mail-Adresse wird als Antwortadresse verwendet, um Elemente an die G DATA Security Labs zu übermitteln. Unter MAILGRUPPEN können die Empfängergruppen definiert werden, die später für E-Mail-Berichte und andere Funktionen verwendet werden. Gruppen wie „Administratoren“, „Verwaltung“ und „Technisches Personal“ sind sinnvoll, d. h. jede Entität, die in die Benachrichtigungsschleife für wichtige Server-Ereignisse oder Notfallbenachrichtigungen aufgenommen werden soll. Einstellungen für Mail-Server- und Empfängergruppen können später auf der Registerkarte E-MAIL des Moduls ALLGEMEINE EINSTELLUNGEN bearbeitet werden.

Der Server-Einrichtungsassistent beinhaltet auch Einstellungen für die Android-Geräteverwaltung. Dazu muss das Kennwort eingegeben werden, mit dem sich Android-Geräte am ManagementServer authentifizieren. Zum Einsatz von Notfallaktionen müssen die SENDER-ID und der API-KEY (Server-Key) des Firebase Cloud Messaging-Kontos eingegeben werden (weitere Informationen zur Konfiguration eines Kontos finden Sie in Abschnitt 11.1.6). Die Einstellungen können später über die Registerkarte ANDROID im Modul ALLGEMEINE EINSTELLUNGEN bearbeitet werden.

Im letzten Schritt des Server-Einrichtungsassistenten können Zugangsdaten zum ActionCenter konfiguriert werden, die zur iOS-Geräteverwaltung erforderlich sind (siehe Abschnitt 11.2) oder Network Monitoring (siehe Kapitel 16).

4.5.2. Zusatzkonfiguration

Der Server-Einrichtungsassistent wird mit der Client-Installation abgeschlossen (siehe Abschnitt 4.8). Vor der Installation der Client-Software im Netzwerk müssen jedoch noch einige zusätzliche Einstellungen konfiguriert werden. Im Modul ALLGEMEINE EINSTELLUNGEN bietet die Registerkarte SYNCHRONISATION wichtige Einstellmöglichkeiten zur Synchronisation und Aktualisierung von Clients. Unter CLIENTS wird die Option ZEITINTERVALL FÜR DIE SYNCHRONISATION MIT DEM SERVER UND DIE ANFRAGE NACH NEUEN UPDATES KONFIGURIERT WERDEN. Dies legt fest, wie oft sich Clients mit dem ManagementServer verbinden, um neue Updates oder Einstellungen anzufragen. Je mehr Clients installiert werden, desto höher ist die Netzwerklast bei geplanten, regelmäßigen Synchronisationen. Ein Durchschnittswert sind fünf Minuten. In einem kleinen Netzwerk mit wenigen Clients kann das Intervall kürzer sein; ergeben sich jedoch Lastspitzen, muss der Wert verringert werden. Auf der Registerkarte PROGRAMM-UPDATES kann die stufenweise Verteilung von Client-Software-Updates aktiviert werden. In Netzwerken mit mehr als zehn Clients werden Server- und Netzwerklastspitzen bei Updates für Client-Programmdateien durch die stufenweise Verteilung verringert. Zusätzlich können die Clients so gruppiert werden, dass kritische Systeme später aktualisiert werden und die ersten Phasen als Testplattform dienen. Auf der Registerkarte SIGNATURUPDATES im Modul

UPDATES kann die Peer-to-Peer-Verteilung aktiviert werden, um hohe Serverlasten bei Signaturupdates zu vermeiden. Dadurch können Clients gegenseitig als Update-Server fungieren, um aktualisierte Programmdateien und Signaturen zu verteilen. Die Peer-to-Peer-Verteilung der Updates wird vollständig vom primären ManagementServer verwaltet und erfolgt ohne Eingreifen von außen, wenn der entsprechende Client-Port konfiguriert wurde (siehe Abschnitt 4.4). Erweiterte Einstellungen können durch Bearbeitung der entsprechenden Konfigurationsdatei geändert werden (siehe Kapitel 18). Weitere Informationen zur stufenweisen Verteilung und Peer-to-Peer-Verteilung finden Sie in Abschnitt 7.3.2.

4.5.3. Standardmäßige Client-Sicherheitseinstellungen

Vor einer netzwerkweiten Client-Installation müssen die standardmäßigen Client-Sicherheitseinstellungen entsprechend der Anforderungen und Richtlinien konfiguriert sein. Mit den G DATA Administrator-Modulen CLIENT-EINSTELLUNGEN (siehe Kapitel 8) und ANDROID-EINSTELLUNGEN (siehe Kapitel 11) können die Sicherheitseinstellungen aller Clients durch Auswahl des primären ManagementServers gleichzeitig konfiguriert werden, oder es wird eine Gruppe nach der anderen ausgewählt, falls separate Einstellungen erforderlich sind.

4.6. Server-Updates und Registrierung

Der Server-Einrichtungsassistent konfiguriert den ManagementServer, um regelmäßig nach Updates für Client-Programmdateien und -Virensignaturen anzufragen. Da Server-Updates einen Neustart des ManagementServer-Hintergrunddienstes erfordern, müssen sie immer manuell ausgeführt werden. Ist ein Programm-Update für den ManagementServer verfügbar, zeigt der G DATA Administrator im Bereich ÜBERSICHT eine Benachrichtigung an. Alternativ können Updates manuell mit dem Internet Update-Tool angefragt werden. Mit der Option PROGRAMMDATEIEN (SERVER) AKTUALISIEREN werden Updates angefragt. Hierzu werden die G DATA Update-Server auf aktualisierte ManagementServer-Programmdateien durchsucht und der Installationsvorgang startet, falls Updates verfügbar sind.

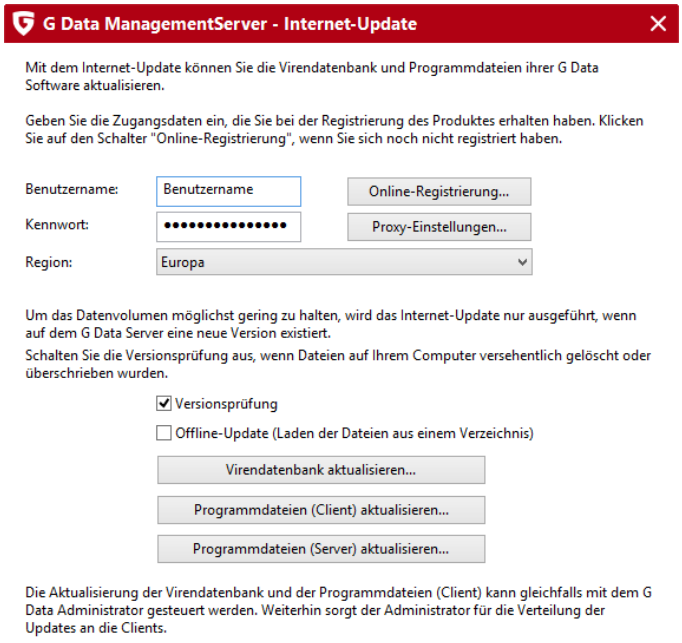

Abbildung 14: Internet-Update

Neben Aktualisierungen für den ManagementServer kann das Internet-Update auch aktualisierte Client-Programmdateien und Virensignaturen herunterladen. Diese Funktion wird auch von G DATA Administrator ausgeführt, allerdings mit einem Unterschied: Muss ein Offline-Server aktualisiert werden, können Updates mit dem Internet-Update aus einem lokalen Ordner geladen werden (siehe Abschnitt 7.3.1).

Benutzername und Kennwort müssen eingegeben werden, um Updates durchzuführen, ob mit dem Internet-Update oder automatisch mit dem G DATA ManagementServer. Diese Daten stehen nach der Online-Registrierung bereit, die normalerweise bei der Installation vom ManagementServer durchgeführt wird. Der Assistent fordert automatisch die Eingabe des Benutzernamens und Kennworts an und speichert sie. Wurde die Software jedoch nicht registriert, kann die Online-Registrierung später auch manuell mit dem Internet-Update-Tool durchgeführt werden.

Das Registrierungsformular wird über die Option ONLINE-REGISTRIERUNG geöffnet. In dieses Formular muss unter anderem die richtige Registrierungsnummer eingetragen werden. Durch Klicken auf ANMELDEN werden die Daten an G DATA übermittelt und Benutzername sowie Kennwort generiert. Benutzername und Kennwort müssen sorgfältig aufbewahrt werden, da die Registrierungsnummer nur einmal eingegeben werden darf. Bei der Neuinstallation vom ManagementServer können Benutzername und Kennwort in den Installationsassistenten eingegeben werden, um Updates zu aktivieren.

4.7. Server-Datenbank – Backup und Wiederherstellung

Wie mit allen Daten wird auch für die Datenbank des G DATA ManagementServers empfohlen, sie regelmäßig zu sichern. Bei einem Hardware-Ausfall oder anderen Problemen mit der Datenspeicherung ist so ein aktuelles Backup verfügbar, um den ManagementServer schnell wieder verfügbar zu machen. Je nach Auswahl während der Installation wird die Datenbank entweder lokal als SQL Server Express oder auf einem externen SQL Server gespeichert. Mit GdmmsConfig.exe kann ungeachtet des Speicherorts ein vollständiges Backup der Datenbank erstellt werden.

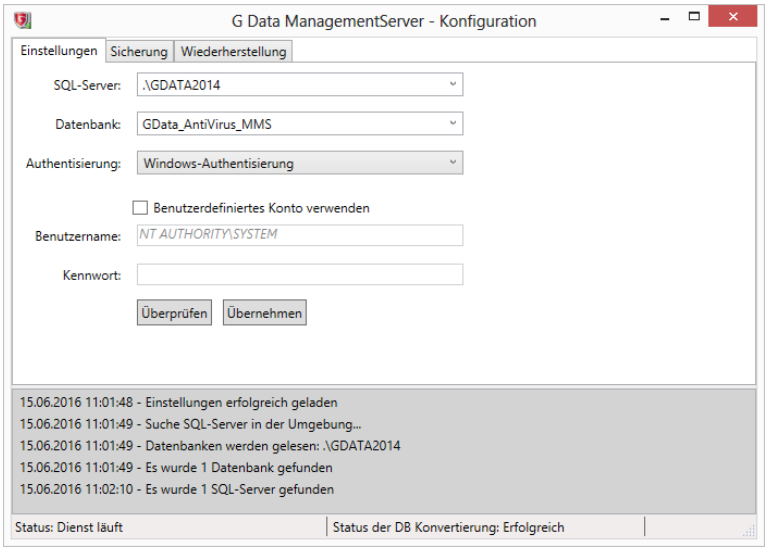

Abbildung 15: GdmmsConfig.exe

GdmmsConfig.exe befindet sich im Installationsordner vom G DATA ManagementServer, normalerweise in C:\Programme (x86)\G DATA\G DATA AntiVirus ManagementServer. Die Benutzeroberfläche zeigt

verschiedene Parameter für die SQL Server-Installation an. Durch Klicken auf EINSTELLUNGEN TESTEN wird verifiziert, ob die Datenbank erfolgreich geöffnet werden kann.

Datenbanksicherungen können jeweils mithilfe der Registerkarten BACKUP und WIEDERHERSTELLUNG angelegt bzw. wiederhergestellt werden. Bei beiden Aktionen muss ein Ordner ausgewählt werden. Wurde ein lokaler Datenbankserver definiert, kann dies ein lokaler Ordner sein. Wurde ein externer SQL-Server festgelegt, muss ein UNC-Pfad eingegeben werden, z. B. **\\Backupserver\C$\Backups**. Das zugehörige Konto des SQL Server-Dienstes benötigt Schreibrechte (für das Backup) und Leserechte (zum Wiederherstellen eines Backups) für den jeweiligen Ordner. Bitte beachten Sie, dass es sich bei diesem Konto nicht unbedingt um das handelt, das in der Registerkarte EINSTELLUNGEN konfiguriert wurde, da der ManagementServer damit nur auf den SQL Server zugreift.

Mit GdmmsConfig.exe als Befehlszeilenanwendungen können Datenbank-Backups automatisch durchgeführt werden. Damit die Datenbank regelmäßig gesichert wird, kann eine Aufgabe zur Windows-Aufgabenplanung hinzugefügt werden (Start > Ausführen > **taskschd.msc**). Durch eine wöchentliche Aufgabe mit dem entsprechenden Backup-Befehl kann im Notfall immer eine aktuelle Datenbanksicherung wiederhergestellt werden. Wie bei allen Backup-spezifischen Aufgaben muss überprüft werden, ob die konfigurierte Aufgabe erfolgreich ausgeführt und tatsächlich ein Backup am gewünschten Speicherort erstellt wurde. Die Parameter lauten wie folgt:

Parameter	Beschreibung
/dbfullbackup	Startet eine Datenbanksicherung.
/DBBackupFolder:<Ordner>	Optional. Zielordner des Backups. <Ordner> sollte ein absoluter Pfad oder ein UNC-Pfad sein, wenn die Verbindung über einen entfernten SQL Server erfolgt).
/ServerInstance:<SQL Server-Name>	Optional. Die SQL Server-Instanz mit der Datenbank.
/Database:<Datenbank>	Optional. Die zu sichernde Datenbank.
/Login:<Benutzername>	Optional. Der Benutzername, mit dem sich der ManagementServer am SQL Server anmeldet.
/Password:<Kennwort>	Optional. Das Kennwort, mit dem sich der ManagementServer am SQL Server anmeldet.

Die meisten Parameter sind optional. Wurde über GdmmsConfig zuvor ein Backup-Ordner ausgewählt, wird dieser verwendet, sofern kein Parameter gesetzt wurde. Ebenso werden Serverinstanz, Datenbankname, Benutzername und Kennwort von der vorhandenen GdmmsConfig-Konfiguration übernommen. Bei der Befehlszeilenanwendung ist also, wie auch beim Backup über die grafische Benutzeroberfläche, Vorsicht geboten: Das zum SQL Serverdienst gehörende Konto muss über die entsprechenden Schreibrechte für den Backup-Ordner verfügen. Dabei handelt es sich nicht notwendigerweise um das Konto, das mit den Parametern /Login bzw. /Password angegeben wird.

Wurde der ManagementServer mit lokalem SQL-Server-Express konfiguriert, lautet der Befehl meist **gdmmsconfig.exe /dbfullbackup /DBBackupFolder:<Ordner>** wobei **<Ordner>** durch einen absoluten Pfad zum Backup-Ordner ersetzt werden muss. Sind alle Parameter festgelegt, lautet der Befehl folgendermaßen (mit der Datenbank GData_AntiVirus_MMS auf der Instanz GDATA2014, dem Backup-Ordner MMS auf dem Server BACKUPSRV und dem Benutzerkonto „SQLAdmin“ mit dem Kennwort „Kennwort“): **gdmmsconfig.exe /dbfullbackup /DBBackupFolder:\\BACKUPSRV\MMS /Logon:SQLAdmin /Password:Kennwort /Database:GData_AntiVirus_MMS /ServiceInstance:GDATA2014**.

4.8. Client-Installation

Welche Clients in die G DATA Client-Installation einbezogen werden sollen, entscheidet der Administrator. Alle Computer im Unternehmensnetzwerk sollten geschützt werden, da bereits ein einziger ungeschützter Computer ein möglicher Zugangspunkt für Malware sein kann. Alle Windows-, Mac-, Linux-, Android- und iOS-Geräte sollten durch G DATA geschützt werden. Dazu gehören sowohl Clients als auch Server. Obwohl nicht alle G DATA Sicherheitsmodule für Server geeignet sind (z. B. die auf Clients ausgerichtete Firewall), bieten die Anti-Malware-Module vom G DATA Security Client, also beispielsweise der Dateisystemwächter, auch hervorragenden Serverschutz. Je nach Servertyp müssen zusätzliche Tests durchgeführt werden. Stabilität und Leistung sollten optimiert werden. Für den Dateisystemwächter und die Scans müssen eventuell mehrere Ausnahmen konfiguriert werden, damit regelmäßig verwendete Dateien auf einem Datenbankserver, die E-Mail-Datenbank eines Mail-Servers oder verschiedene Protokollarten und Verwaltungsdateien auf einem Domänencontroller nicht überwacht und gescannt werden.

4.8.1. Aktivieren von Windows-, Linux- und Mac-Clients

Windows-, Linux- und Mac-Clients müssen in der Ansicht CLIENTS vom G DATA Administrator hinzugefügt („aktiviert“) werden, bevor die Client-Software auf ihnen installiert werden kann. Dadurch behält der Administrator den Überblick über die Netzwerk-Clients, auch über die, auf denen die Software noch nicht installiert wurde. Der SERVER-EINRICHTUNGSASSISTENT vom G DATA Administrator enthält eine Liste mit Netzwerk-Clients, die im lokalen Netzwerk erkannt wurden und mit einem Klick aktiviert werden können. Fehlt ein Client auf der Liste, kann er manuell durch Eingabe von Namen oder IP-Adresse aktiviert werden. Wird einer oder mehrere Clients aktiviert und CLIENT-SOFTWARE AUTOMATISCH AUF DEN AKTIVIERTEN COMPUTERN INSTALLIEREN ausgewählt, werden die Clients nach Abschluss des Assistenten per Fernzugriff installiert (siehe Abschnitt 4.8.2.1). Alternativ kann die Ansicht CLIENTS verwendet werden. Hierzu wird der entsprechende ManagementServer ausgewählt, in der Symbolleiste auf CLIENT AKTIVIEREN geklickt und der Client-Name oder die IP-Adresse eingegeben. Im folgenden Fenster kann die Anzahl der zu aktivierenden Clients angegeben werden. Die dritte Option ist das Fenster COMPUTER SUCHEN im Menü ORGANISATION. In diesem Fenster kann ein ganzer IP-Bereich nach aktiven Netzwerk-Clients durchsucht werden, um sie anschließend direkt zu aktivieren. Und schließlich kann die Active Directory-Synchronisation automatisch Windows-Clients aktivieren. Dazu muss eine ManagementServer-Gruppe mit einer Active Directory-Organisationseinheit verknüpft werden, um automatisch die enthaltenen Clients auf den ManagementServer zu importieren (siehe Abschnitt 7.2).

4.8.2. Windows-Clients

Nach der Aktivierung eines oder mehrerer Windows-Clients kann der G DATA Security Client installiert werden. Vorzugsweise sollte die Installation per Fernzugriff erfolgen. Der G DATA Security Client kann auch lokal über ein Installationsmedium oder ein Client-Installationspaket bereitgestellt werden.

4.8.2.1. Installation per Fernzugriff

Die Installation vom G DATA Security Client per Fernzugriff kann folgendermaßen eingeleitet werden: Über den SERVER-EINRICHTUNGSASSISTENTEN, die Active Directory-Synchronisation (siehe Abschnitt 7.2) oder die

Auswahl eines Clients in der Übersicht CLIENTS und Auswahl der Option G DATA SECURITY CLIENT INSTALLIEREN im Kontextmenü. Eine Installation per Fernzugriff ist die einfachste und zeitsparendste Möglichkeit, um den G DATA Security Client zu installieren, da sie keinen physischen Zugang zum Client erfordert. Es könnten jedoch einige Konfigurationsänderungen notwendig sein, um den G DATA Security Client per Fernzugriff zu installieren:

- Ein Benutzerkonto mit Administrationsrechten auf dem Client muss eingegeben werden. Das Konto muss nicht unbedingt über ein Kennwort verfügen. In dem Fall müssen die Zielcomputer jedoch explizit so konfiguriert sein, dass die Netzwerkanmeldung für Konten ohne Kennwort zugelassen wird. Hierzu öffnen Sie den Group Policy Editor (START > RUN > **gpedit.msc**) und deaktivieren die Option COMPUTERKONFIGURATION > WINDOWS-EINSTELLUNGEN > SICHERHEIT EINSTELLUNGEN > LOKALE RICHTLINIEN > SICHERHEITSOPTIONEN > KONTEN: FÜR LOKALE KONTEN MUSS DIE NUTZUNG VON LEEREN KENNWÖRTERN AUF „KONSOLENANMELDUNG“ EINGESCHRÄNKT WERDEN. Wird ein Subnet-Server per Fernzugriff installiert, muss ein Kontokennwort eingerichtet werden, da ein leeres Kennwortfeld nicht zulässig ist.
- Der Service Control Manager auf dem Client muss per Fernzugriff mit dem angegebenen Benutzerkonto zugänglich sein.
- Das angegebene Benutzerkonto muss für mindestens eine Netzwerkfreigabe, z. B. C$, Admin$ oder eine benutzerdefinierte Freigabe, auf dem Client über Schreibrechte verfügen. Unter Windows Vista und höher kann der Zugriff über das NETZWERK- UND FREIGABE-CENTER > ERWEITERTE FREIGABEEINSTELLUNGEN ÄNDERN und die Aktivierung der Option DATEI- UND DRUCKERFREIGABE aktiviert werden. Unter Windows XP wird in der WINDOWS FIREWALL auf der Registerkarte AUSNAHMEN die Option DATEI- UND DRUCKERFREIGABE aktiviert.
- Befindet sich der Client in keiner Domäne, müssen zusätzliche Einstellungen konfiguriert werden:
    - Die Option EINFACHE DATEIFREIGABE (Windows XP) oder FREIGABE-ASSISTENT VERWENDEN (Windows Vista/Windows Server 2008 oder höher) muss deaktiviert werden. Sie ist standardmäßig in allen Windows-Installationen aktiviert und kann folgendermaßen deaktiviert werden: beliebigen Ordner im Windows Explorer öffnen, auf ORGANISIEREN > ORDNER- UND SUCHOPTIONEN > ANSICHT klicken und entsprechende Option deaktivieren.
    - Bei Clients unter Windows Vista und höher: Im Registrierungseditor den Schlüssel „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System“ bearbeiten. Der DWORD-Wert **LocalAccountTokenFilterPolicy** mit dem Wert 1 muss hinzugefügt werden. Weitere Informationen zu diesen Einstellungen bietet die Microsoft Website[6].

Sind alle Anforderungen erfüllt, kann die Software per Fernzugriff installiert werden. Die Sprache der G DATA Security Client-Installation kann aus einem Dropdown-Menü ausgewählt werden. Hinweis: Diese Einstellung kann nur geändert werden, wenn der Client neu installiert wird.

Im Fenster INSTALLATIONSÜBERSICHT kann der Fortschritt einer Installation per Fernzugriff mitverfolgt werden. Das Fenster öffnet sich automatisch, wenn eine Installation per Fernzugriff als Auftrag hinzugefügt wird. Es kann auch durch Klick auf die Schaltfläche INSTALLATIONSÜBERSICHT in der Symbolleiste der Ansicht CLIENTS geöffnet werden. Das Fenster enthält eine Liste aller Clients, für die Installationen per Fernzugriff

[6] Siehe https://technet.microsoft.com/en-us/library/ee844186(v=ws.10).aspx.

ausstehen oder abgeschlossen wurden. Die Spalte TYP zeigt den Installationstyp an (z. B. G DATA Security Client, G DATA Internet Security für Android oder Subnet-Server). Nach Abschluss einer Installation per Fernzugriff wird die Spalte STATUS aktualisiert. Für Clients, die durch eine Active Directory-Synchronisation hinzugefügt wurden (siehe Abschnitt 7.2), wird die Installation geplant. Unter NÄCHSTER INSTALLATIONSVERSUCH wird das geplante Installationsdatum mit Uhrzeit angezeigt. Durch Rechtsklick auf einen Eintrag und Auswahl der Option INSTALLATIONSBERICHT ANZEIGEN wird ein Protokoll angezeigt, das bei der Fehlersuche behilflich sein kann.

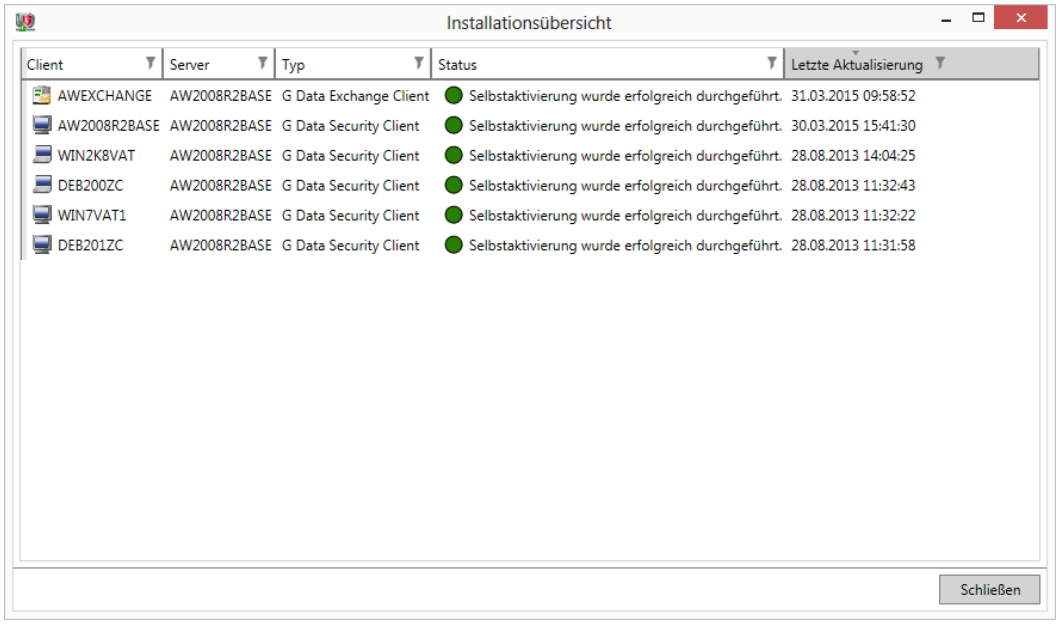

Abbildung 16: G DATA Administrator – Installationsübersicht

In manchen Fällen muss der Client neu gestartet werden, um die Installation abzuschließen. Ist ein Neustart erforderlich, wird dem Modul SICHERHEITSEREIGNISSE während der Installation ein Bericht hinzugefügt. Ist keine Installation per Fernzugriff möglich, wird der Fehler in der Spalte STATUS angezeigt. Weitere relevante Fehlercodes finden Sie in der Client-Registry (siehe Abschnitt 4.8.2.4).

4.8.2.2. Lokale Installation

Der G DATA Security Client kann lokal auf einem beliebigen Client oder Server mit unterstütztem Betriebssystem installiert werden. Das ist für Szenarien hilfreich, in denen sich ein Netzwerk-Client nicht in derselben Domäne wie der primäre ManagementServer befindet, die Systemvoraussetzungen für die Installation per Fernzugriff nicht erfüllt werden oder der Client sich nicht regelmäßig mit dem Netzwerk verbindet (Laptops). Das G DATA Installationsmedium enthält eine Installationsdatei, die mit lokalen Administratorrechten auf einem beliebigen Client ausgeführt werden kann. Das Security Client-Installationsprogramm umfasst alle verfügbaren Sprachen. Der Installationsassistent ist völlig unkompliziert: Es muss nur der Name des primären ManagementServers eingegeben werden, mit dem sich der Client verbinden soll. Optional kann ein Gruppenname eingegeben werden (weitere Informationen zur Syntax finden Sie in Abschnitt 4.8.2.3. Nach der Installation kontaktiert der Client den ManagementServer innerhalb von wenigen Minuten. Wurde ein Gruppenname eingegeben, wird er automatisch der entsprechenden Gruppe hinzugefügt. Lokal installierte Clients sind erst nach der

Autorisierung über das Modul CLIENTS voll funktionstüchtig, um unbefugten Zugriff auf den ManagementServer zu verhindern.

4.8.2.3. Client-Installationspaket

Ist keine Installation per Fernzugriff möglich und würde die Koordination lokaler Installationen aller Clients zu viel Zeit in Anspruch nehmen, ist das Client-Installationspaket eine praktische Lösung. Der ManagementServer kann eine ausführbare Datei mit der neuesten Version von Programmdateien und Virensignaturen für den G DATA Security Client und vorkonfigurierten Einstellungen erstellen, damit sich der Client nach der Installation automatisch mit dem ManagementServer verbindet. Das Client-Installationspaket kann ohne Eingreifen des Benutzers ausgeführt werden und ist die perfekte Lösung, um den G DATA Security Client im Handumdrehen in der gesamten Domäne zu installieren. Netzwerke mit Active Directory können ein Startskript verwenden, damit der Client die Installationsdatei nach der Anmeldung abruft und automatisch im Hintergrund ausführt.

Das Client-Installationspaket kann im G DATA Administrator erstellt werden. Dazu wird im Menü ORGANISATION die Option INSTALLATIONSPAKET FÜR WINDOWS-CLIENTS ERSTELLEN ausgewählt. Der Administrator fordert zur Eingabe von Installationssprache und ManagementServer auf. Der Security Client wird dann in dieser Sprachversion installiert und verbindet sich mit dem genannten ManagementServer. Die Gültigkeit des Installationspakets kann eingeschränkt werden, damit es nicht endlos verwendet werden kann (Clients, die mit einem abgelaufenen Paket installiert wurden, müssen manuell im G DATA Administrator autorisiert werden).

Wird ein Gruppenname eingegeben, wird der Client automatisch bei der ersten Verbindung zum ManagementServer dieser Gruppe hinzugefügt. Ist die Gruppe noch nicht vorhanden, wird sie automatisch angelegt. Gruppennamen können hierarchisch, mit einem Schrägstrich („/“) getrennt, eingegeben werden. Jedes Anführungszeichen im Gruppenname muss verdoppelt werden. Enthält ein Gruppenname ein „/“, muss der Gruppenname selbst in Anführungszeichen eingeschlossen werden. Um beispielsweise einen Client zur Gruppe „Workstations“ hinzuzufügen, die eine Teilgruppe von „Marketing“ ist, geben Sie **Marketing/Workstations** ein. Um einen Client zu einer Gruppe namens „Standorte 1/2/3“ hinzuzufügen, geben Sie **"Standorte 1/2/3"** ein. Um einen Client zu einer Gruppe namens „Standort “A““ hinzuzufügen, geben Sie **Standort ""A""** ein.

Und schließlich kann ein Speicherordner angegeben werden. Der G DATA Administrator erstellt das Paket im Hintergrund. Dieser Vorgang kann einige Minuten dauern. Während dieser Zeit darf der Administrator nicht geschlossen werden. Das Client-Installationspaket enthält die neueste Version des Security Clients und der Virensignatur-Updates. Dadurch wird sichergestellt, dass der Client sofort optimal geschützt ist, ohne dass separat Updates vom ManagementServer heruntergeladen werden müssen. Das heißt jedoch, dass regelmäßig ein neues Client-Installationspaket erstellt werden muss, falls die Installation über einen längeren Zeitraum andauert.

Die Erstellung von Installationspaketen kann mithilfe des Tools GData.Business.Server.Cli.exe automatisiert werden. Es befindet sich im Installationsordner vom G DATA ManagementServer. Über den Parameter **--create-install-packages** kann beispielsweise ein regelmäßig nachts durchgeführter Auftrag erstellt werden, der das Tool startet. Ein Client-Paket wird automatisch in dem über die Option

INSTALLPACKAGESFOLDER in config.xml festgelegten Ordner gespeichert (siehe Abschnitt 18.3) und kann dann im gesamten Netzwerk verteilt werden.

Die Installationspakete müssen dann nur noch auf die Clients kopiert und ausgeführt werden. Das kann manuell oder mithilfe einer Gruppenrichtlinie erfolgen. Wurde der G DATA Security Client bereits auf dem Computer installiert, wird er aktualisiert. Aufgrund der Dateigröße sollte das Client-Installationspaket nicht auf einer Netzwerkfreigabe ausgeführt werden, da die Installation fehlschlagen könnte. Soll die Installation ohne Eingreifen des Benutzers erfolgen, wird das Installationspaket mit dem Parameter **/@_QuietInstallation="true"** begonnen. Während der Security Client installiert wird, kann der Endbenutzer weiterhin mit dem Client arbeiten. Der Client muss neu gestartet werden, damit alle Komponenten einsatzbereit sind.

4.8.2.4. Fehlerbehebung

Egal, ob der Client lokal, per Fernzugriff oder mit einem Client-Installationspaket installiert wurde: Bei jeder Variante können Komplikationen auftreten. Besonders bei der Installation per Fernzugriff sind Fehler oft nicht sofort erkennbar. Es kann verschiedene Gründe geben, warum sich ein Client nach der Installation nicht mit dem ManagementServer verbindet. Am wichtigsten ist, dass der Client eine Netzwerkverbindung mit dem ManagementServer herstellen kann und umgekehrt (siehe Abschnitt 4.9). Besteht zwar eine Netzwerkverbindung, aber der Client kann nach wie vor nicht mit dem ManagementServer kommunizieren, ist die Installation vom G DATA Security Client möglicherweise fehlgeschlagen. Die Installation wird lokal protokolliert (siehe Abschnitt 18.6.1). Bei der Installation des G DATA Security Clients unter Windows Server 2016 wird der Windows Defender unter Umständen nicht automatisch deaktiviert. In diesem Fall muss er vor der Installation des G DATA Security Clients manuell deaktiviert werden. Hierfür stehen der Assistent zum Hinzufügen von Rollen und Features, die PowerShell und Gruppenrichtlinien zur Verfügung.

4.8.3. Linux-/Mac-Clients

Der G DATA Security Client für Linux und der G DATA Security Client für Mac können nach der Aktivierung eines oder mehrerer Linux- bzw. Mac-Clients installiert werden. Vorzugsweise sollte die Installation per Fernzugriff erfolgen. Alternativ können sie lokal über ein Installationsskript installiert werden.

4.8.3.1. Installation per Fernzugriff

Eine Installation per Fernzugriff erfordert auf dem Linux- bzw. Mac-Client einen aktiven SSH-Server, der so konfiguriert ist, dass eine kennwortgeschützte Authentifizierung und Root-Anmeldungen möglich sind. Dies sind normalerweise Standardeinstellungen, die jedoch bei Bedarf manuell geändert werden können. Dazu muss die SSH-Daemon-Konfigurationsdatei (normalerweise „/etc/ssh/sshd_config“) geöffnet und „PermitRootLogin“ und „PasswordAuthentication“ auf „yes“ gesetzt werden. Zu guter Letzt muss die DNS-Namensauflösung für den ManagementServer und den Client funktionieren.

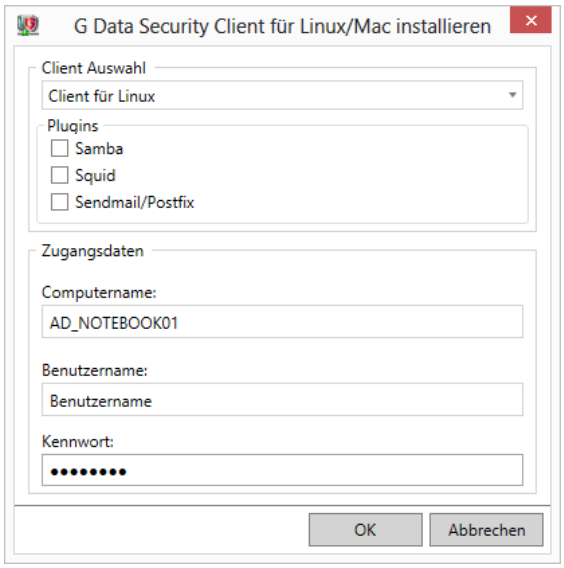

Abbildung 17: G DATA Administrator – G DATA Security Client für Linux/Mac installieren

Im Modul CLIENTS wird dann ein beliebiger Linux- bzw. Mac-Client ausgewählt, um den G DATA Administrator per Fernzugriff zu installieren. Hierzu wird im Menü CLIENTS die Option G DATA SECURITY CLIENT FÜR LINUX/MAC INSTALLIEREN gewählt. Es muss eine der beiden Client-Arten ausgewählt werden. Wird die Linux-Version installiert, können optional zusätzliche Sicherheitsmodule aktiviert werden (siehe Abschnitt 4.8.3.3). Geben Sie den BENUTZERNAMEN und das KENNWORT für ein Konto mit Root-Berechtigungen ein. Mit einem Klick auf OK wird die Installation per Fernzugriff gestartet. Das Fenster INSTALLATIONSÜBERSICHT zeigt den Installationsfortschritt an.

4.8.3.2. Lokale Installation

Starten Sie den G DATA Administrator, wählen Sie den Bereich CLIENTS und aktivieren Sie die Option INSTALLATIONSSKRIPT FÜR LINUX/MAC-CLIENTS ERSTELLEN im Menü ORGANISATION. Nach der Auswahl eines Speicherortes wird das Skript im Hintergrund erstellt. Alternativ kann die Erstellung des Installationsskripts auch automatisiert werden. Hierfür erstellen Sie einen wiederkehrenden Auftrag für das GData.Business.Server.Cli.exe-Tool, das sich im Installationsordner vom G DATA ManagementServer befindet. Das Tool wird über den Parameter **--create-install-packages** gestartet und speichert automatisch ein Installationsskript in dem über die Option INSTALLSCRIPTSFOLDER in config.xml festgelegten Ordner (siehe Abschnitt 18.3).

Kopieren Sie das Installationsskript auf den Client und fügen Sie dann die Berechtigung zur Ausführung des Skripts hinzu (Befehlszeile: **chmod +x install-client.sh**). Der Benutzerstatus kann in einem Terminal-Fenster durch Eingabe von **su** und des Root-Kennworts erhöht werden. Alternativ wird der Installationsbefehl mithilfe von sudo ausgeführt. Nun muss die Datei im Ordner, in den sie kopiert wurde, ausgeführt werden: **./install-client.sh -t <Produkt[,Produkt]>**. Bei der Installation des G DATA Security Clients für Mac sollte der Produktparameter **WS** lauten. Für die Linux-Version können es einer oder mehrere der folgenden Werte sein:

Parameter	Wert	Beschreibung
-t	**ALL**	G DATA Security Client für Linux und alle zusätzlichen Module.

WS	G DATA Security Client für Linux.
SMB	Samba-Modul.
AMAVIS	Linux Mail Security Gateway (Sendmail/Postfix)-Modul.
WEB	Linux Web Security Gateway (Squid)-Modul.

Lokal installierte Clients sind erst nach der Autorisierung über das Modul CLIENTS voll funktionstüchtig, um unbefugten Zugriff auf den ManagementServer zu verhindern.

4.8.3.3. Zusatzmodule

G DATA Security Client für Linux umfasst Zusatzmodule zum Schutz mehrerer Linux-Komponenten. Bei der Auswahl von Zusatzmodulen während der Fern- oder lokalen Installation werden die Module automatisch installiert. Einige Module müssen jedoch vor oder nach der Installation zusätzlich konfiguriert werden.

Bei der Installation zusätzlicher Module unter CentOS, Fedora, OpenSUSE, Red Hat Enterprise Linux oder SUSE Linux Enterprise Server verteilt das Installationsprogramm automatisch die Konfigurationsrichtliniendateien für SELinux. Nach der Installation befinden sich die *.te-Richtliniendateien im Ordner /etc/gdata/selinux.

Samba

Das Samba-Plug-in führt bei jedem Zugriff auf Samba-Freigaben einen Dateiscan durch und verhindert, dass sich Malware von Windows auf Linux bzw. umgekehrt ausbreitet. Nach der Installation vor Ort oder per Fernzugriff kann der Samba-Schutz aktiviert werden, indem die Zeile **vfs objects = gdvfs** in die Samba-Konfigurationsdatei eingefügt wird (normalerweise /etc/samba/smb.conf). Zum Schutz aller Freigaben muss sie in den Abschnitt **[global]** eingefügt werden. Wenn sich die Zeile in einem anderen Abschnitt befindet, gilt der Schutz nur für die entsprechende Freigabe. Nach dem Speichern der Konfigurationsdatei muss der Samba-Dienst neu gestartet werden.

Linux Mail Security Gateway

Das Linux Mail Security Gateway-Modul ist optional verfügbar.

Es wurde als Plug-in für das Amavis-Framework entwickelt. Zur Ausführung sind Amavis 2.8.0 und höher sowie altermime erforderlich. Ist Amavis nicht auf dem System verfügbar, wird es automatisch mit dem Linux Mail Security Gateway (Sendmail/Postfix)-Modul installiert. Folgende Konfigurationsschritte sind erforderlich:

1. Das Linux Mail Security Gateway-Modul benötigt einen betriebsbereiten Sendmail/Postfix-Mail-Server.
2. Der Mail-Server muss E-Mails an AMAVIS weiterleiten. Weitere Informationen finden Sie in der Dokumentation von Amavis oder des entsprechenden Mail-Servers.
3. In der Amavis-Konfiguration müssen Spam- und Virenprüfungen aktiviert sein. Weitere Informationen finden Sie in der Amavis-Dokumentation.
4. Bearbeiten Sie die Konfigurationsdatei /etc/gdata/amavis/mms.cfg. Der Name der Mail-Server-(Sub)-Domäne muss unter localDomains (z. B. mail.domaene.de) eingegeben werden.

Die Verwendung einer vorhandenen Amavis-Installation wird nicht empfohlen, da sonst direkt nach der Installation des Linux Mail Security Gateway-Moduls viele Änderungen an Konfigurationsdateien erforderlich sind. Bei Amavis-Versionen vor 2.10.0 sind nicht alle Funktionen des Moduls verfügbar. Vor der Installation des Moduls sollte Amavis auf Version 2.10.0 oder höher aktualisiert werden, um vollständige Funktionalität sicherzustellen.

Nach der Aktivierung überprüft das Linux Mail Security Gateway-Modul automatisch den E-Mail-Verkehr und meldet dem G DATA ManagementServer etwaige Viren. Dessen Einstellungen können über den G DATA Administrator im SENDMAIL/POSTFIX-Modul verwaltet werden (siehe 17.2).

Linux Web Security Gateway

Das Linux Web Security Gateway-Modul ist optional verfügbar.

Bei Auswahl des Linux Web Security Gateway (Squid)-Moduls wird es bei der Installation des G DATA Security Clients für Linux automatisch installiert und konfiguriert. Verfügt das System bereits über Squid, wird diese Version zuvor deinstalliert. Bei der Installation des Squid-Servers wird das im Repository der jeweiligen Distribution verfügbare Paket verwendet. Ist dies eine Squid-Version vor 3.3.8, können keine HTTPS-Scans ausgeführt werden.

Nach der Installation sollte der Hostname oder die IP-Adresse des Squid-Servers als Proxyserver auf allen Systemen konfiguriert werden, deren Datenverkehr mit Squid (Port 3128) gefiltert werden soll. Zusätzlich sollte ein HTTPS-Proxy mit dem Hostnamen oder der IP-Adresse und Port 6789 konfiguriert werden, um HTTPS-Datenverkehr scannen zu können. Die erforderlichen Zertifikate befinden sich im Ordner /etc/gdata/ssl auf dem Squid-Server und sollten auf alle Clients importiert werden. Eigene SSL-Zertifikate müssen zur Verwendung auf dem Server im Ordner /etc/gdata/ssl gespeichert werden.

Nach der Aktivierung gleicht das Linux Web Security Gateway-Modul automatisch den Datenverkehr mit der Black- und Whitelist ab und meldet dem G DATA ManagementServer etwaige Viren. Dessen Einstellungen können über den G DATA Administrator im SQUID-Modul verwaltet werden (siehe Abschnitt 8.5).

4.8.3.4. Fehlerbehebung

Bei der Installation des G DATA Security Client für Mac unter Mac OS X 10.7 schlägt die Ferninstallation von Upgrades unter Umständen fehl, falls der G DATA Security Client bereits auf dem Client installiert war. In diesem Fall sollte das Upgrade lokal ausgeführt werden.

4.8.4. Android-Clients

Android-Clients können mit dem G DATA Administrator installiert werden. Vor der Installation muss in ALLGEMEINE EINSTELLUNGEN > ANDROID > AUTHENTIFIZIERUNG FÜR ANDROID-CLIENTS ein Kennwort eingegeben werden. Die Installation erfolgt per E-Mail. In der Ansicht CLIENTS wird ein Android-Client oder eine Gruppe ausgewählt und auf die Symbolleistenschaltfläche INSTALLATIONSLINK AN MOBILE CLIENTS SENDEN geklickt. Es können mehrere E-Mail-Adressen eingegeben werden, denn die Aktivierungs-Mail kann an beliebige E-Mail-Adressen gesendet werden. Die E-Mail enthält einen Link, um die Installationsdatei von Internet Security für Android vom ManagementServer herunterzuladen. Die APK-Installationsdatei wird durch

Tippen auf den Download-Link heruntergeladen. Dabei muss die Option UNBEKANNTE HERKUNFT (INSTALLATION VON APPS AUS UNBEKANNTEN QUELLEN ZULASSEN) aktiviert sein, um die APK-Dateien installieren zu können. Diese Option befindet sich im Android-Systemmenü unter EINSTELLUNGEN > SICHERHEIT > GERÄTEVERWALTUNG. Nach dem Öffnen der APK-Datei und der Bestätigung der angefragten Berechtigungen wird die G DATA Internet Security für Android installiert und kann im Android App-Menü gestartet werden.

Zur Aktivierung der Administration per Fernzugriff muss der zweite Link in der Installations-Mail geöffnet werden. Die G DATA Internet Security für Android wird automatisch mit den richtigen Serverdaten konfiguriert. Alternativ kann die Administration per Fernzugriff manuell konfiguriert werden. Dazu muss auf das Einstellungssymbol in der oberen rechten Ecke des Bildschirms getippt, das Kontrollkästchen FERNADMINISTRATION GESTATTEN aktiviert und unter SERVERADRESSE der Name oder die IP-Adresse vom ManagementServer eingegeben werden. Unter GERÄTENAME kann ein Name zur Identifizierung des Geräts im G DATA Administrator angegeben werden. Das Feld KENNWORT muss das im G DATA Administrator eingegebene Kennwort enthalten (auch in der Installations-Mail enthalten). Das Gerät wird im Modul CLIENTS des G DATA Administrators zusammen mit den anderen Clients aufgeführt und von dort verwaltet. Wird das Gerät nicht automatisch angezeigt, muss es neu gestartet werden, um eine Anmeldung am ManagementServer zu erzwingen.

4.8.5. iOS-Clients

iOS-Clients können mit über den G DATA Administrator installiert werden. Da die Kommunikation mit iOS-Geräten vom G DATA ActionCenter verwaltet wird, muss unter https://ac.gdata.de ein kostenloses Konto angelegt werden. Im G DATA Administrator sind die Kontodetails im Modul ACTIONCENTER einzugeben. Außerdem ist eine gültige G DATA Lizenz erforderlich. Benutzername und Kennwort für das Internet-Update müssen unter UPDATES > ZUGANGSDATEN UND EINSTELLUNGEN eingegeben werden.

Die Installation erfolgt per E-Mail. Dazu wird in der Ansicht CLIENTS unter IOS MOBILE DEVICE MANAGEMENT ein Gerät ausgewählt und auf die Symbolleistenschaltfläche INSTALLATIONSLINK AN MOBILE CLIENTS SENDEN geklickt. Wie bei der Android-Client-Installation können mehrere E-Mail-Adressen eingegeben werden. Zusätzlich ist die Angabe von Parametern möglich, die auf dem iOS-Gerät angezeigt werden, wenn der Endbenutzer die MDM-Anfrage prüft. In der MDM-Anfrage und auch in der Liste der iOS-MDM-Profile werden NAME, BESCHREIBUNG und ORGANISATION angezeigt. Mit dem END USER LICENSE AGREEMENT kann der Endbenutzer darüber informiert werden, dass das Gerät per Fernzugriff verwaltet wird. Öffnet der Endbenutzer den Link aus der Installations-Mail auf einem iOS-Gerät, wird es sofort im G DATA Administrator angezeigt (wobei der SICHERHEITSSTATUS auf der Registerkarte CLIENTS als „Ausstehend“ angezeigt wird). Sobald der Endbenutzer die MDM-Anfrage akzeptiert, kann das iOS-Gerät vollständig über den G DATA Administrator verwaltet werden.

4.9. Abschließen der Installation

Nach der Installation von Server(n) und Clients muss überprüft werden, ob alle Prozesse ordnungsgemäß ausgeführt werden und alle Sicherheitsmaßnahmen eingerichtet wurden. Am wichtigsten ist, dass sich alle Clients mit dem ManagementServer verbinden können. Jeder Windows-, Mac- und Linux-Client meldet seinen Status standardmäßig alle fünf Minuten an den ManagementServer (allerdings nicht während eines geplanten Scans). Mit dem Modul CLIENTS vom G DATA Administrator können

Verbindungsprobleme erkannt und behoben werden. Zunächst muss geprüft werden, ob alle Netzwerk-Clients in der Ansicht CLIENTS aufgeführt sind. Fehlt ein Client, wurde er möglicherweise nicht richtig installiert. Je nach Installationsmethode kann nun versucht werden, den Client manuell hinzuzufügen und zu aktivieren. Alternativ kann im Domänencontroller des Netzwerks überprüft werden, ob der Client zu Active Directory hinzugefügt wurde. Wird der Client aufgeführt, zeigt die Spalte LETZTER ZUGRIFF an, wann sich der Client das letzte Mal mit dem ManagementServer verbunden hat. Der Client muss mit dem Netzwerk verbunden und eingeschaltet sein. Der TCP-Datenverkehr muss für die relevanten Ports sowohl auf dem Client (7169) als auch auf dem Server (7161) zugelassen sein. Und schließlich muss der Client in der Lage sein, die IP-Adresse des Servers aufzulösen. Als Verbindungstest dient der Befehl **telnet** auf dem Client, um eine Verbindung mit dem Server herzustellen: **telnet <ManagementServer-IP> <ManagementServer-Port>**. Kann sich der Client mit dem Server verbinden, werden in der Eingabeaufforderung kryptische Zeichen angezeigt. Besteht keine Verbindung, erscheint ein leeres Eingabefenster. Weitere Informationen zum Modul CLIENTS und zur Clientverwaltung finden Sie in Kapitel 7.

Wenn sich alle Clients regelmäßig mit dem ManagementServer verbinden und durch die standardmäßigen Netzwerkeinstellungen geschützt sind, ist die grundlegende Installation abgeschlossen. Es gibt jedoch weitere Dienste, die konfiguriert werden müssen. Damit die Konfiguration schnell geändert werden kann, sollte die G DATA Lösung für die Administration per Fernzugriff konfiguriert werden (siehe Kapitel 5). Die Echtzeitschutzeinstellungen müssen für jeden Client nach Bedarf angepasst werden (siehe Kapitel 8). Es können wiederkehrende Aufgaben geplant werden, um Malware-Scans (siehe Kapitel9) und Backups (siehe Kapitel 12) durchzuführen. Wird auch die Firewall der G DATA Lösung installiert, sind ihre Einstellungen zu konfigurieren (siehe Kapitel 13). Einige erweiterte Einstellungen erfordern jedoch die Bearbeitung der Konfigurationsdateien oder das spezialisierte G DATA Konfigurationstool (siehe Kapitel 18).

4.10. Subnet-Server

Ist die Systemleistung nach der Installation des primären ManagementServer und seiner Clients nicht zufriedenstellend, kann die Serverlast über Verbindungsbegrenzungen oder eine Neukonfiguration der Aufgaben verringert werden (siehe Abschnitt 7.5). Eine effektive Alternative ist jedoch die Installation eines oder mehrerer Subnet-Server. Ein Subnet-Server unterstützt den primären ManagementServer. Clients können einem Subnet-Server zugeordnet werden und verbinden sich mit diesem Server, um Virensignaturen zu erhalten. Dies verringert sowohl die Last auf dem primären ManagementServer als auch den Netzwerkdatenverkehr zwischen Clients und primärem ManagementServer. Ein Teilnetz wird insbesondere für lokale Niederlassungen empfohlen: Müssen sich die Clients nicht mehr über das WAN mit dem primären ManagementServer verbinden, kann eine optimale Geschwindigkeit der Server-Client-Kommunikation erreicht werden.

Jeder Netzwerkcomputer, der die Systemvoraussetzungen erfüllt, kann als Subnet-Server konfiguriert werden. Empfohlen wird eine Installation per Fernzugriff über den G DATA Administrator. Mit der Option SUBNET-SERVER INSTALLIEREN in SERVERS > ÜBERSICHT kann ein beliebiger Computer im Netzwerk ausgewählt werden. Nach der Eingabe der Anmeldedetails für ein Administratorkonto mit Berechtigungen für diesen Computer erfolgt die Installation per Fernzugriff. Im Fenster INSTALLATIONSÜBERSICHT wird der Installationsstatus angezeigt. Eine Installation per Fernzugriff erfordert, dass der zukünftige Subnet-

Server die gleiche Konfiguration wie ein für die Installation per Fernzugriff eingestellter Client aufweist. Weitere Informationen zu den Voraussetzungen finden Sie in Abschnitt 4.8.2.1. Unter Windows Server 2003/2008 und Windows Vista können Subnet-Server nicht per Fernzugriff installiert werden, da Microsoft SQL Server 2014 Express diese Betriebssysteme nicht unterstützt. Auf solchen Systemen können Subnet-Server nach der manuellen Installation von Microsoft SQL Server 2008 R2 Express über eine lokale Installation des G DATA ManagementServers installiert werden (siehe Abschnitt 4.2.1).

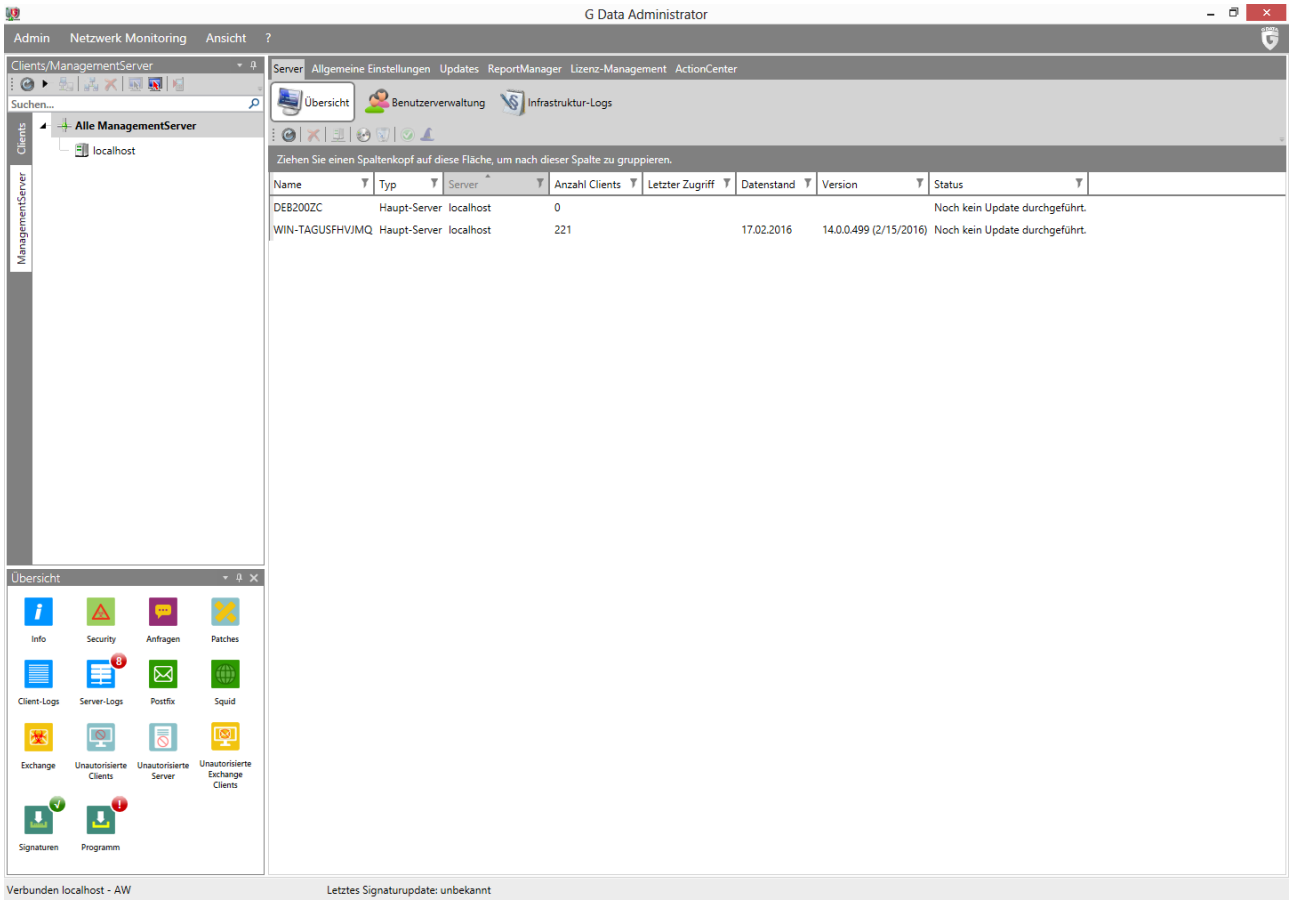

Abbildung 18: G DATA Administrator – Server-Übersicht

Ist keine Installation per Fernzugriff möglich, können Subnet-Server auch über das G DATA Installationsmedium lokal installiert werden. Die Installation entspricht dem Vorgang für einen primären ManagementServer (siehe Abschnitt 4.2.1). Dazu wird der Server-Typ SUBNET-SERVER ausgewählt und der Computername des primären ManagementServer eingegeben, damit der Subnet-Server den richtigen Hauptserver kontaktieren kann. Nach Abschluss der Installation verbindet sich der Subnet-Server mit dem primären ManagementServer. Damit keine betrügerischen Subnet-Server im Netzwerk installiert werden, die unbefugt Daten vom ManagementServer erhalten könnten, muss jeder lokal installierte Subnet-Server manuell autorisiert werden. Dazu wird in SERVER > ÜBERSICHT der neu hinzugefügte Subnet-Server ausgewählt und auf AUTORISATION ERTEILEN geklickt, um dem ManagementServer die Synchronisation seiner Datenbank mit dem Subnet-Server zu erlauben.

Nach der Installation des Subnet-Servers können die Clients vom primären ManagementServer durch die Option CLIENTS ZUORDNEN auf den neu installierten Subnet-Server verschoben werden.

5. Administration per Fernzugriff

Manchmal muss die Konfiguration ungeplant geändert werden. Möglicherweise muss von unterwegs oder über einen Computer ohne das Konfigurationstool G DATA Administrator auf die Konfiguration vom G DATA ManagementServer zugegriffen werden. G DATA lässt sich vollständig über den Browser bzw. eine Auswahl der am häufigsten genutzten mobilen Geräte (wie Smartphones und Tablets) konfigurieren.

Während der Installation vom G DATA ManagementServer wird das Konfigurationstool G DATA Administrator auf demselben Computer installiert. Die Konfiguration vom G DATA ManagementServer kann dann lokal am Servercomputer, per Fernzugriff über das Remotedesktopprotokoll von Windows oder mithilfe einer Fernsteuerlösung eines Drittanbieters erfolgen. Außerdem kann der G DATA Administrator auf anderen Computern ausgeführt werden, ohne dass eine Sitzung auf dem Server erforderlich ist. Dazu wird das Tool auf einem Computer mit Netzwerkzugriff zum Server installiert.

Optional können die Konfigurationsfunktionen der G DATA Lösung per Fernzugriff zugänglich gemacht werden. Der G DATA Administrator kann so installiert und konfiguriert werden, dass der Zugriff von außerhalb des Netzwerks möglich ist. Falls der Administrator jedoch nicht installiert werden kann, bietet der G DATA WebAdministrator eine Browser-basierte Oberfläche zum Zugriff auf alle Einstellungen und Module. Für mobile Benutzer ist der G DATA MobileAdministrator die perfekte Oberfläche für die am häufigsten ausgeführten Aufgaben wie z. B. Client- und Sicherheitsverwaltung bzw. Berichtprüfung.

5.1. Desktop-Anwendung

Bei der standardmäßigen Installation des G DATA ManagementServers wird der G DATA Administrator auf demselben Computer installiert. Die Anmeldung am G DATA Administrator kann lokal oder per Fernzugriff am Server erfolgen, um auf alle Module zuzugreifen. Ist der Zugriff auf den Server über eine Desktop-Anwendung nicht möglich oder praktikabel, kann der G DATA Administrator auch auf einem anderen Windows-Client installiert werden, solange sich dieser mit dem ManagementServer verbinden kann.

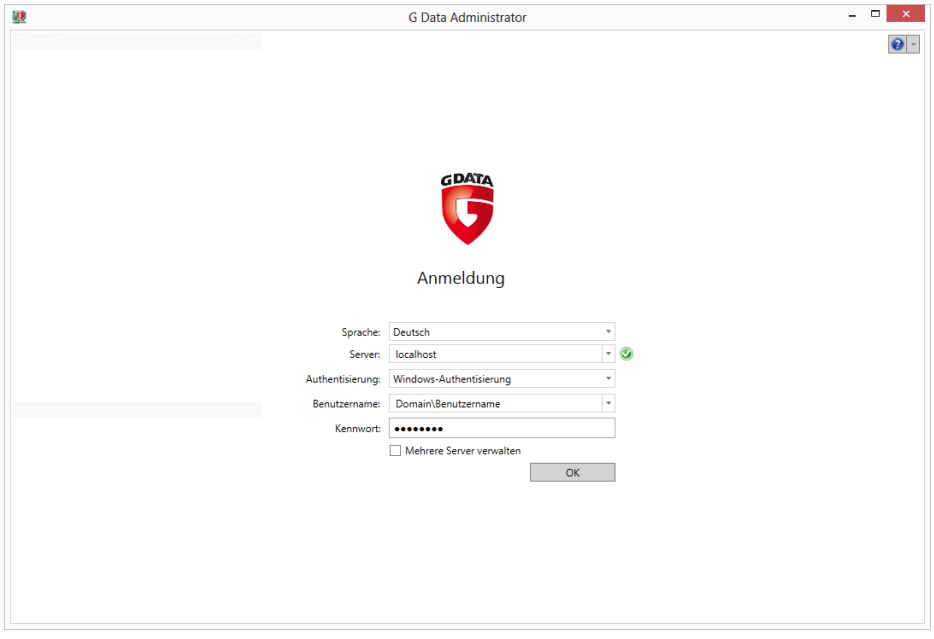

Abbildung 19: G DATA Administrator – Anmeldung

Über das G DATA Installationsmedium wird der G DATA Administrator auf dem Computer installiert, über den die Konfigurationsaufgaben ausgeführt werden. Zur Anmeldung muss die IP-Adresse oder (falls auflösbar) der Name des ManagementServer-Computers als SERVER-Adresse eingegeben werden. Der Server-Port darf dabei nicht von der Firewall gesperrt werden und muss ggf. auf Routerebene weiterleitbar sein.

5.2. Browser

Nicht immer steht genügend Zeit zur Verfügung, um den G DATA Administrator auf einem Computer zu installieren. Lokale Richtlinien können die Installation der Software verhindern oder eine dringende Angelegenheit erfordert die sofortige Aufmerksamkeit und lässt keine Zeit für eine Software-Installation. In diesen Fällen ist es sehr praktisch, den G DATA ManagementServer einfach über den Browser zu konfigurieren. Genau diese Möglichkeit bietet das webbasierte Modul G DATA WebAdministrator. Der WebAdministrator wird am häufigsten auf einem vorhandenen Webserver im Unternehmensnetzwerk installiert, kann jedoch auch auf einem beliebigen Windows-Computer mit Microsoft-Internetinformationsdiensten (IIS) ausgeführt werden. Die folgenden Versionen von IIS werden mit den entsprechenden Betriebssystemen unterstützt:

IIS-Version	*Betriebssystem*
5.1	Windows XP Professional
6.0	Windows Server 2003
7.0	Windows Server 2008, Windows Vista
7.5	Windows Server 2008 R2, Windows 7
8.0	Windows Server 2012, Windows 8
8.5	Windows Server 2012 R2, Windows 8.1
10	Windows Server 2016, Windows 10

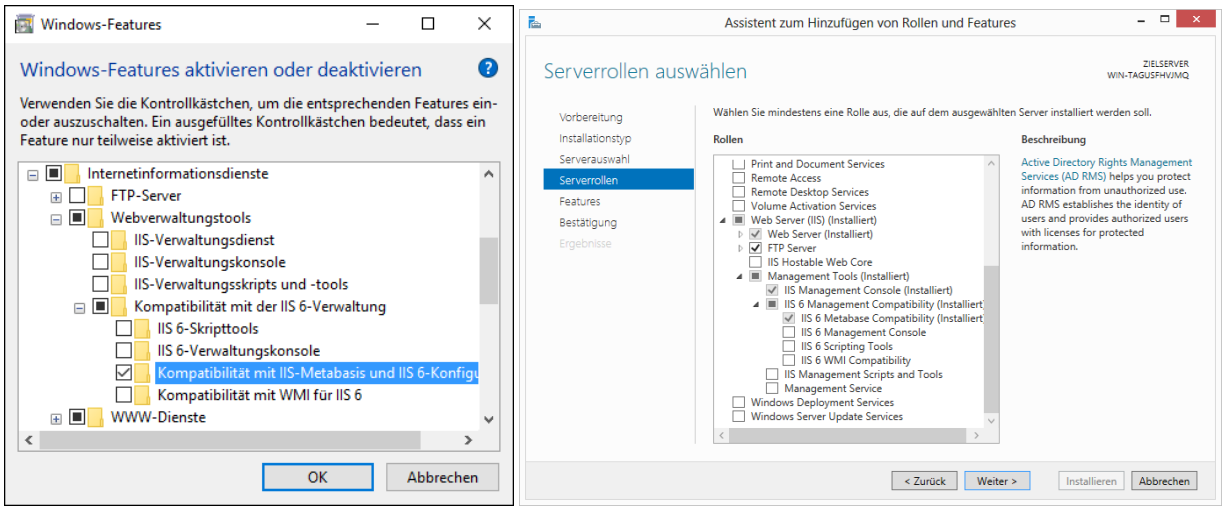

Abbildung 20; 21: Windows 10 > Windows-Features; Windows Server 2012 > Assistent zum Hinzufügen von Rollen und Features

Microsoft IIS muss vor dem WebAdministrator installiert werden. Jede oben aufgeführte Windows-Version beinhaltet die IIS-Komponente, die oft jedoch manuell aktiviert werden muss. Dazu muss unter Windows Vista der Bereich WINDOWS-FUNKTIONEN geöffnet werden (unter SYSTEMSTEUERUNG > PROGRAMME UND FUNKTIONEN). Durch Auswahl von INTERNETINFORMATIONSDIENSTE wird das vollständige Webserver-Paket installiert. Es können jedoch auch einzelne Komponenten ausgesucht werden. Außerdem muss KOMPATIBILITÄT MIT DER IIS 6-VERWALTUNG > KOMPATIBILITÄT MIT IIS-METABASIS UND IIS 6-KONFIGURATION aktiviert werden, da der WebAdministrator diese Funktionalität benötigt, sowie das .NET Framework 3.5 und 4.5 samt entsprechender Funktion HTTP-AKTIVIERUNG (für Windows 8/Windows Server 2012 und höher). Durch Klicken auf OK werden die IIS installiert und der Computer wird bei Aufforderung neu gestartet.

Unter Windows Server 2003 muss nun die Anwendung „Serververwaltung“ aus dem Startmenü aufgerufen werden. Bei Windows Server 2008 und höher wurde diese Funktion in „Server-Manager“ umbenannt. Bei beiden Anwendungen kann die aktuelle Serverkonfiguration um Rollen erweitert werden. Unter Windows Server 2003 heißt die entsprechende Rolle ANWENDUNGSSERVER (IIS, ASP.NET) und unter Windows Server 2008 und höher WEBSERVER (IIS). Für die letzten beiden muss im Fenster ROLLENDIENSTE die Option IIS 6-METABASISKOMPATIBILITÄT ausgewählt werden. Nach der Installation der Webserver-Rolle (und einem eventuellen Neustart des Servers) muss der Zugriff auf den Webserver getestet und im lokalen Browser **http://localhost** geöffnet werden.

Wie bei jeder Website besteht auch beim Browser-Zugriff auf den G DATA WebAdministrator die Gefahr, den HTTP-Verkehr für Angreifer mit Netzwerkzugang zu öffnen. Insbesondere in Szenarien, in denen von außerhalb des Unternehmensnetzwerks auf den G DATA WebAdministrator zugegriffen wird, empfiehlt sich der Schutz des Datenverkehrs, beispielsweise mit einem SSL-Zertifikat. Zertifikate können von einer Zertifizierungsstelle erworben oder kostenlos lokal erstellt und selbst signiert werden. Die erste Option wird dann empfohlen, wenn von außerhalb des Unternehmensnetzwerks auf den WebAdministrator zugegriffen wird. Sie ist jedoch mit zusätzlichen Kosten verbunden, wenn das Unternehmen nicht bereits ein oder mehrere Zertifikate besitzt. Die zweite Option ist einfach konfigurierbar und schützt vor dem Abhören des HTTP-Verkehrs.

Mit Windows XP Professional oder Windows Server 2003 kann über das kostenlose Microsoft-Tool „SelfSSL“, das auf der Microsoft-Website als Teil der IIS 6.0-Tools im Resource Kit verfügbar ist, ein SSL-Zertifikat hinzugefügt werden[7]. Nach der Installation wird die SelfSSL-Befehlszeile über „Start > Programme > IIS-Ressourcen > SelfSSL“ geöffnet. Der lokalen Website kann mit einem einzigen Befehl **selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T** ein selbstsigniertes Zertifikat hinzugefügt werden. Die Zertifikatserstellung wird durch Drücken auf **Y** bestätigt. Hierdurch wird ein Zertifikat für die IIS-Standard-Website auf dem lokalen Server angelegt und der **localhost** zur Liste der vertrauenswürdigen Zertifikate hinzugefügt. Die Schlüssellänge beträgt 2.048 und das Zertifikat ist 365 Tage lang gültig. Ist die Website keine standardmäßige IIS-Website, muss der BEZEICHNER unter „Start > Verwaltungstools > Internetinformationsdienste (IIS)-Manager“ gesucht und der Parameter **/S:1** entsprechend geändert werden.

Unter Windows Vista/Windows Server 2008 und höher wird nun der Internetinformationsdienste (IIS)-Manager geöffnet. Hierzu wird unter „Start > Ausführen“ (oder alternativ die Windows-Taste und R drücken) der Befehl **inetmgr** eingegeben. Anschließend wird der lokale Webserver im Bereich „Verbindungen“ ausgewählt. In der Mitte des Fensters muss im Bereich IIS nun auf SERVERZERTIFIKATE

[7] Siehe www.microsoft.com/en-us/download/details.aspx?id=17275.

doppelgeklickt werden. In AKTIONEN wird SELBSTSIGNIERTES ZERTIFIKAT ERSTELLEN ausgewählt. Nach der Eingabe eines Anzeigenamens wird das Zertifikat erstellt und im Bereich SERVERZERTIFIKATE gelistet. Hinweis: Das standardmäßige Ablaufdatum des Zertifikats liegt genau ein Jahr nach dem Erstelldatum. Die entsprechende Website muss im Bereich VERBINDUNGEN ausgewählt werden, um das Zertifikat auf die Websitekommunikation anzuwenden. Dazu wird im rechten Bereich AKTIONEN die Option BINDUNGEN ausgewählt. Durch Klicken auf „Hinzufügen“ wird eine neue Bindung hinzugefügt. Anschließend wird der Typ **https** und im Dropdown-Menü SSL-ZERTIFIKAT das neue Zertifikat ausgewählt. Durch Klicken auf OK wird die Bindung hinzugefügt.

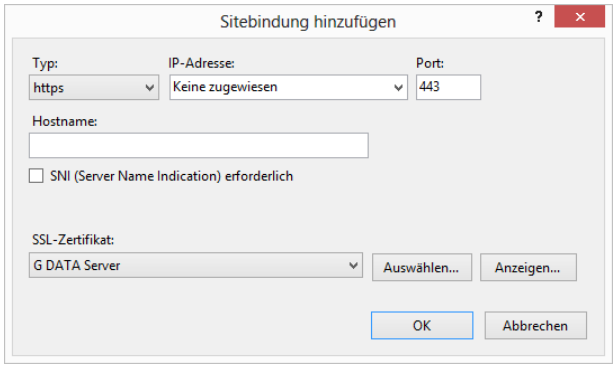

Abbildung 22: Internetinformationsdienste (IIS)-Manager – Websitebindung hinzufügen

Nach der Konfiguration der IIS kann der G DATA WebAdministrator installiert werden. Dies erfolgt mit dem Einrichtungsassistenten auf dem G DATA Installationsmedium. Microsoft .NET Framework wird automatisch installiert, wenn die erforderliche Version nicht auf dem Server verfügbar ist. Nach der Installation kann über den Browser auf den WebAdministrator zugegriffen werden, indem der Unterordner „/GDAdmin“ (wie z. B. **https://10.0.2.150/GDAdmin**) geöffnet wird. Falls kein SSL-Zertifikat auf dem Webserver installiert ist, kann alternativ **http://** eingegeben werden. Der Ordner lautet anders, falls der Installationsordner geändert wurde. Bei einem selbstsignierten Zertifikat zeigen manche Browser möglicherweise eine Warnung an, bevor der WebAdministrator geöffnet wird. Die Kommunikation ist dennoch komplett verschlüsselt. Wurde noch kein Silverlight-Browser-Plug-in installiert, wird der Benutzer beim ersten Besuch dazu aufgefordert.

Der G DATA WebAdministrator ermöglicht die Anmeldung an jedem beliebigen ManagementServer. Anmeldungsauthentifizierung, Benutzeroberfläche und Funktionen entsprechen genau denen vom G DATA Administrator. Über die Weboberfläche können alle Konfigurations- und Verwaltungsaufgaben durchgeführt werden.

5.3. Mobile

Bei direkt auszuführenden Konfigurationsaufgaben sind der G DATA Administrator und der G DATA WebAdministrator nicht immer die ideale Lösung. Für den Fall, dass kein Zugriff per Software oder Desktop-Browser möglich ist, hat G DATA die Anwendung MobileAdministrator entwickelt. Über eine für mobile Geräte optimierte Weboberfläche bietet er Zugriff auf die am häufigsten verwendeten Funktionen vom G DATA Administrator. Der MobileAdministrator kann auf allen Smartphone-Plattformen und auf allen Tablets verwendet werden und benötigt im Gegensatz zum WebAdministrator auch kein Silverlight-Plug-in.

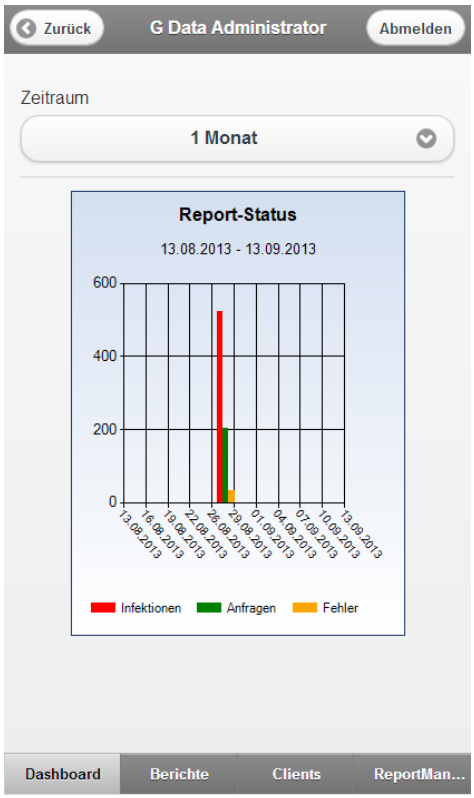

Abbildung 23: G DATA MobileAdministrator – Dashboard

Mit der Webanwendung können Clients verwaltet und die neuesten Berichte über Malware-Infektionen, PolicyManager-Anfragen und mehr eingesehen werden. Die Webanwendung bietet nicht nur passive Berichtsfunktionen, sondern unterstützt auch direkte Reaktionen. Malware-Infektionen können überprüft und direkt behoben werden. Dateien können in Quarantäne gestellt bzw. zurückgeholt werden und mit dem PolicyManager lassen White- und Blacklists sich direkt bearbeiten. Außerdem ist die Webanwendung eine gute Möglichkeit, um sich einen schnellen Überblick über den Status aller Netzwerk-Clients zu verschaffen. Berichte können mithilfe des ReportManager-Moduls definiert und in einer Vorschau angezeigt werden.

Der MobileAdministrator ist wie der WebAdministrator eine Webanwendung. Sie kann über das G DATA Installationsmedium installiert werden, wenn die Microsoft-Internetinformationsdienste (IIS) bereits vorhanden sind. Der MobileAdministrator erfordert mindestens Windows 7 oder Windows Server 2008 R2. Weitere Informationen zur Konfiguration der IIS, einschließlich eines SSL-Zertifikats, finden Sie in Abschnitt 5.2.

5.4. MasterAdmin

Auch wenn sich der Administrator mit G DATA Administrator, WebAdministrator oder MobileAdministrator an jedem ManagementServer anmelden kann, sollten sehr große Netzwerke aus Gründen der Effektivität mit dem MasterAdmin verwaltet werden. Mit dieser Version vom G DATA Administrator lassen sich mehrere ManagementServer über eine einzige Oberfläche verwalten, wodurch Konfiguration und Installation vereinfacht werden. Zur Verwaltung von mehreren Servern kann die MasterAdmin-Funktion im G DATA Administrator aktiviert werden. Managed-Service-Partner sowie Endkunden, die ein großes Netzwerk mit mehreren ManagementServer-Installationen verwalten, können

bei G DATA einen MasterAdmin-Aktivierungscode anfordern. Zur Aktivierung der entsprechenden Anmeldeoptionen muss im normalen Anmeldefenster die Option MEHRERE SERVER VERWALTEN ausgewählt werden. Anschließend werden der Aktivierungscode sowie ein Benutzername und ein Kennwort der Wahl eingegeben. Nach der erfolgreichen Anmeldung wird automatisch der MASTERADMIN-ASSISTENT gestartet. Mit dem Assistenten können die ManagementServer hinzugefügt werden, die per Fernzugriff administriert werden sollen. Dazu müssen Domänenname oder IP-Adresse des Servers sowie Benutzernamen und Kennwort eingegeben werden. Durch Eingabe eines Aliasnamens kann der Server von anderen Servern in der MasterAdmin-Schnittstelle unterschieden werden. Durch Klicken auf WEITER wird ein neuer Server hinzugefügt. Mit Klick auf FERTIGSTELLEN wird der Assistent geschlossen. Der MasterAdmin-Assistent kann jederzeit über das Menü ADMIN geöffnet werden.

Nach dem Hinzufügen der Server können die in MasterAdmin verfügbaren Optionen praktisch nicht mehr von den normalen Funktionen von G DATA Administrator unterschieden werden. Jeder ManagementServer und seine Clients können in der Ansicht CLIENTS ausgewählt und so verwaltet werden. Je nach Lizenz des ausgewählten Servers werden die entsprechenden Module auf der rechten Seite angezeigt.

Abschnitt B: Verwenden von G DATA Unternehmenslösungen

6. Dashboard und Überwachung

Nach der erfolgreichen Installation von G DATA Unternehmenslösungen im Netzwerk sind alle Clients laufend geschützt. Der Sicherheitsstatus jedes Clients muss jedoch regelmäßig überprüft werden. Es gibt verschiedene Gründe, warum der Schutz unterbrochen werden kann. Netzwerkprobleme oder ungenügender Festplattenspeicher können die Verteilung von Updates verhindern. Programm- und Treiber-Updates können mit einem Schutzmodul in Konflikt stehen oder die Leistung beeinträchtigen. Die Ausführung einer Sicherheitslösung ist kein in sich geschlossener Prozess. Alle relevanten Informationen müssen effizient zugänglich sein und der Administrator muss bei potenziellen Dienstunterbrechungen benachrichtigt werden.

G DATA Sicherheitslösungen bieten verschiedene Benachrichtigungsoptionen. Die wichtigsten Informationen werden im Bereich ÜBERSICHT des G DATA Administrators angezeigt. Die Übersicht umfasst ungelesene Berichte, Protokolle und andere Statusinformationen. Über die Symbole und vorkonfigurierte Filtereinstellungen kann auf die jeweiligen Module zugegriffen werden, um nur die angeforderten Daten anzuzeigen. Eine weitere Statistik befindet sich im Modul DASHBOARD. Es enthält Diagramme mit Informationen über Infektionen, Client-Verbindungen und vielem mehr. Gängige Aufgaben können direkt ausgeführt werden, wie die Aktualisierung von Virensignaturen oder die Aktivierung der Firewall. Einen umfassenderen Überblick über den Client-Status bietet die Registerkarte ÜBERSICHT im Modul CLIENTS. Sie enthält die Spalte SECURITY-STATUS, die sofort zeigt, wenn einzelne Clients besonderes Augenmerk erfordern. Weitere Statistiken finden Sie im Modul STATISTIK. Auch die Clients erstellen Berichte über Malware-Infektionen, beschädigte Dateien und vieles mehr. Diese Berichte können über das Modul SICHERHEITSEREIGNISSE aufgerufen werden, wo bei einigen Benachrichtigungsarten direkt reagiert werden kann. Mit dem Modul REPORTMANAGER schließlich kann der Administrator eigene Berichte aus verschiedenen Modulen zusammenstellen und regelmäßig per E-Mail erhalten.

Empfohlen wird die Einrichtung eines ausgewogenen Benachrichtigungssystems. Die Kombination aus statistischen Informationen, E-Mail-Benachrichtigungen und ReportManager-Berichten bietet einen guten Überblick. Enthält der Softwarebericht jedoch mehr Informationen als notwendig, können wichtige Benachrichtigungen untergehen.

6.1. Übersicht, Dashboard und Statistik

Standardmäßig wird im G DATA Administrator unten links der Bereich ÜBERSICHT angezeigt. Je nach installierter Lösung enthält er Verknüpfungssymbole und Statusangaben zu Berichten, Protokollen, Updates und unautorisierten Clients. Gibt es ungelesene Berichte oder Protokolle, wird deren Anzahl in einem Statusindikator angezeigt. Durch Klicken auf ein Symbol wird das relevante Modul bzw. die jeweilige Ansicht direkt mit den passenden Filtern aktiviert und ermöglicht Zugriff auf grundlegende Angaben.

Über die Ansicht DASHBOARD erhält der Administrator sofort einen detaillierteren Überblick über wichtige Statistiken. Die Diagramme sind ein sehr wertvolles Hilfsmittel, um Anomalien im Schutzstatus der Netzwerk-Clients zu erkennen. Die Spalte G DATA SECURITY STATUS enthält einen unverzichtbaren Überblick

in Zahlen. Wird in einem der verwalteten Systeme kein G DATA Security Client ausgeführt, zeigt die Spalte diesen Client an. Ebenso werden Clients mit veralteten Virensignaturen aufgeführt, damit der Administrator sie umgehend aktualisiert. Wurden wichtige Sicherheitskomponenten deaktiviert, können sie direkt wieder aktiviert werden.

Auf Computern mit dem G DATA Security Client zeigt die Übersicht CLIENT-VERBINDUNGEN den letzten Verbindungszeitpunkt. Durch die aufmerksame Beobachtung des Diagramms CLIENT-VERBINDUNGEN behält der Administrator einen Überblick darüber, wann die Computer zuletzt mit dem ManagementServer verbunden waren, und kann so potenzielle Server- und Netzwerkprobleme erkennen. Computer, die sich nicht regelmäßig mit dem ManagementServer verbinden, erhalten keine Virensignatur-Updates und können keine Aufgaben und andere Einstellungen synchronisieren. Laptops oder andere mobile Geräte verbinden sich, beispielsweise auf Dienstreise, manchmal über einen längeren Zeitraum nicht mit dem Server, während normale Desktop-Clients dies häufiger tun. Stellt also eine erhebliche Anzahl von Clients für mehr als drei oder sieben Tage keine Verbindung zum ManagementServer her, kann dies ein Hinweis auf Server- und Netzwerkprobleme sein. Ist ein Computer mit dem Netzwerk verbunden und eingeschaltet, verbindet sich aber dennoch nicht mit dem ManagementServer, müssen die Verbindung zwischen Client und ManagementServer (siehe Abschnitt 4.9) sowie der Netzwerkschutz und die Portkonfiguration (siehe Abschnitt 4.4) untersucht werden.

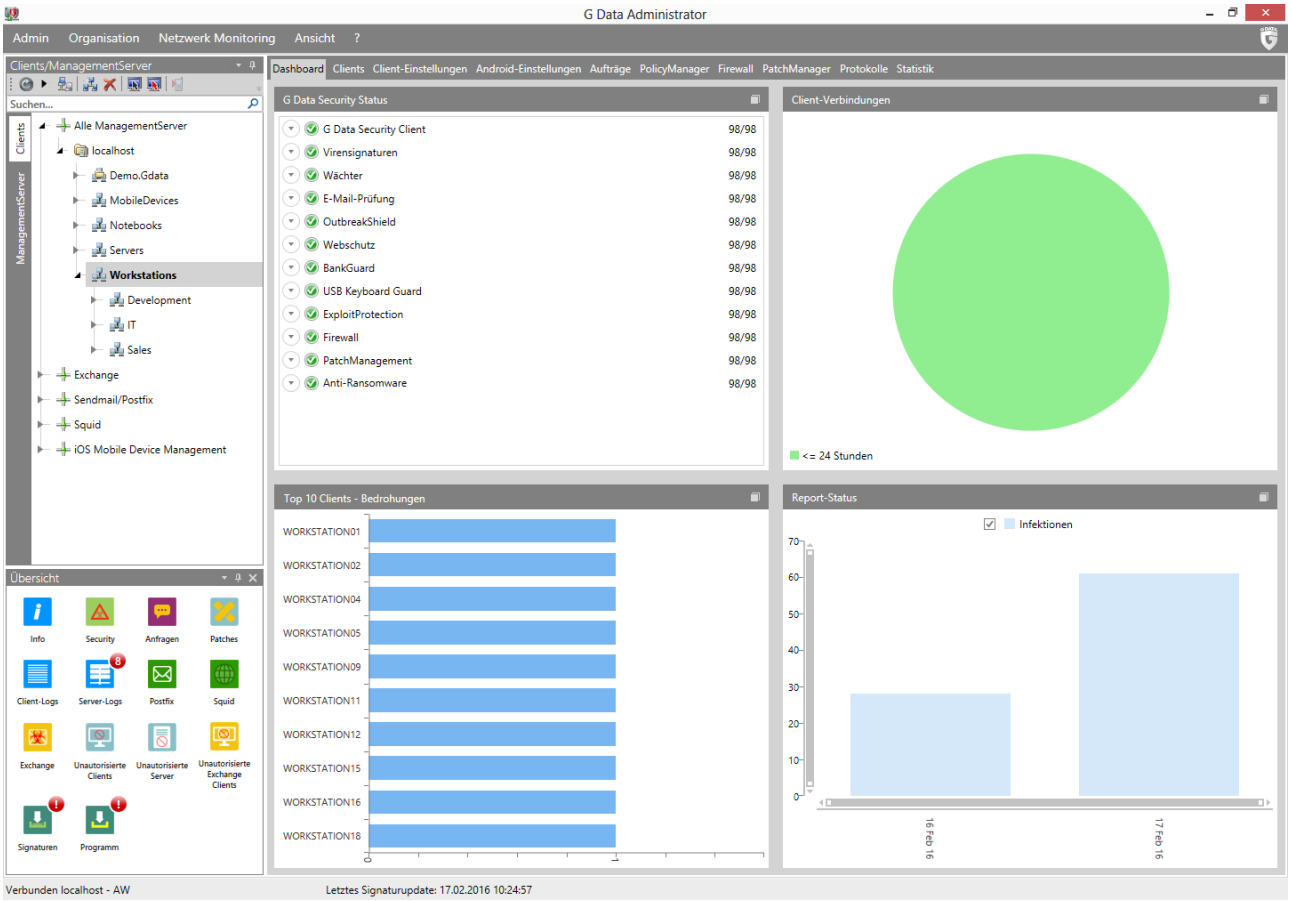

Abbildung 24: G DATA Administrator – Dashboard

Die Übersicht TOP 10 CLIENTS – BEDROHUNGEN hilft beim Auffinden problematischer Clients. Das Tortendiagramm zeigt die Clients mit den meisten Virenberichten. G DATA wehrt diese Infektionen zwar erfolgreich ab, doch die Tatsache, dass bestimmte Clients oft von Malware angegriffen werden, kann auf

Probleme hinweisen. Eventuell ist einer der anderen Schutzmechanismen falsch konfiguriert oder der Endbenutzer ist aufgrund von gezielten Malware-Angriffen oder unvorsichtigem (Surf-)Verhalten besonders gefährdet. Hier sollte die Sicherheitskonfiguration des Clients überprüft werden. Ist das (Fehl-)Verhalten des Endbenutzers eine mögliche Ursache, lässt sich mit den PolicyManager-Richtlinien der Zugriff auf dubiose Ressourcen einschränken (siehe Kapitel 14). Das Tortendiagramm zeigt standardmäßig nur die abgewehrten Infektionen der letzten beiden Wochen an. Durch Klicken auf das Kalendersymbol oben rechts kann der Zeitraum auf die letzten Tage, Wochen oder Monate festgelegt oder manuell ein Zeitraum eingestellt werden.

REPORT-STATUS zeigt eine Übersicht der Berichte (verfügbar im Modul SICHERHEITSEREIGNISSE) an. Das Diagramm zeigt Infektionen, Fehler sowie Firewall- und PolicyManager-Anfragen. Übermäßige Fehler von einem der Module oder andere nennenswerte Spitzen im Diagramm können über die einzelnen Berichte im Modul SICHERHEITSEREIGNISSE geprüft werden. Wie das Diagramm TOP 10 CLIENTS – BEDROHUNGEN kann auch der REPORT-STATUS so konfiguriert werden, dass Informationen nur für einen bestimmten Zeitraum angezeigt werden.

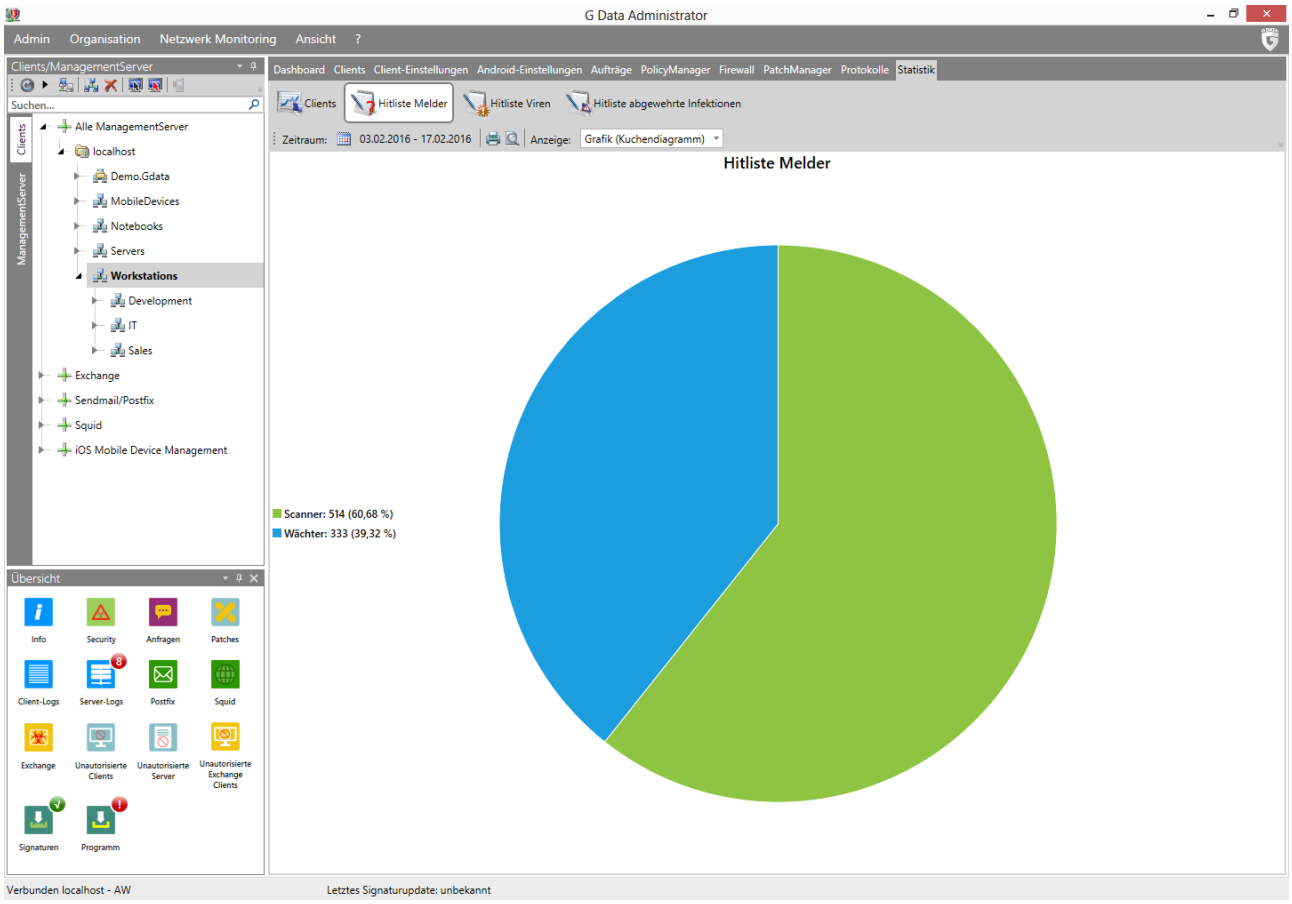

Abbildung 25: G DATA Administrator – Statistik

Neben dem Dashboard bietet die Registerkarte Statistik ausführlichere Informationen, die in verschiedene Bereiche gruppiert sind und den Schutzstatus des Netzwerks anzeigen. Der Bereich CLIENTS umfasst die Anzahl der Clients, auf denen der Wächter, OutbreakShield und der E-Mail-Schutz aktiviert sind, sowie den Engine-Status, die Einstellungen und vieles mehr. Der Bereich CLIENTS kann so konfiguriert werden, dass bis zu acht verschiedene Statistiken angezeigt werden, entweder in einer Tabelle (Text), in einem Balkendiagramm oder in einem Tortendiagramm. Die HITLISTE MELDER enthält die Systemkomponenten,

die Malware erkannt haben, und weitere Angaben zu potenziellen Malware-Angriffsvektoren bzw. Schutzkomponenten, die nicht die erwartete Leistung bringen oder falsch konfiguriert sind. Im Bereich HITLISTE VIREN wird die am häufigsten erkannte Malware angezeigt. Diese Informationen unterstützen auch die Angriffsanalyse. In der HITLISTE ABGEWEHRTE INFEKTIONEN schließlich finden sich die Clients, die am häufigsten von Malware angegriffen wurden. Fallen einer oder mehrere Clients besonders auf, sollte dies weiter untersucht und der Client aktiv geschützt werden, da dies auf einen (halb-)gezielten Angriff oder Nachlässigkeit des Endbenutzers hinweist. Über die Funktion DRUCKEN kann die Statistik beispielsweise für externe Berichte ausgedruckt werden.

6.2. Berichte und Alarmmeldungen

Die Registerkarte PROTOKOLLE > SICHERHEITSEREIGNISSE enthält Berichte (Benachrichtigungen) von allen Sicherheitsmodulen. Obwohl Bedrohungen voll automatisch blockiert werden, müssen die Berichte mitverfolgt werden. Sie enthalten detaillierte Informationen über den Status der Netzwerk-Clients, potenzielle Probleme und andere Module. Beim Modul POLICYMANAGER oder PATCHMANAGER muss in den Berichten beispielsweise auf Anfragen zu Richtlinienänderungen, Patch-Installationen und Rollbacks geachtet werden. Da unter Umständen enorme Mengen an Berichten generiert werden, muss der Administrator die für ihn relevanten Berichte herausfiltern.

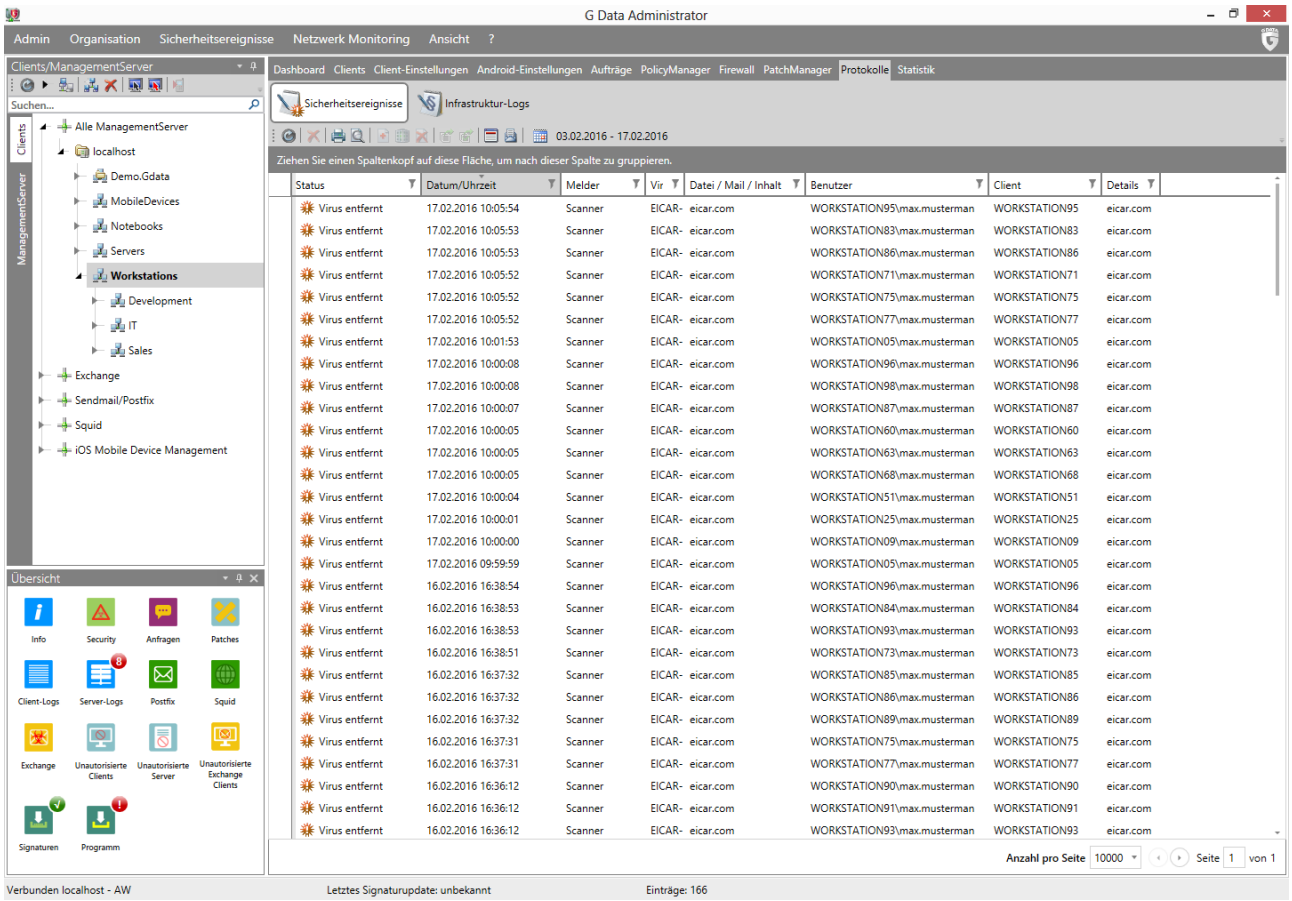

Abbildung 26: G DATA Administrator – Sicherheitsereignisse

Berichte werden von den verschiedenen Modulen der G DATA Sicherheitslösung generiert. Standardmäßig werden alle Berichte in einer Liste in umgekehrter zeitlicher Reihenfolge (neuester

zuerst) aufgeführt. Je nach Anzahl der Clients kann diese Liste sehr lang werden. Über das Steuerelement am Seitenende wird die Anzahl der pro Seite angezeigten Elemente eingestellt. Mit der Gruppenleiste über den Spaltenkopfzeilen können die Berichte spaltenweise gruppiert werden. Wird beispielsweise die Spalte MELDER in die Gruppenleiste gezogen, werden die Berichte nach dem Modul gruppiert, das sie gemeldet hat. Das Modul SICHERHEITSEREIGNISSE bietet noch viele weitere Möglichkeiten zum Filtern der Liste. Mithilfe der Symbolleiste können verschiedene Berichtarten ausgeblendet werden, wie z. B. solche, die von anderen Berichten auf der Liste abhängen (zur Verhinderung von Duplikaten) oder bereits gelesen wurden. Außerdem lassen sich Berichte für spezifische Kategorien anzeigen, wie z. B. noch nicht entfernte Viren, Quarantäneinhalte oder BankGuard-Berichte. Mit dem ZEITFENSTER kann der Administrator die Anzahl der angezeigten Berichte auf einen bestimmten Zeitraum begrenzen.

Die meisten dieser Berichte befassen sich mit bereits blockierter Malware, sind aber dennoch sehr wichtig, da sie Einblick in den Netzwerkstatus und die angegriffenen Computer bieten. Auch können false positive Ergebnisse erkannt und zu einer Ausnahmeliste hinzugefügt werden. Wächter- und Scanner-Berichte enthalten die Aktion, die beim Virenfund ergriffen wurde, wie z. B. Virenentfernung, Quarantäne oder Löschung der Datei. Über die entsprechende Schaltfläche können in Quarantäne verschobene Dateien bei false positive Erkennung zurück verschoben oder direkt über die Registerkarte SICHERHEITSEREIGNISSE und Klick auf die jeweilige Symbolleistenschaltfläche bereinigt werden. Das kann riskant sein, denn falls die Datei nicht vollständig bereinigt wurde, bleibt sie infektiös und kann das Client-System weiter schädigen. Außerdem kann im Modul SICHERHEITSEREIGNISSE direkt eine Ausnahme definiert werden. Wurde eine Datei fälschlich als Malware erkannt, kann im Kontextmenü die Option ALS WÄCHTERAUSNAHME DEFINIEREN ausgewählt werden, um die Datei für Wächter-Scans als sicher zu markieren. Auch Clients, auf denen das Modul „Firewall“ installiert ist, erstellen Berichte, beispielsweise wenn eine Anwendung freigegeben werden soll. In diesen Berichten können mit der Option EIGENSCHAFTEN direkt Firewall-Regeln angepasst werden, um die Anwendung zuzulassen.

Zusätzlich zu den Sicherheitsberichten generieren auch einige unterstützende Module einen Bericht. Das PolicyManager-Modul protokolliert Webinhalte, Anwendungen und Geräte, die aufgrund von Richtlinieneinstellungen blockiert wurden und auf die der Benutzer zugreifen möchte. In den Berichtseigenschaften kann dieser Zugriff über die entsprechende Whitelist oder Blacklist hinzugefügt werden. Auch die Berichte des PatchManager enthalten Benutzeranfragen, beispielsweise zur Patch-Verteilung oder zum Rollback. Die Komponente „Internet Security für Android“ erstellt für das Modul einen Bericht, wenn ein Endbenutzer auf eine Telefonnummer auf der Blacklist zugreifen möchte.

Berichte können automatisch gelöscht werden. In der Registerkarte BEREINIGUNG des Moduls ALLGEMEINE EINSTELLUNGEN kann der Administrator automatisch Berichte löschen, die älter als eine bestimmte Anzahl von Monaten sind. Dadurch kann die Anzahl der Berichte zwar drastisch verringert werden, es werden unter Umständen aber auch wichtige Benachrichtigungen entfernt, die noch nicht gelesen wurden. Berichte sollten nur dann automatisch gelöscht werden, wenn sie regelmäßig gelesen (oder per E-Mail verteilt) werden.

Die Alarmmeldungen unter ALLGEMEINE EINSTELLUNGEN > E-MAIL sollten auf jeden Fall konfiguriert werden. Mit dieser Einstellung kann der Administrator wichtige Berichte, beispielsweise zu Virenfunden, veralteten Clients, Firewall-Aktionen und PolicyManager-Anfragen, direkt an seine E-Mail-Adresse senden lassen. Auch wenn nicht jedes Virenereignis kritisch ist, so sind Alarmmeldungen ein entscheidendes Hilfsmittel, um über die Vorgänge im Netzwerk auf dem Laufenden zu bleiben. Alarmmeldungen benachrichtigen

den Administrator oder das Bereitschaftsteam bei Notfällen und helfen Benutzern, die keinen Zugriff auf den G DATA Administrator haben oder sich nicht oft anmelden. In der Registerkarte ALLGEMEINE EINSTELLUNGEN > E-MAIL wird konfiguriert, wer welche Berichte erhält. Hier kann eine Empfängergruppe mit der E-Mail-Adresse des Administrators und des IT-Personals (und eventuell weitere) für den Notfallschutz festgelegt werden[8]. Standardmäßig werden nur veraltete Virensignaturen sowie Probleme mit Virensignaturdatenbanken und Programmdateien von Clients gemeldet. Auf diese Benachrichtigungen muss normalerweise (fast) sofort reagiert werden, da die Client-Sicherheit direkt betroffen ist. Berichte zu Virenerkennungen und durch die Firewall blockierte Anwendungen dienen zur Information, können jedoch aktiviert werden, um einen umfassenderen Überblick zu erhalten. Im PolicyManager-Modul kann durch die Aktivierung von Benachrichtigungen bei FREIGABE ANFRAGEN eine E-Mail aktiviert werden, wenn Benutzer Anfragen über den PolicyManager stellen (um beispielsweise bestimmte Websites oder Anwendungen zur Whitelist hinzuzufügen).

6.3. ReportManager

Mit dem ReportManager können Berichte von verschiedenen Informationsmodulen zusammengestellt werden. Er kann umfassend angepasst werden und bietet einen fundierten Einblick in den Netzwerk- und Sicherheitsstatus. Der ReportManager kann als proaktives Gegenstück zu E-Mail-Benachrichtigungen angesehen werden. Wurden E-Mail-Benachrichtigungen für Ereignisse wie Virenalarme und PolicyManager-Anfragen konfiguriert, kann der Administrator schnell darauf reagieren. Auf der anderen Seite bietet der ReportManager analytische Informationen und ermöglicht die Vorausplanung. Als Ergänzung zur regelmäßigen Anmeldung beim G DATA Administrator sollten periodische E-Mail-Berichte in den täglichen Administrationsablauf integriert werden.

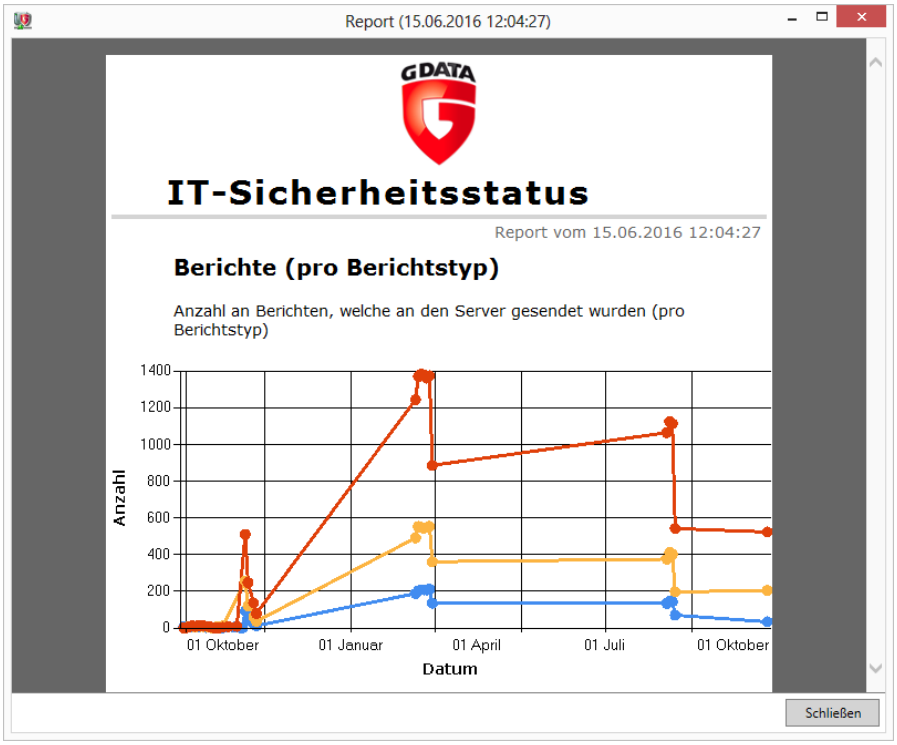

Abbildung 27: G DATA Administrator – Bericht vom ReportManager

[8] Die E-Mail-Empfängergruppen und ein SMTP-Server müssen im Fenster „E-Mail-Einstellungen“ eingegeben werden. Siehe Abschnitt 4.5.

Der ReportManager ermöglicht die Erstellung von Berichten mit Informationen von verschiedenen Teilen der G DATA Sicherheitslösung. Zusätzlich können Diagramme in Berichte integriert werden, um die Angaben auf bestimmte Zielgruppen abzustimmen. Ein Bericht für leitende Mitarbeiter enthält z. B. allgemeine statistische Angaben über die Anzahl der geschützten Clients, die aktuellen Software-Versionen und den Patch-Status. Technische und administrative Berichte wiederum benötigen ausführliche Statistiken zu Netzwerk-Clients und abgewehrten Vireninfektionen.

Wie Scan- und Backup-Aufträge kann auch die Berichterstellung vom ReportManager geplant werden. Für einen neu definierten Bericht lässt sich festlegen, dass er einmal, täglich, wöchentlich, monatlich, vierteljährlich, halbjährlich oder jährlich erstellt wird. Auch wenn bereits Einmalberichte einen sehr guten Einblick in bestimmte Komponenten des G DATA Schutzes ermöglichen, liegt die wahre Stärke vom ReportManager darin, Statusberichte automatisch über einen längeren Zeitraum zu erstellen. Die Berichte bieten auswertbare Informationen, damit der Administrator bezüglich des Netzwerks immer auf dem neuesten Stand ist, können aber auch gespeichert werden, um später externe Berichte zu generieren.

Berichte sollten regelmäßig per E-Mail an die relevanten Mitarbeiter gesendet werden. Mit E-Mail-Empfängergruppen kann die Berichtzustellung koordiniert werden (siehe Alarmmeldungen im Abschnitt 6.2). Die Auswahl der Module hängt von der Zielgruppe und vom Informationsbedarf ab. Die Kategorien CLIENT-ALLGEMEIN und CLIENT-SCHUTZ enthalten eine Vielzahl von Diagrammen mit präzisen und konkreten Angaben. Als Quelle für auswertbare Informationen sollten mindestens zwei Arten von täglichen Berichten erstellt werden: eine Version für leitende Mitarbeiter mit allgemeinen Informationen und ein ausführlicher technischer Statusbericht für Administratoren. Soll der Netzwerkschutz mithilfe von Berichten über einen längeren Zeitraum erfasst werden, kann ein wöchentlicher oder monatlicher Bericht definiert werden. Dabei müssen keine E-Mail-Empfänger festgelegt werden, wenn Berichte vorzugsweise im G DATA Administrator gelesen werden. Die zusätzliche Kategorie PATCHMANAGER im PatchManager-Modul enthält verschiedene Diagramme, um den Patchstatus anzuzeigen. Das ist insbesondere bei der Patchverwaltung hilfreich (siehe Kapitel 15).

Allerdings sind tägliche oder wöchentliche Berichte kein Ersatz für regelmäßige Überprüfungen wie z. B. die Überprüfung der Abschnitte DASHBOARD und SICHERHEITSEREIGNISSE.

7. Verwalten von Clients

Funktionierende Netzwerksicherheit basiert auf der richtigen Client-Verwaltung. Aktive Netzwerk-Clients zu überwachen und in relevante Gruppen zu organisieren, senkt die Wahrscheinlichkeit von Komplikationen bei Softwareinstallationen und Konfigurationsänderungen. Im Idealfall wurde das Layout jedes Unternehmensnetzwerks im Voraus gemäß logischen Strukturen definiert (siehe Kapitel 1). Diese Strukturen können in der G DATA Sicherheitslösung abgebildet werden, um die Clients effizienter zu verwalten. Client-Gruppen dienen als logische, gemeinsam verwaltete Einheiten, für die Sicherheitseinstellungen, Backup-Aufträge, Richtlinien und viele weitere Optionen definiert werden. Mit Active Directory können Einheiten automatisch importiert werden, um die Gruppen schneller zu konfigurieren. Große Netzwerke, in denen Active Directory bereits installiert wurde, sollten AD-Einheiten in die G DATA Administrator-Gruppen integrieren. Dies beschleunigt die Reorganisation von Gruppen und die Sicherheitskonfiguration neu installierter Clients.

7.1. Verwenden von Gruppen

Die Ansicht CLIENTS vom G DATA Administrator bietet Tools zur Gruppierung von Clients. Gruppen können manuell oder automatisch in einem vorhandenen Active Directory erstellt und bestückt werden (siehe Abschnitt 7.2). Gruppen sind mit einer Ordnerstruktur vergleichbar. Die Strukturen lassen sich in kurzer Zeit vervollständigen, da Clients beliebig zwischen Gruppen verschiebbar sind. Dennoch ist ein wenig Vorausplanung nötig. Das Gruppieren von Clients geschieht aus unterschiedlichen Gründen. Computer für ähnliche Tätigkeiten (z. B. Entwicklung, Back Office, Vertrieb) besitzen auch ähnliche Software, so dass ihnen als Gruppe dieselben Software-Nutzungsrichtlinien zugewiesen werden können. Der PatchManager kann eine mit ähnlicher Software bestückte Gruppe schnell testen, indem Patches auf einem speziellen Test-Client installiert werden. Eine zweite Möglichkeit, die sich zum Teil mit der aufgaben- und softwarebasierten Gruppierung überschneidet, ist die räumliche Gruppierung. Räumliche nahe Client-Computer können zusammengefasst werden. Dies entspricht oftmals einer Niederlassung oder Abteilung (hier kommt es dann zu Überschneidungen mit der aufgabenbasierten Gruppierung). Die standortbasierte Gruppierung hat den Vorteil, dass Wartungs- und Konfigurationsänderungen mit physischem Zugriff auf die Computer einfacher planbar sind. Viele dieser Überlegungen entsprechen den Fragen, die auch bei der Definition und Einrichtung des lokalen Netzwerks gestellt werden müssen. Eine einfache Lösung ist die Spiegelung des Netzwerk-Layouts (siehe Abschnitt 1.1).

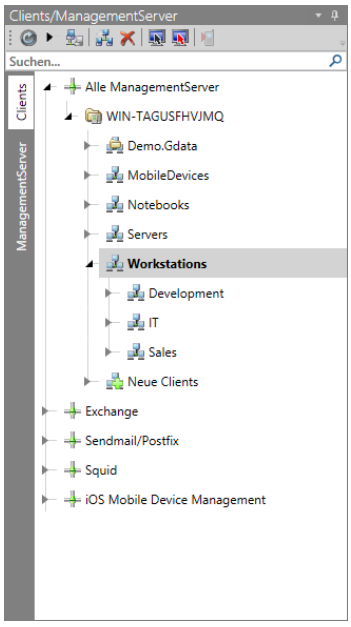

Abbildung 28:
G DATA Administrator – Clients

Das Arbeiten mit Gruppen bietet verschiedene Vorteile. Ganz elementar können Einstellungen gleichzeitig auf mehrere Clients angewendet werden. Dazu werden Gruppen in der Ansicht CLIENTS ausgewählt und ihre Einstellungen bearbeitet (z. B. die Schutzeinstellungen im Modul CLIENT-EINSTELLUNGEN). Mit der Option ÜBERNEHMEN werden die ausgewählten Einstellungen auf alle Clients in der Gruppe angewendet. Alternativ können die Einstellungen von einem Client einfach mit der Option AKTUELLE CLIENTEINSTELLUNGEN FÜR GESAMTE GRUPPE ÜBERNEHMEN auf die gesamte

Gruppe übertragen werden. Dadurch können verschiedene Einstellungen auf einem Client ausprobiert und anschließend als bewährte Konfiguration auf den Rest der Gruppe angewandt werden.

Bei Auswahl einer Gruppe in der Ansicht CLIENTS haben möglicherweise nicht alle Clients dieselben Einstellungen. Clients mit Einstellungen, die nicht den Gruppeneinstellungen entsprechen, sind am Ende des Modulbereichs unter CLIENTS/GRUPPEN MIT ABWEICHENDEN EINSTELLUNGEN aufgeführt. Sie können umgehend auf die Gruppeneinstellungen zurückgesetzt oder im Bereich CLIENTS ausgewählt werden, damit sich der Administrator die Konfiguration dieses spezifischen Clients ansehen kann.

Mit Gruppen lassen sich Clients deutlich einfacher auswählen. Durch Auswahl der entsprechenden Gruppe werden Patch-Verteilung oder die Planung der stufenweisen Update-Verteilung beschleunigt. Jede Gruppe benötigt einen aussagekräftigen Namen entsprechend physischem Standort, Aufgabentyp, Abteilung oder logischer Systemeinheit. Darüber hinaus lassen sich Einstellungen unkompliziert exportieren und importieren. Die PolicyManager- und Client-Einstellungsmodule werden durch Auswahl eines Clients über die Kontextmenüoption EINSTELLUNGEN EXPORTIEREN in eine .dbdat-Datei exportiert. Mit EINSTELLUNGEN IMPORTIEREN können Einstellungen aus einer .dbdat-Datei selektiv in einen Client oder eine Gruppe zurückimportiert werden.

Lokal installierte Clients verbinden sich automatisch mit dem ManagementServer. Da sie noch keiner Gruppe angehören, werden alle derartigen Clients der Gruppe NEUE CLIENTS hinzugefügt. Über die Baumstruktur des G DATA Administrators können sie manuell verschoben werden. Der Vorgang ist aber auch automatisierbar, um insbesondere in Netzwerken mit regelmäßig lokal installierten Clients Zeit zu sparen. Mit dem REGELASSISTENTEN können Regeln auf Basis von Computername, IP-Adresse, Domäne oder Standard-Gateway erstellt werden. Die Liste der Clients wird regelmäßig überprüft. Clients, die einer Regel entsprechen, werden in eine vordefinierte Gruppe verschoben. Es wird empfohlen, den Assistenten so zu konfigurieren, dass die Regeln nur für Clients der Gruppe NEUE CLIENTS übernommen werden, obwohl sie natürlich auch auf alle Clients angewendet werden können.

7.2. Integrieren von Active Directory

Active Directory ist ein Verzeichnisdienst für Windows-Netzwerke. In einem Netzwerk befindliche Active Directory-Server enthalten Informationen über Einheiten innerhalb des Netzwerks, wie z. B. Benutzer, Computer und Ressourcen. Active Directory (AD) erleichtert die Organisation eines Netzwerks, die Authentifizierung von Benutzern und die Koordination des Ressourcenzugriffs. Die Netzwerkstruktur in AD muss zur Installation und Nutzung einer Sicherheitslösung von G DATA nicht erneut eingerichtet werden.

Jeder AD-Container bzw. jede Organisationseinheit kann mit einer Gruppe in der Ansicht CLIENTS verknüpft werden. Alle aktuellen und zukünftigen Computer des Elements werden automatisch zur Übersicht im G DATA Administrator hinzugefügt. Über die Option ACTIVE DIRECTORY EINTRAG DER GRUPPE ZUORDNEN im Kontextmenü der Gruppe kann ihr ein AD-Element zugewiesen werden. Jeder Gruppe kann nur ein AD-Element zugewiesen werden. Im Dialogfenster kann der Administrator Elemente aus der Standarddomäne oder durch Eingabe von Domänencontroller, Domänenname, Benutzername und Kennwort eine weitere Domäne auswählen. Nachdem die AD-Gruppe bestätigt und die Ansicht CLIENTS aktualisiert wurde, erfolgt die Umwandlung der Gruppe in eine mit AD verknüpfte Gruppe. Diese Gruppe enthält alle Computer der AD-Einheit. Der G DATA ManagementServer synchronisiert die AD-Elemente

automatisch alle sechs Stunden mit dem Domänencontroller. Das Zeitintervall kann unter ALLGEMEINE EINSTELLUNGEN > SYNCHRONISATION geändert werden. Außerdem können mit AD verknüpfte Gruppen direkt über das Kontextmenü (Rechtsklick auf die Gruppe oder den übergeordneten ManagementServer) und die Option ACTIVE DIRECTORY AKTUALISIEREN aktualisiert werden.

Durch die zugewiesenen AD-Elemente können Clients schneller manuell zu einer Gruppe hinzugefügt werden. Da neue Clients ihre Konfigurationseinstellungen und andere Richtlinien automatisch von der übergeordneten Gruppe erben, müssen neue Computer nicht sofort konfiguriert werden. Weitere Automatisierungen sind möglich, wenn der G DATA Security Client automatisch auf Computern installiert wird, die der AD-Gruppe neu hinzugefügt wurden. Diese Option kann während der Zuweisung eines AD-Elements zu einer Gruppe im G DATA Administrator aktiviert werden. Sind die Systemvoraussetzungen für eine Installation per Fernzugriff erfüllt (siehe Abschnitt 4.8.2.1), wird der G DATA Security Client automatisch auf jedem neu hinzugefügten Active Directory-Client installiert.

7.3. Signatur- und Programmdatei-Updates

Die signaturbasierten Schutzebenen der G DATA Sicherheitslösung benötigen aktualisierte Virensignaturen, um die neuesten Bedrohungen zu erkennen. Clients können den Update-Vorgang von sich aus starten und beim Server neue Signaturdateien anfragen, oder die Virensignaturen werden automatisch auf die Clients verteilt. Der Netzwerkadministrator kann festlegen, ob die Clients den zentralen G DATA ManagementServer des Netzwerks abfragen oder direkt die von G DATA gehosteten Update-Server kontaktieren. Für Unternehmensnetzwerke wird empfohlen, die Clients so zu konfigurieren, dass sie die Signatur-Updates vom G DATA ManagementServer erhalten. Dies verbessert die Kontrolle, wenn beispielsweise ein Update rückgängig gemacht werden muss, und spart Netzwerkverkehr. Neben Signaturdateien können Clients auch aktualisierte Programmdateien beziehen. Der G DATA Security Client erhält regelmäßig Updates, um seine Schutzleistung weiter zu verbessern. Im Gegensatz zu Virensignaturen können Programmdateien nicht direkt von G DATA gehosteten Update-Servern an die Clients übertragen werden. Zur Entlastung des Servers können aktualisierte Virensignaturen und Programmdateien mit Peer-to-Peer verteilt werden: veraltete Clients erhalten ihre Dateien von bereits aktualisierten Clients.

Automatische Virensignatur- und Programmdatei-Updates für alle Clients werden in zwei Schritten aktiviert: Zunächst muss der ManagementServer die Update-Dateien regelmäßig von den G DATA Update-Servern erhalten. Dabei ist die Konfiguration von automatischen Updates die optimale Lösung. Andernfalls können die Updates durch die manuelle Verbindung mit dem G DATA Update-Server oder offline durchgeführt werden. Im zweiten Schritt müssen die aktualisierten Dateien auf die Clients verteilt werden. Dies sollte ebenfalls automatisiert werden, wobei verschiedene Optimierungseinstellungen verfügbar sind, damit keine Lastspitzen im Netzwerk auftreten.

7.3.1. Erhalt von Updates

Der ManagementServer muss die neuesten Dateien von den G DATA Update-Servern erhalten. Dies kann manuell gestartet oder im Modul UPDATES des G DATA Administrators als regelmäßige Aufgabe eingerichtet werden.

Die empfohlene Einstellung ist die stündliche Anfrage beim Update-Server auf neue Virensignaturen. Programmdatei-Updates werden nicht stündlich herausgegeben, weshalb das Update-Intervall auf eine tägliche oder wöchentliche Anfrage eingestellt werden kann. Die Planung der Virensignatur- und Programmdatei-Updates wird auch für Server empfohlen, die nicht permanent mit dem Internet verbunden sind. Die Option INTERNETVERBINDUNGSAUFBAU führt nur dann ein Update durch, wenn der G DATA ManagementServer erkennt, dass der Server über eine Internetverbindung verfügt. Der einzige Grund, um Signaturen und Programmdateien nicht automatisch vom G DATA ManagementServer aktualisieren zu lassen, ist eine nicht immer verfügbare Internetverbindung. Damit Dateien nicht automatisch auf die Clients verteilt werden, sind entsprechende Konfigurationen im Modul CLIENT-EINSTELLUNGEN erforderlich.

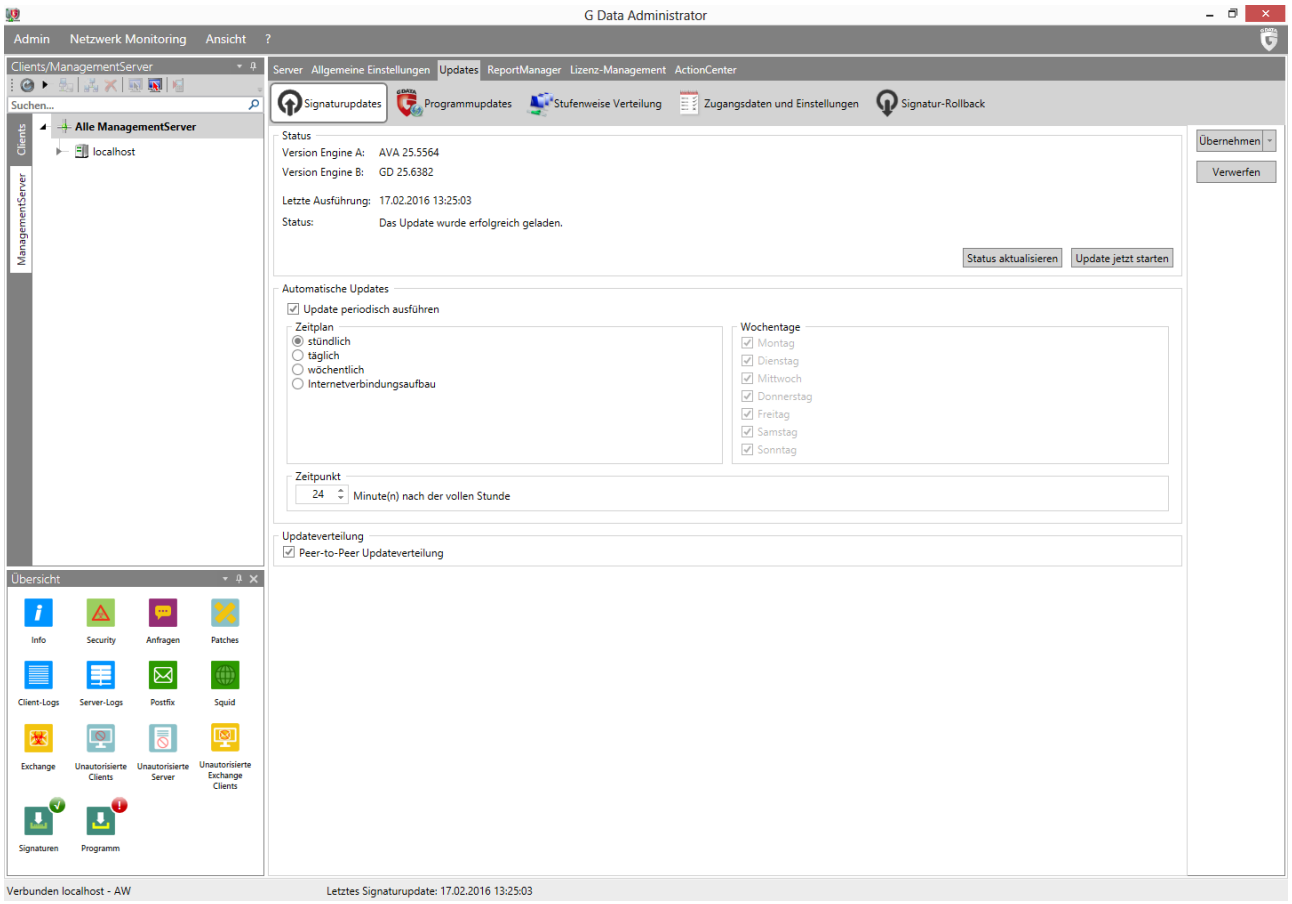

Abbildung 29: G DATA Administrator – Updates, Signaturupdates

Beim ManagementServer kann es praktische oder sicherheitstechnische Gründe geben, warum er nicht immer mit dem Internet verbunden ist. Der ManagementServer kann sich zwar nur mit aktiver Internetverbindung automatisch selbst aktualisieren, kann jedoch über Offline-Updates die neuesten Server- und Client-Programmdateien sowie Virensignaturen erhalten. Das Internet-Update-Tool (siehe Abschnitt 4.6) kann zur Übernahme von Update-Dateien genutzt werden, die ohne Internetverbindung von einem anderen ManagementServer auf den Server kopiert wurden. So können Updates übernommen werden, indem sie auf einen USB-Stick bzw. eine CD oder DVD übertragen werden. Wichtig ist, dass ein ManagementServer mit Internetverbindung entweder über das Internet-Update-Tool oder über den G DATA Administrator die neuesten Updates bezogen hat. Aus dem Ordner „%ProgramData%\G Data\AntiVirus ManagementServer\Updates“ müssen folgende Unterordner auf einen USB-Stick bzw. eine CD oder DVD übertragen werden: bd, Client, GD_SIG und SERVER12. Nach dem

Einlegen der CD/DVD bzw. Anstecken des USB-Sticks im Ziel-ManagementServer werden die Update-Ordner in einen temporären Ordner (z. B. C:\Updates) kopiert. Im Internet-Update-Tool wird dann die Option OFFLINE-UPDATE aktiviert. Dadurch verändert sich das Verhalten der drei Update-Schaltflächen: Beim Start eines Updates der VIRENDATENBANK, der PROGRAMMDATEIEN DES CLIENTS oder der PROGRAMMDATEIEN DES SERVERS wird in einem Popup-Fenster nach einem Ordner gefragt. Nach Auswahl des Ordners mit allen Update-Ordnern (z. B. C:\Updates) wird auf OK geklickt. Zuerst sollten die Server-Programmdateien aktualisiert werden, damit der Server über die neueste Version verfügt. Als Nächstes werden Client-Programmdateien und Virendatenbank auf den neusten Stand gebracht.

7.3.2. Updates installieren

Der zweite Schritt ist die eigentliche Verteilung der Virensignatur- und Programmdatei-Updates auf die Clients. Auf der Registerkarte ALLGEMEIN im Modul CLIENT-EINSTELLUNGEN können Update-Einstellungen für einen oder mehrere Clients konfiguriert werden (durch die Auswahl einer Gruppe von Clients oder des gesamten ManagementServers). Virensignaturen sollten automatisch aktualisiert werden, da die Clients sie benötigen, um neue Bedrohungen zu erkennen. Das Fenster UPDATE-EINSTELLUNGEN bietet verschiedene Optionen zum Herunterladen von Virensignaturen. Clients können sich mit dem zentralen ManagementServer verbinden und von dort die Virensignaturen beziehen. Sie fragen den ManagementServer in dem unter ALLGEMEINE EINSTELLUNGEN > SYNCHRONISATION definierten Intervall auf aktualisierte Virensignaturen an. Bei der zentralen Verwaltung (mit Optionen wie Signatur-Rollbacks) sollten die Clients ihre Virensignaturen vom ManagementServer herunterladen. Alternativ können sie die Virensignaturen von den G DATA Update-Servern herunterladen, entweder immer (INTERNET-UPDATE DER VIRENSIGNATUREN SELBST DURCHFÜHREN) oder nur, wenn keine Verbindung mit dem ManagementServer besteht (INTERNET-UPDATE BEI VERALTETEN VIRENSIGNATUREN SELBST DURCHFÜHREN, WENN KEINE VERBINDUNG ZUM MANAGEMENT-SERVER HERGESTELLT WERDEN KANN). Clients, die sich nur selten mit dem ManagementServer verbinden (wie Laptops außerhalb des Unternehmensnetzwerks), sollten so konfiguriert werden, dass sie die G DATA Update-Server als Ausfallsicherung nutzen. Die Anmeldeinformationen im Fenster EINSTELLUNGEN UND ZEITPLANUNG müssen definiert werden, damit sich die Clients selbstständig mit den G DATA Update-Servern verbinden können. Clients können eigene Zugangsdaten (falls verfügbar) oder die vom ManagementServer verwenden. In diesem Fall müssen die Virensignatur-Updates auf der Registerkarte ZEITPLANUNG SIGNATUR-UPDATE geplant werden. Für Virensignaturen werden stündliche Updates empfohlen. Bei Clients, die nicht immer online sind, kann die Option INTERNETVERBINDUNGSAUFBAU verwendet werden.

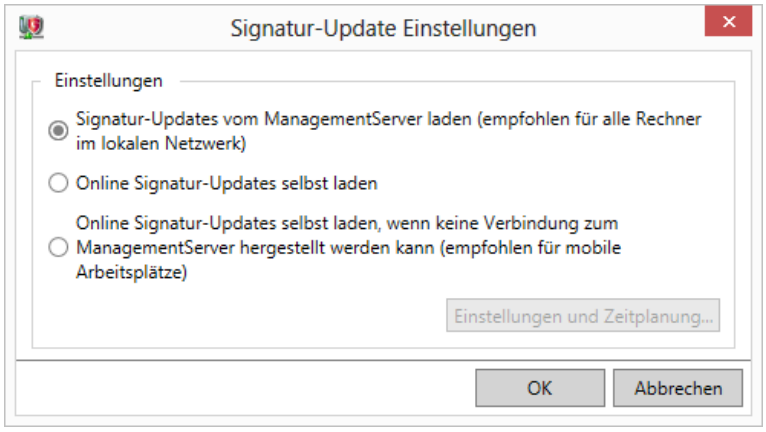

Abbildung 30: G DATA Administrator – Client-Einstellungen, Allgemein, Update-Einstellungen

Auch Programmdatei-Updates lassen sich automatisch installieren, damit die Clients die neuesten Sicherheitsfunktionen der Software nutzen können. Hierbei ist jedoch größere Vorsicht als bei den Signatur-Updates geboten. Aktualisierte Client-Software muss eventuell getestet werden, um die Kompatibilität mit allen Client-Konfigurationen im Netzwerk sicherzustellen. Auch wenn kleine Versionsänderungen normalerweise keine Nebenwirkungen haben, wird ein stufenweises Rollout empfohlen. Die STUFENWEISE VERTEILUNG kann im Modul UPDATES aktiviert werden . Dies leitet eine mathematische Berechnung ein, wobei alle aktiven Netzwerk-Clients in Gruppen aufgeteilt werden (Stufen). Erst wenn die Programmdatei erfolgreich auf den Clients einer Stufe aktualisiert wurde, wird sie auf den Clients der nächsten Stufe installiert. Schlägt die Installation auf zu vielen Clients fehl, wird die Verteilung automatisch angehalten. Die Anzahl der Stufen kann manuell definiert werden. Je größer das Netzwerk, desto mehr Stufen werden empfohlen, um eine reibungslose Installation sicherzustellen. Außerdem kann konfiguriert werden, nach wie vielen Tagen die nächste Stufe aktualisiert wird. Mit dem Standardwert von drei Tagen können Clients auf Probleme geprüft werden, um die Verteilung eines bestimmten Updates anzuhalten, falls schwerwiegende Probleme auftreten. Gegebenenfalls können die Einstellungen der stufenweisen Verteilung durch die Bearbeitung der Konfigurationsdatei „Config.xml“ optimiert werden (siehe Abschnitt 18.2).

Manche Programmdatei-Updates erfordern einen Neustart des Clients. Bei manchen Client-Rollen muss dies sorgfältig geplant werden, damit der Computer nicht während einer wichtigen Aufgabe neu gestartet wird. In diesen Fällen steuert die Einstellung NEUSTART NACH DER AKTUALISIERUNG das Client-Verhalten. Der Endbenutzer kann benachrichtigt werden, dass sein Computer neu gestartet werden muss. Dieser Neustart kann erzwungen werden oder es wird ein Bericht im Abschnitt Sicherheitsereignisse erstellt, damit der Administrator manuell eingreifen und den Computer zu einem späteren Zeitpunkt neu starten kann.

Die Verteilung von Updates erfordert eine ausreichende Netzwerkbandbreite. Der ManagementServer und seine Subnet-Server senden regelmäßig Signatur- und Programmdatei-Updates an alle Clients im Netzwerk. Update-Dateien sind inkrementell und deshalb relativ klein. In Netzwerken mit vielen Clients kann dies dennoch zu Lastspitzen führen. Diese können verhindert werden, wenn die Clients ihre Updates mit Peer-to-Peer erhalten. Die Option kann unter UPDATES > SIGNATURUPDATES aktiviert werden. Nach der Aktivierung verteilt ManagementServer Signatur-Updates auf einige Clients, die sich wiederum gegenseitig aktualisieren. Mit jedem durch den ManagementServer verteilten Update erfahren die Clients auch, welche Computer in ihrer Nähe noch nicht aktualisiert wurden, um die Updates auch dorthin zu verteilen. Das Peer-to-Peer-System kann mit Standardeinstellungen verwendet werden, lässt sich aber auch für bestimmte Netzwerksituationen optimieren (siehe Abschnitt 18.2).

Die Clients können auch ohne automatische Updates aktualisiert werden. Der Administrator kann dem Endbenutzer erlauben, selbst Signatur-Updates zu starten (siehe Abschnitt 7.4). Das kann eine Möglichkeit für Endbenutzer sein, die sich nur selten mit dem Unternehmensnetzwerk verbinden, aber die Kontrolle über den Update-Vorgang behalten möchten. Alternativ kann der Administrator mit dem Modul CLIENTS vom G DATA Administrator die Versionsnummern und Updates kontrollieren, die auf jedem Client installiert wurden. Das Modul CLIENTS zeigt die Version vom G DATA Security Client, Informationen über die neuesten Updates für die Engines A und B sowie den Zeitpunkt an, zu dem die Clients das letzte Mal mit dem Server verbunden waren. Durch die Sortierung bzw. Gruppierung der Client-Liste nach diesen Eigenschaften können veraltete Clients schnell erkannt und manuell aktualisiert werden. Dazu wird im Kontextmenü des Clients die Option VIRENDATENBANK JETZT AKTUALISIEREN oder PROGRAMMDATEIEN JETZT

AKTUALISIEREN ausgewählt. Alternativ zum Modul CLIENTS können Versionsinformationen auch dem DASHBOARD entnommen oder entsprechende E-Mail-Berichte konfiguriert werden (siehe Kapitel 6).

7.3.3. Rollbacks

Gelegentlich können Virensignatur-Updates auf bestimmten Clients Probleme verursachen. Eine generische Virensignatur könnte eine Datei fälschlicherweise als schadhaft erkennen oder eine Signaturdatei könnte beschädigt werden. Die erste Maßnahme ist die Blockierung des spezifischen Virensignatursatzes (Engine-Update), der das Problem verursacht. Mit der Funktion UPDATES > SIGNATUR-ROLLBACK kann das Update blockiert werden. Danach wird es nicht mehr durch den ManagementServer verteilt, und alle Clients, die den ManagementServer kontaktieren, werden über die Blockierung informiert.

Wenn ein Rollback das Problem nicht behebt (z. B. bei einer beschädigten Datei), könnte ein vollständiges Update der Virensignaturen notwendig sein. Normalerweise laden der G DATA ManagementServer und der G DATA Security Client nur partielle (inkrementelle) Virensignatur-Updates herunter, um die Netzwerklast und den Datenverkehr zu verringern. Im Fenster UPDATES enthält die Registerkarte ZUGANGSDATEN UND EINSTELLUNGEN die Option VERSIONSPRÜFUNG. Sie ist standardmäßig aktiviert, wodurch der G DATA ManagementServer Updates nur anhand der Versionsnummer vergleicht. Wird die Option deaktiviert und ein Virendatenbank- bzw. Programmdatei-Update erzwungen, überprüft der ManagementServer die Integrität aller Update-Dateien und lädt sie gegebenenfalls erneut herunter. Mit dem Modul CLIENT-EINSTELLUNGEN kann die VERSIONSPRÜFUNG für betroffene Clients nachträglich deaktiviert werden. Dazu dient die Option UPDATE-EINSTELLUNGEN auf der Registerkarte ALLGEMEIN. Daraufhin wird für das Update dieser Clients ein vollständiger Satz Signaturen bzw. Programmdateien installiert.

7.4. Sicherheitsberechtigungen für Endbenutzer

Sicherheitseinstellungen werden zentral durch den Administrator verwaltet. Manchmal ist es jedoch hilfreich, dass der Endbenutzer einen Virenscan startet oder Einstellungen ändert. Es kann auch sein, dass der Administrator als Reaktion auf einen Support-Fall auf lokale Sicherheitseinstellungen zugreifen muss. Auf der Registerkarte ALLGEMEIN im Modul CLIENT-EINSTELLUNGEN können über die Infobereichssymbole vom G DATA Security Client verschiedene Berechtigungen erteilt werden. Diese Optionen können mit einem Kennwort geschützt werden, damit nur gewisse Endbenutzer des Computers oder nur der Administrator Einstellungen ändern dürfen.

Dürfen die Endbenutzer Dateien oder Ordner manuell auf Malware prüfen, kann dies die Anzahl der Support-Anrufe bei einer möglichen Malware-Infektion verringern. Durch Aktivierung der Option DER BENUTZER DARF SELBST VIRENPRÜFUNGEN DURCHFÜHREN kann ungeachtet des serverseitigen Scanzeitplans ein manueller Virenscan gestartet werden. Weitere Informationen über lokale Scans finden Sie in Abschnitt 9.4. Wurde die Option DER BENUTZER DARF SELBST SIGNATURUPDATES LADEN aktiviert, darf der Endbenutzer die lokalen Virensignaturen unabhängig vom Update-Zeitplan aktualisieren. Das kann für Endbenutzer hilfreich sein, die ihr Gerät (z. B. Laptops) regelmäßig nutzen, ohne mit dem Unternehmensnetzwerk verbunden zu sein. Andererseits kann dies die Anzahl der im Netzwerk kursierenden Signaturdateiversionen erhöhen, was wiederum die Client-Verwaltung und Fehlerhebung erschwert.

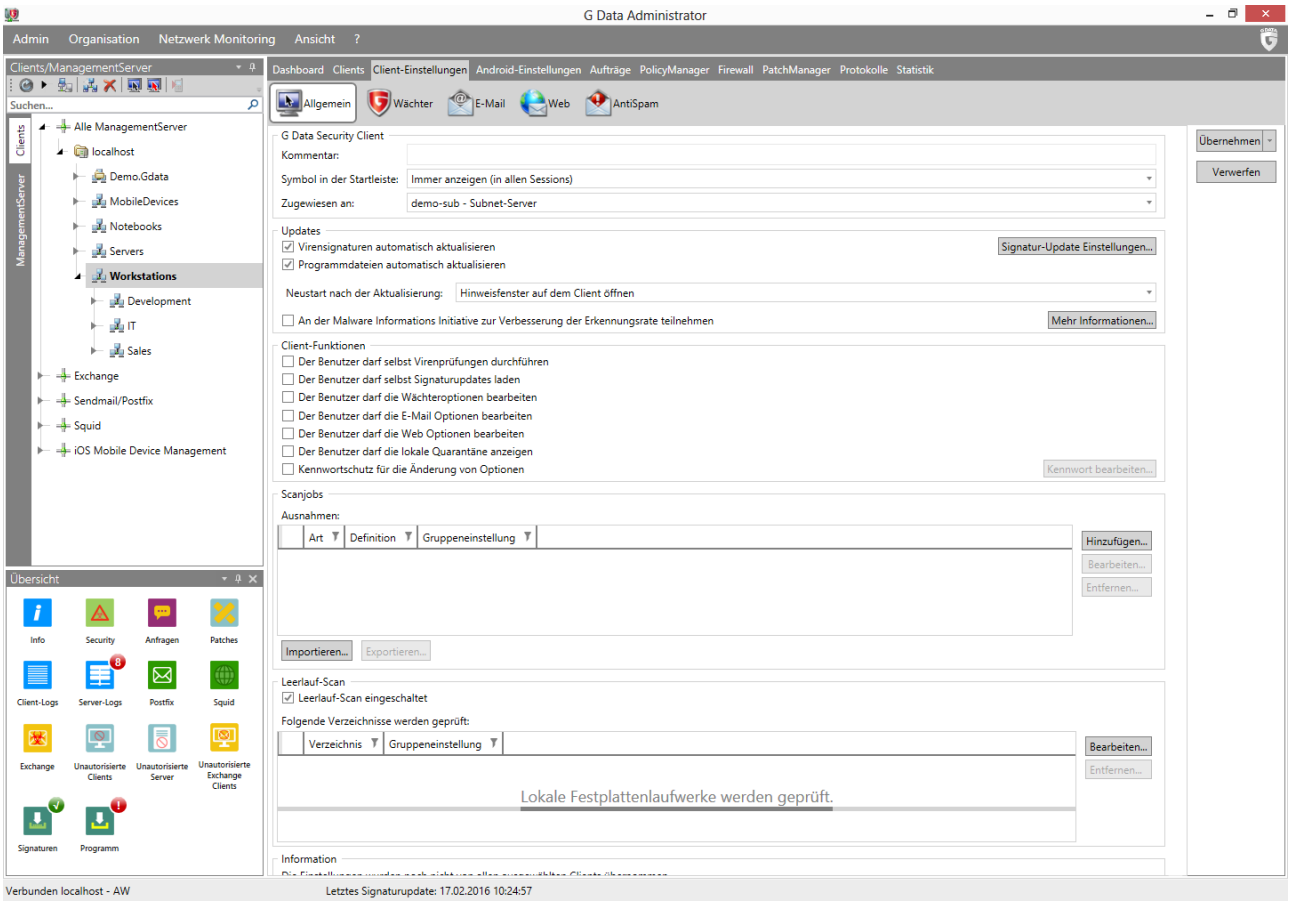

Abbildung 31: G DATA Administrator – Client-Einstellungen, Allgemein

Dem Endbenutzer können alle Sicherheitsoptionen für den Dateisystemwächter, den E-Mail-Scan und den Web-Scan zugänglich gemacht werden. Diese Möglichkeit sollte jedoch mit Bedacht genutzt werden. Dürfen die Endbenutzer keine Sicherheitseinstellungen ändern, kann eine einheitliche Sicherheitsrichtlinie beibehalten werden. Alle Änderungen sollten durch den Administrator autorisiert und zuvor getestet werden. Durch die Aktivierung einer der entsprechenden Optionen kann der Endbenutzer alle Sicherheitsmaßnahmen außer Kraft setzen. Daher sollte diese Option nur verwendet werden, wenn lokaler Zugriff auf die Clients zu administrativen Zwecken erforderlich ist und ein Kennwort eingestellt wurde.

Der G DATA Security Client ermöglicht Zugriff auf die lokale Quarantäne. Wurden Regeln für die Verschiebung von infizierten Dateien in Quarantäne definiert, kann sich der Endbenutzer die isolierten Dateien ansehen. Für jede infizierte Datei werden Datum und Uhrzeit der Erkennung, vollständiger Datei- und Ordnerpfad sowie Name des Virus aufgeführt. Dateien können manuell desinfiziert, gelöscht und zurück verschoben werden. Die letzte Option ist der Grund, warum der lokale Zugriff auf die Quarantäne nur erfahrenen Benutzern oder Administratoren gewährt werden sollte. Dateien, die ohne Desinfektion zurück verschoben werden, stellen ein Risiko für das System dar.

Im PatchManager-Modul kann entschieden werden, ob der Endbenutzer installierte Patches oder verfügbare, aber noch nicht installierte Patches anzeigen darf. Diese Option stellt kein Sicherheitsrisiko dar. Sie kann bei Problemen nach einer Patch-Installation nützlich sein, falls der Endbenutzer eine Rollback-Anfrage stellen möchte oder ein Patch priorisiert werden soll, um ein Kompatibilitätsproblem zu beheben. Weitere Informationen finden Sie in Kapitel 15.

Ist die Firewall aktiviert, kann Benutzern die Aktivierung oder Deaktivierung der Firewall und die Änderung der dezentralen Konfiguration erlaubt werden. Dies wird jedoch nur empfohlen, wenn es auf Netzwerkebene eine strikte Sicherheitslösung gibt. Das Ändern der standortfremden Konfiguration ist für Clients hilfreich, die sich oft mit Netzwerken außerhalb des Unternehmens verbinden. Dadurch lassen sich Regeln und Regelgruppen für diese Netzwerke erstellen, die bei Verbindung mit dem Unternehmensnetzwerk automatisch außer Kraft gesetzt werden. Weitere Informationen über Regelgruppen finden Sie in Kapitel 12.

Hinweis: Die Berechtigung zur Änderung von G DATA Security Client-Einstellungen umfasst keine Anwendungs- und Geräteberechtigungen, Webinhaltskontrolle oder Internetnutzungsdauer. Diese Aktionen können über den PolicyManager zugelassen oder abgelehnt werden (siehe Kapitel 14).

7.5. Leistung

Der G DATA ManagementServer kann sehr viele Clients verwalten. Je nach Größe des Netzwerks, Anzahl der konfigurierten Aufträge und Synchronisationseinstellungen kann es bei Ausführung vieler gleichzeitiger Aktionen zu Leistungsengpässen kommen. Abhilfe können hier verschiedene Maßnahmen schaffen, die aber nur bei erheblichen Leistungseinbußen ergriffen werden sollten. Gleichzeitige Client-Aktivitäten sollten nicht von vornherein beschränkt werden, falls die Leistung nicht beeinträchtigt ist.

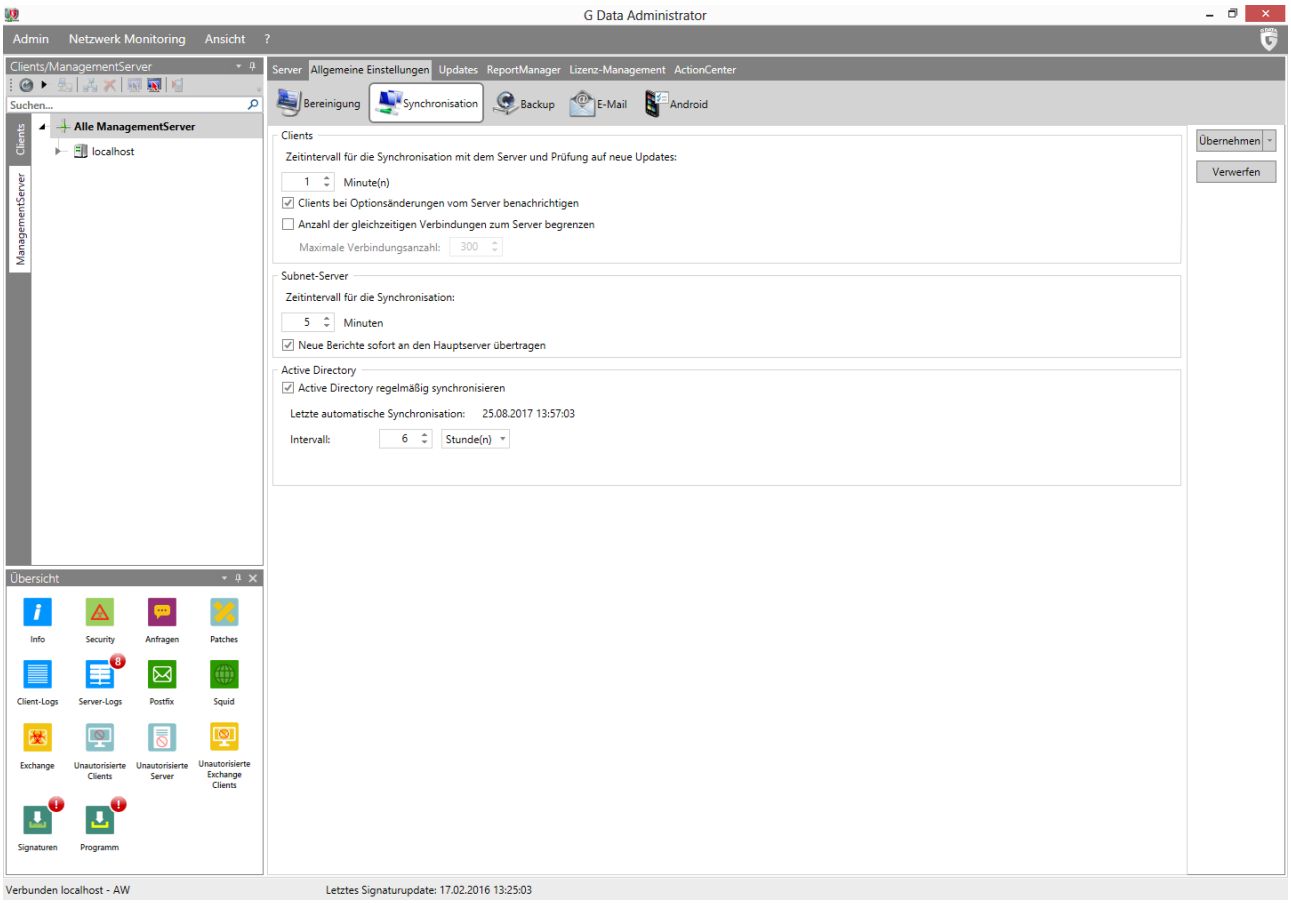

Abbildung 32: G DATA Administrator – Allgemeine Einstellungen, Synchronisierung

Auf der Registerkarte ALLGEMEINE EINSTELLUNGEN > SYNCHRONISIERUNG kann die Anzahl gleichzeitiger Verbindungen mit dem ManagementServer begrenzt werden. Leidet die Leistung wegen zu vieler

gleichzeitiger Client-Verbindungen, können mit der Verbindungsbegrenzung weniger gleichzeitige Verbindungen zugelassen werden. Setzen geplante Aufgaben oder Aufträge die Serverleistung herab, sollte deren Anzahl verringert werden. Eine mögliche Leistungsbeeinträchtigung können Berichte sein, über die Clients ihren Status regelmäßig an den Server melden. Auch die Synchronisationshäufigkeit zwischen Servern, Subnet-Servern und Clients kann reduziert werden; dadurch wird die Leistung in den meisten Fällen jedoch nicht merklich gesteigert.

Eine Alternative zur Verringerung der geplanten Aufgaben oder Client-Verbindungen mit dem ManagementServer ist die Installation eines oder mehrerer Subnet-Server. Zur Entlastung vom ManagementServer verbinden sich die Clients dann nicht mehr mit dem ManagementServer, sondern dem ihnen zugewiesenen Subnet-Server. Weitere Informationen zur Installation von Subnet-Servern finden Sie in Abschnitt 4.10.

7.6. Malware Information Initiative

Die G DATA SecurityLabs erforschen laufend neue Technologien, um Kunden vor Malware (Viren, Würmer, Schadsoftware) zu schützen. Je mehr Informationen verfügbar sind, desto höher die Effizienz dieser Technologien. Viele dieser Informationen finden sich jedoch nur auf Systemen, die angegriffen bzw. infiziert wurden. Damit solche Informationen in die Analysen einfließen können, wurde die G DATA Malware Information Initiative gegründet, in deren Rahmen Malware-bezogene Informationen an die G DATA SecurityLabs gesendet werden. Unter CLIENT-EINSTELLUNGEN > ALLGEMEIN > UPDATES kann ausgewählt werden, ob der Client an der Malware Information Initiative teilnehmen soll oder nicht.

7.7. Verwalten von Linux-/Mac-Clients

Nach der Installation vom G DATA Security Client für Linux/Mac (siehe Abschnitt 4.8.3) werden die Clients automatisch der Ansicht CLIENTS hinzugefügt. Sie werden mit den gleichen Modulen wie ihr Windows-Gegenpart verwaltet. Einige Optionen sind jedoch aufgrund abweichender Funktionalität nicht verfügbar. Wurde ein einzelner Linux-/Mac-Client oder eine Gruppe von Linux-/Mac-Clients in der Ansicht CLIENTS ausgewählt, werden die Nicht-Linux-/Mac-Funktionen ausgegraut. Wurde eine Gruppe mit Windows- und Linux-/Mac-Clients ausgewählt, werden Nicht-Linux-/Mac-Funktionen mit grünem Text angezeigt. Diese Funktionen gelten dann für Windows-Clients, nicht aber für Linux-/Mac-Clients.

7.8. Entfernen eines Clients

Clients mit Kompatibilitätsproblemen oder die nicht mehr durch die G DATA Sicherheitssoftware verwaltet werden sollen, können entfernt werden. Dies geschieht in zwei Phasen: Zuerst wird der G DATA Security Client vom Client entfernt und danach wird der Client aus der Client-Liste vom G DATA ManagementServer gelöscht. Zuerst wird also das Modul CLIENTS im G DATA Administrator geöffnet, der entsprechende Client aktiviert und dann die Option G DATA SECURITY CLIENT DEINSTALLIEREN im Menü CLIENTS ausgeführt. Danach muss entschieden werden, ob nur der Client oder auch die damit verknüpften Aufträge, Berichte, Nachrichten und Backup-Archive entfernt werden sollen. Soll ein Client später wiederhergestellt werden, sollten die verknüpften Daten erhalten bleiben. Bei Clients auf Geräten, die endgültig außer Betrieb genommen werden, können alle Daten entfernt werden. Alternativ zur Remote-Deinstallation kann der Vorgang auch lokal auf dem Client ausgeführt werden (siehe Abschnitt 18.7).

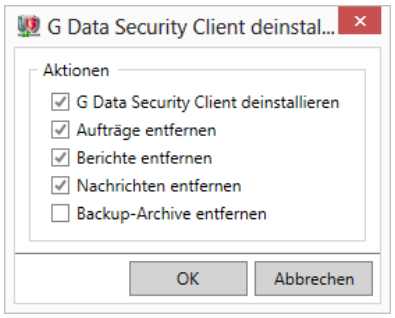

Abbildung 33: G DATA Administrator – Clients, G DATA Security Client deinstallieren

Auch nach der Entfernung vom G DATA Security Client wird der Client-Computer weiterhin in der Ansicht CLIENTS vom G DATA Administrator aufgeführt. Er kann weiter verwaltet werden, obwohl viele Funktionen erst nach einer erneuten Installation vom Security Client wieder verfügbar sind. Per Rechtsklick auf den Client in der Ansicht CLIENTS und Auswahl der Option LÖSCHEN wird er endgültig vom Server entfernt. Nach Bestätigung der Aktion wird der Client aus der Liste entfernt und muss manuell hinzugefügt werden, wenn er erneut verwaltet werden soll.

8. Echtzeitschutz

Client Security ist eine mehrschichtige Lösung, die Malware-Infektionen in unterschiedlichen Phasen abwehrt. Bevor Malware einen Computer infizieren kann, muss sie die Sicherheitslösung für das Netzwerk (z. B. Gateway-Firewall) und den Client (z. B. Dateisystemwächter oder HTTP-Datenverkehrsfilter) überwinden. Daher spielen lokale Sicherheitskomponenten eine entscheidende Rolle, um Malware-Infektionen zu verhindern. Unbefugte Netzwerkverbindungen werden durch die lokale Firewall blockiert (weitere Informationen in Kapitel 13). Zulässiger Datenverkehr erreicht den Client, der ihn dann mithilfe verschiedener Sicherheitsmodule filtert. Echtzeit-Sicherheitsmodule wie Dateisystemwächter, heuristische und verhaltensbasierte Scans stellen sicher, dass die Malware ungeachtet des Angriffsvektors vor der Ausführung gestoppt wird. Bei infektiösen E-Mails werden Malware-Anhänge entfernt oder direkt in Quarantäne verschoben, ohne dass die Datei jemals das Dateisystem erreicht. Bei der Internet-Sicherheit wird ähnlich vorgegangen; HTTP-Datenverkehr wird gefiltert und bei Verdacht blockiert. Erreicht Malware das System über andere Quellen wie z. B. Wechseldatenträger, wird sie durch den Dateisystemwächter blockiert, sobald die bösartige Datei auf der Festplatte gespeichert oder ausgeführt wird. Gemeinsam sorgen die Sicherheitsmaßnahmen dafür, dass keine Malware das System infiziert. Daher sollten die Maßnahmen als Ganzes, und nicht als „Alleinkämpfer“ konfiguriert werden.

Alle Clients mit der maximalen Sicherheitsstufe zu schützen, mag zwar als beste Option erscheinen, ist aber nicht möglich, da nicht alle Clients die gleichen Sicherheitseinstellungen haben können. Bei manchen Clients steht maximale Sicherheit im Vordergrund, bei anderen ist die Leistung wichtiger. Je nach ausgewähltem Element in der Ansicht CLIENTS können Sicherheitsoptionen für einzelne Clients oder Gruppen konfiguriert werden. Alle Netzwerk-Clients sollten geeignet gruppiert werden, um relevante Sicherheitseinstellungen gleichzeitig auf mehrere Computer anzuwenden. Weitere Informationen über die Verwaltung von Clients finden Sie in Kapitel 7.

Der Client-Echtzeitschutz sollte vor der Installation konfiguriert werden. Mit dem G DATA Administrator können Client-Geräte im Netzwerk vor der Installation vom G DATA Security Client ermittelt, organisiert und konfiguriert werden. Für jeden Client und jede Gruppe muss direkt bei der Installation die optimale Schutzstufe konfiguriert und aktiviert werden. Idealerweise wurden diese Einstellungen bereits für jeden Client optimiert. Da sich die tatsächliche Leistung in dieser Phase nicht messen lässt, ist eine Bewertung der Maßnahmen manchmal schwierig. Eine Möglichkeit wäre, standardmäßig restriktive Sicherheitseinstellungen festzulegen, die dann nach Bedarf gelockert werden. Alternativ hierzu können elementare Sicherheitseinstellungen verwendet werden, die Leistung und Benutzerfreundlichkeit nicht einschränken, solange sie nach der Installation noch nicht angepasst wurden.

Welche Einstellungen auf welchen Client angewendet werden, hängt von der Software und Hardware eines Clients sowie von seiner Rolle (Verwendungskontext des Computers) ab. Für die meisten Sicherheitseinstellungen kann nur eine allgemeine Empfehlung gegeben werden. Viele Unternehmensrichtlinien schreiben bestimmte Sicherheitsebenen vor, die beim Implementieren einer Sicherheitslösung nützlich sein können. Es kann aber auch sein, dass eine fallspezifische Richtlinie pro Netzwerkzone oder sogar Client-Ebene erforderlich ist. Dies kann nur in der Praxis herausgefunden werden. Daher gilt die Empfehlung, eine Sicherheitslösung Schritt für Schritt einzuführen und die einzelnen Einstellungen sorgfältig zu überwachen.

Die wichtigsten Sicherheitseinstellungen für den Echtzeitschutz können mit dem Modul CLIENT-EINSTELLUNGEN vom G DATA Administrator konfiguriert werden. Diese Einstellungen lassen sich pro Client oder Gruppe und Verwendungszweck anpassen. Die Registerkarte ALLGEMEIN enthält das Feld BEMERKUNG, damit jeder Client ordnungsgemäß konfiguriert werden kann. Dort kann der Client und seine Software beschrieben oder eine Bemerkung hinzugefügt werden, um zwischen spezifischen Sicherheitskonfigurationen zu unterscheiden.

8.1. Scans des Internet-Datenverkehrs

Die nächste Verteidigungslinie hinter der Firewall ist die Überprüfung, welcher Datenverkehr passieren darf. Der G DATA Security Client analysiert verschiedene Arten von Datenverkehr.

8.1.1. HTTP

Durch die Eingabe eines Ports unter CLIENT-EINSTELLUNGEN > WEB > INTERNETINHALTE (HTTP) scannt der G DATA Security Client den eingehenden HTTP-Datenverkehr (standardmäßig: 80 und 443/SSL). Durch das Surfen auf Websites mit bösartiger Software, das Herunterladen von Malware und den Besuch von Phishing-Websites wird eine Warnung ausgelöst und der Zugriff blockiert. Größere Dateien auf Malware zu scannen, kann eine Weile dauern. Damit es im Browser zu keiner Zeitüberschreitung kommt, kann das Kontrollkästchen ZEITÜBERSCHREITUNG IM BROWSER VERMEIDEN aktiviert werden. Diese Option sollte aktiviert bleiben. Außerdem kann eine maximale Dateigröße definiert werden, um Verzögerungen zu verhindern. Dadurch wird HTTP-Datenverkehr mit umfangreicheren Dateien nicht gescannt. Diese Option kann die Leistung zwar erhöhen, es muss jedoch sichergestellt werden, dass die Downloads im Anschluss von einer anderen Sicherheitsebene gescannt werden (z. B. dem Dateisystemwächter). Muss Datenverkehr einer bestimmten Website nicht gescannt werden (z. B. das Intranet), kann diese Website zu den NETZWERKWEITEN WEBSCHUTZ-AUSNAHMEN hinzugefügt werden.

8.1.2. E-Mail

Die zweite Kategorie von Datenverkehr, der gescannt wird, sind E-Mails (Standardports: 110/POP3, 143/IMAP, 25/SMTP)[9]. Die Ports können unten im Einstellungsbereich CLIENT-EINSTELLUNGEN > E-MAIL angepasst werden. Dadurch lassen sich Zeitüberschreitungen von E-Mail-Clients verhindern, wenn die Option für die entsprechenden Ports aktiviert wird. Unter SCANOPTIONEN kann die zu verwendende Scan-Engine definiert werden. G DATA nutzt zwei Scan-Engines, um optimale Sicherheit zu bieten. Beeinträchtigt dies jedoch die Leistung, kann mit nur einer Engine gearbeitet werden (siehe Abschnitt 8.4).

8.1.2.1. Eingehender Datenverkehr

Alle eingehenden E-Mails werden automatisch auf Viren geprüft. Bei einem Malware-Fund können E-Mails desinfiziert werden oder der infizierte Inhalt wird entfernt und ein Hinweis zur Infektion in den E-Mail-Text eingefügt. E-Mails sollten zunächst desinfiziert werden. Schlägt die Desinfektion fehl, sollte

[9] Hinweis: Dies bezieht sich nur auf Scans von E-Mails auf dem Client. E-Mail-Scans auf dem Server werden von der G DATA MailSecurity ausgeführt.

infizierter Inhalt automatisch gelöscht werden. Strikter wäre, den infizierten Inhalt automatisch zu entfernen und den Benutzer optional zu benachrichtigen. Die Option NUR PROTOKOLLIEREN / WARNUNG EINFÜGEN kann in Netzwerken, Netzwerkzonen oder Abteilungen verwendet werden, wo Endbenutzer auf eingehende E-Mails zugreifen müssen, auch wenn Inhalt oder Anhang infiziert sind. In diesem Fall kann der Dateisystemscanner die Malware unschädlich machen. Dieses Szenario wird allerdings nicht empfohlen, da die Deaktivierung einer Schutzebene das Risiko einer Malware-Infektion erhöht. Netzwerke mit Microsoft Outlook in Kombination mit Microsoft Exchange können keine standardmäßigen Portüberwachungen anwenden, da Exchange Server und Clients über ein proprietäres Protokoll kommunizieren. Zum Schutz von Exchange-Umgebungen sollte das Outlook-Plug-in aktiviert oder das Exchange-Plug-in der MailSecurity installiert werden (siehe Abschnitt 4.2.4.1).

Als zusätzliche Malware-Erkennungsmaßnahme kann das OutbreakShield aktiviert werden. Es verwendet eigene Signaturen, um noch mehr Malware-verteilende Spam-Kampagnen zu erkennen, und beruht auf allgemeinen Eigenschaften der Massenverteilung. Die Erkennung ist also bereits möglich, noch bevor die Virensignaturen der herkömmlichen Engines aktualisiert wurden. Das OutbreakShield ist relativ ressourcensparend und schont die Client-Leistung.

Neben E-Mail-Bedrohungen findet G DATA auch Spam. Die Funktion CLIENT-EINSTELLUNGEN > ANTISPAM überprüft den E-Mail-Verkehr und filtert Spam (auf Verdacht). In Kombination mit Filterregeln im lokalen E-Mail-Client oder im Outlook-Plug-in filtert ANTISPAM Spam bereits vor dem Posteingang. ANTISPAM schont die Ressourcen, kann jedoch deaktiviert werden, falls andere Spam-Maßnahmen angewendet werden, wie z. B. eine Lösung auf dem Mail-Server.

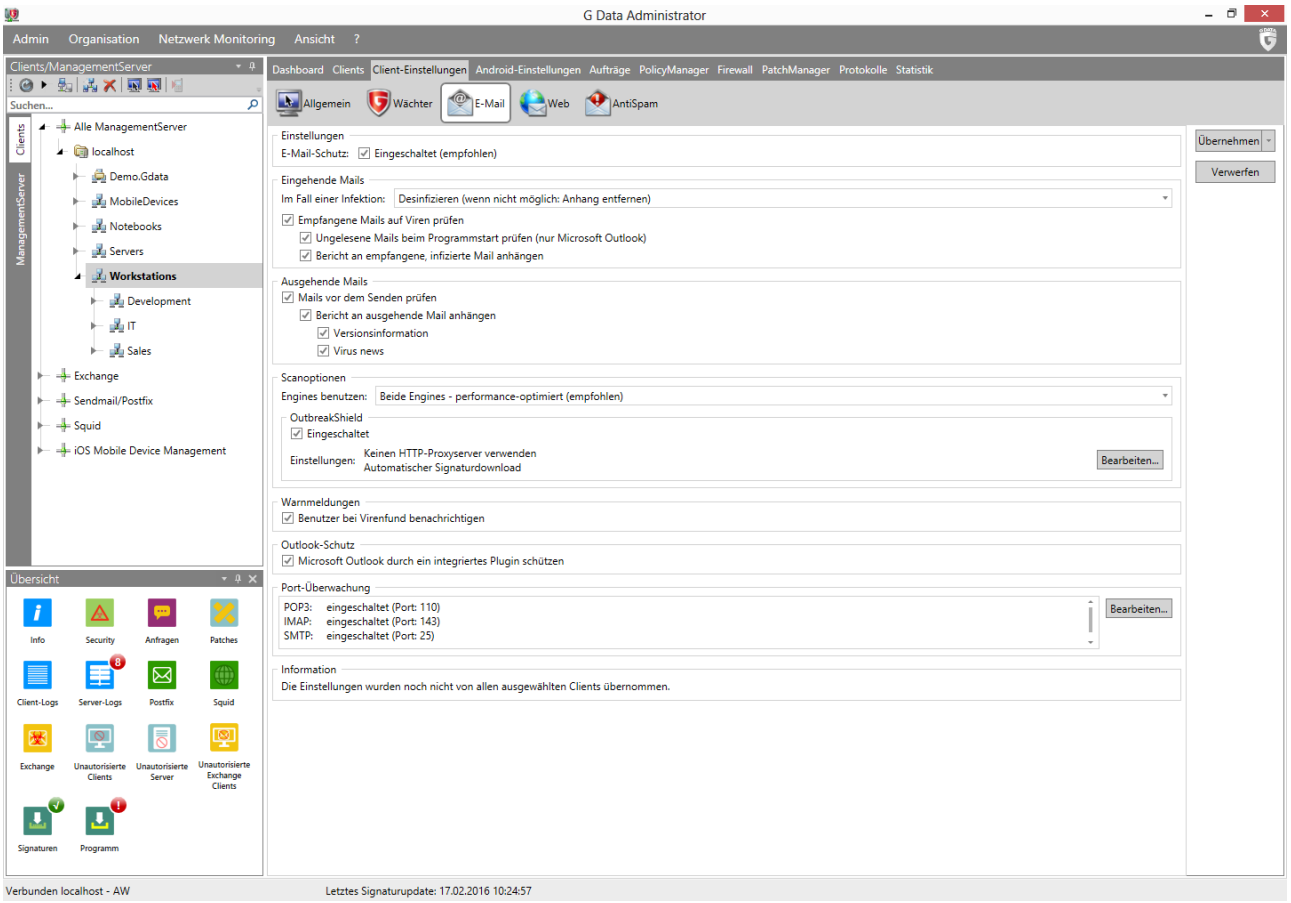

Abbildung 34: G DATA Administrator – Client-Einstellungen, E-Mail

8.1.2.2. Ausgehender Datenverkehr

Auch ausgehende E-Mails sollten nach Viren gescannt werden, um nicht versehentlich Malware zu versenden. Optional kann ein Bericht an ausgehende E-Mails angehängt werden, der besagt, dass die Nachricht gescannt wurde. Dadurch erhalten die Empfänger eine Bestätigung, dass die E-Mail tatsächlich sicher ist.

8.2. Wächter

Die Kategorie „Wächter“ stellt die letzte Sicherheitsebene dar. Sie ist mehrschichtig und schützt durch Dateisystemscans, Verhaltensüberwachung und spezifische Maßnahmen vor Banking-Trojanern und infizierten USB-Geräten.

8.2.1. Dateisystem

Sobald eine Datei lokal gespeichert oder gelesen wird, aktiviert sich der Dateisystemwächter. Als Erstes scannt der Wächter die Datei mit einer oder zwei Scan-Engines, um sie mit lokal gespeicherten Virensignaturen zu vergleichen. Bekannte Malware wird erkannt und der Wächter führt die konfigurierte Aktion aus (z. B. Desinfektion, Entfernung oder Verschiebung der Datei in Quarantäne). Wird eine Datei nach dem Vergleich mit Virensignaturen nicht als Malware erkannt, wird sie heuristisch gescannt. Ähnlich den Virensignaturen wird die Malware-Datei auch hier auf Muster geprüft, die häufig von Malware erzeugt werden. Heuristische Scans verursachen zwar eine leicht erhöhte False-Positive-Rate, unterstützen aber die Erkennung von Malware, für die keine Signaturen verfügbar sind.

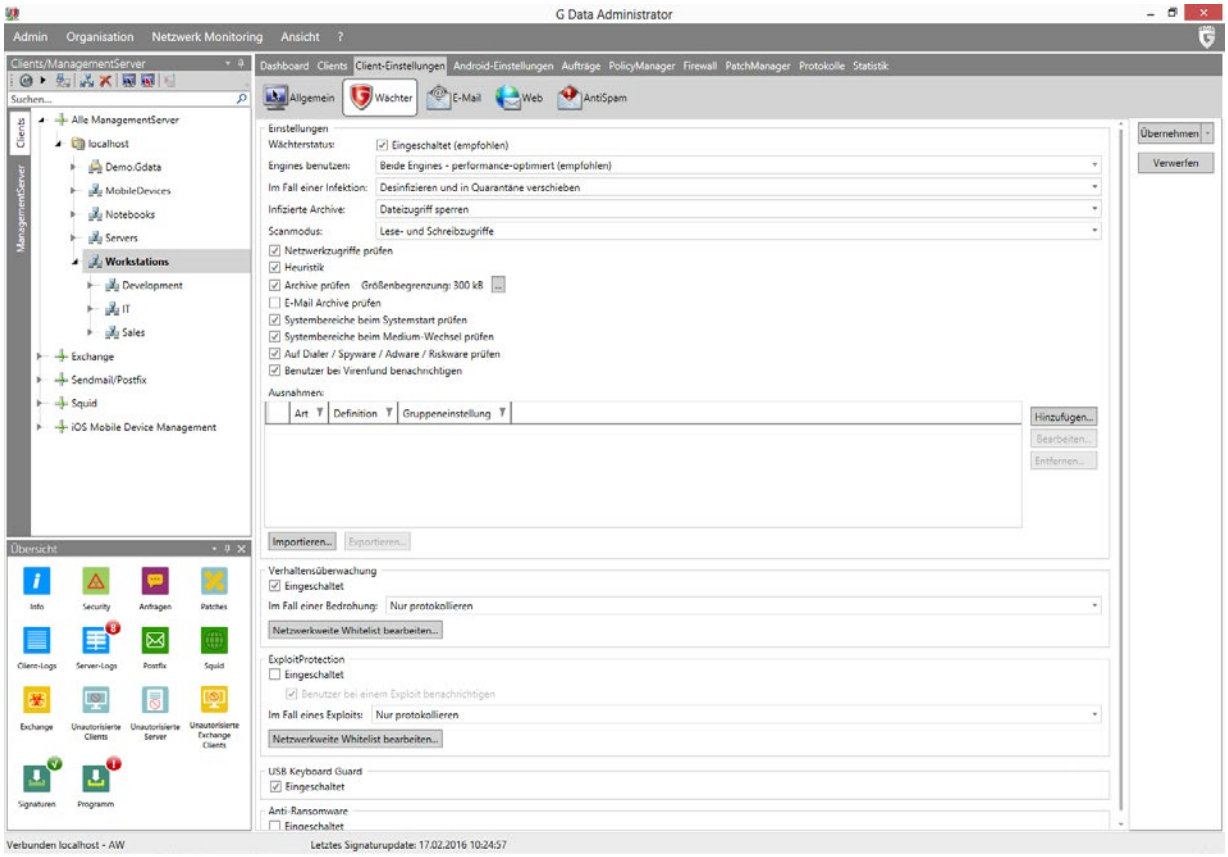

Abbildung 35: G DATA Administrator – Client-Einstellungen, Wächter

Die Registerkarte CLIENT-EINSTELLUNGEN > WÄCHTER bietet Zugriff auf Einstellungen für den Dateisystemwächter. Der Wächter ist standardmäßig mit einem ausgewogenen Profil aktiviert und ermöglicht eine ressourcenschonende Sicherheitsleistung. Es können weitere Sicherheitsmaßnahmen hinzugefügt oder – aus Leistungsgründen – deaktiviert werden. Wie bei den meisten Einstellungen sollte immer optimale Sicherheit gewählt werden, wenn dadurch die Leistung nicht wesentlich beeinträchtigt wird. Der WÄCHTERSTATUS sollte immer auf AKTIVIERT eingestellt sein. Durch die vollständige Deaktivierung des Wächters wird eine der zentralen Komponenten der G DATA Sicherheitslösung ausgeschaltet. Dies sollte nur in Betracht gezogen werden, wenn ein einzelner Client extreme Kompatibilitätsprobleme hat oder ausreichend durch andere Sicherheitsmaßnahmen geschützt wird.

Der Dateisystemwächter scannt die Dateien mit zwei Software-Engines auf Malware. Dies bietet optimale Sicherheit, da eine Malware-Infektion, die Engine 1 passiert, von Engine 2 erkannt wird. Standardmäßig und empfohlen ist die Aktivierung beider Engines. Kommt es zu Leistungseinbußen, können die Dateien auch mit nur einer der beiden Engines gescannt werden.

G DATA kann verschiedene Aktionen durchführen, wenn eine mit Malware infizierte Datei erkannt wird. Die restriktivste Einstellung ist das sofortige Löschen der infizierten Datei. Dadurch hat die Malware keine Chance im System. Es können jedoch Daten verloren gehen, falls wichtige Dokumente infiziert oder fälschlich als Malware erkannt wurden. Als Hauptaktion sollte Desinfektion gewählt werden. Dadurch versucht der Dateisystemwächter, die infizierte Datei zu reparieren. Danach wird sie in Quarantäne verschoben. Andernfalls wird sie sofort in Quarantäne verschoben oder blockiert. Wird der Zugriff blockiert, kann die Malware zwar nicht mehr ausgeführt werden, aber die Datei bleibt erhalten. Durch das Verschieben der Datei in Quarantäne kann sie nicht mehr versehentlich ausgeführt werden. Die Möglichkeit, sie wiederherzustellen oder manuell zu reparieren, bleibt offen. Dateien in Quarantäne können zur weiteren Analyse an G DATA gesendet werden. Der Dateisystemwächter kann die Inhalte von Archiven (z. B. ZIP-Dateien) scannen, jedoch keine einzelnen infizierten Dateien aus einem Archiv entfernen. Archive mit infizierten Dateien können als Ganzes in Quarantäne verschoben, gelöscht oder blockiert werden. Da archivierte Dateien nach der Extraktion oder beim Öffnen gescannt werden, besteht bei infizierten Archiven ein geringeres Risiko. Anstatt eine Datei zu löschen, sollte der Zugriff darauf blockiert werden. Archivüberprüfungen können zugunsten der Leistung vollständig deaktiviert werden. Die Überwachung des Netzwerkzugriffs ist standardmäßig aktiviert, kann jedoch deaktiviert werden, wenn sich der Computer in einem komplett durch G DATA geschützten Netzwerk befindet.

Der Scanmodus entscheidet, wann der Dateisystemwächter seine Arbeit aufnimmt. Dateien können bei LESEZUGRIFF, bei LESE- UND SCHREIBZUGRIFF oder BEI AUSFÜHRUNG gescannt werden. Die Option BEI AUSFÜHRUNG bietet elementaren Schutz beim Scannen von ausgeführten Dateien. Dadurch (wie auch durch das Blockieren) wird zwar verhindert, dass Malware den Client infiziert, nicht aber, dass sie weiter verbreitet wird. Damit infizierte Dateien sogar erkannt werden, wenn sie nicht ausgeführt werden, muss die Option LESEZUGRIFF oder LESE- UND SCHREIBZUGRIFF ausgewählt werden. Dadurch werden Dateien auch beim Kopieren zwischen Ordnern, Festplatten oder Clients gescannt, um Malware zu erkennen, die sich durch das Beschreiben von Netzwerkfreigaben im Netzwerk ausbreitet. Malware mit der Option LESE- UND SCHREIBZUGRIFF zu scannen, beansprucht die Festplatte in hohem Maß. Wird die Client-Leistung beeinträchtigt, kann der Scanmodus auf LESEZUGRIFF herabgesetzt werden. BEI AUSFÜHRUNG sollte nur verwendet werden, wenn selbst Scans bei Lesezugriff das System überlasten.

Standardmäßig prüft der Dateisystemwächter Archive, E-Mail-Archive und Systembereiche auf Malware. Da Archive aufgrund ihrer Größe beim Scannen problematisch sein können, lässt sich eine Größenbegrenzung definieren. So kann der Wächter die Leistung nicht durch langwierige Zugriffsscans von Archiven herabsetzen. Alternativ können Archivscans komplett deaktiviert werden. Auch ohne automatische Zugriffsscans von Archiven können die Benutzer weiterhin einen manuellen Scan starten, wenn sie eine verdächtige Archivdatei finden. Bei der Aktivierung von E-Mail-Archivscans muss berücksichtigt werden, dass die E-Mail-Software einen Fehler verursacht, wenn ihre Datendatei in Quarantäne verschoben wird. In den meisten Fällen ist es besser, E-Mail-Archivscans zu deaktivieren und den Dateisystemwächter Dateien bei der Extraktion prüfen zu lassen (z. B. beim Speichern eines Anhangs auf der lokalen Festplatte). Systembereiche (z. B. Boot-Sektoren) können beim Start oder beim Medienwechsel gescannt werden. Dieser Scan sollte aktiviert sein, um Viren in Boot-Bereichen zu erkennen. Außerdem ist standardmäßig die Option zur Suche nach Dialern, Spyware, Adware und Riskware aktiviert. Obwohl es sich dabei nicht unbedingt um Malware handelt, sind diese Dateiarten normalerweise unerwünscht.

Erkennt der Dateisystemwächter eine Bedrohung, führt er automatisch die vom Administrator definierte Aktion durch. Außerdem kann der G DATA Security Client eine Meldung auf dem Client anzeigen, die den Benutzer über einen Malware-Fund informiert. Die Meldung enthält Dateinamen, Dateipfad und Namen der gefundenen Malware. Durch die Anzeige einer Warnung erfährt der Benutzer, dass das aktuell ausgeführte Programm oder die derzeit besuchte Website schädlich ist. Einige Benutzer könnten jedoch durch die Meldung verwirrt werden. Meldungen über Bedrohungen, die bereits blockiert wurden, sind für keinen Benutzer relevant und können einzeln deaktiviert werden.

Bestimmte Dateien oder Ordner können von den Scans des Dateisystemwächters ausgeschlossen werden. Mit AUSNAHMEN können unhandliche Dateien bei Zugriffsscans ignoriert werden. Dadurch werden selten genutzte, große Dateien von Zugriffsscans ausgeschlossen werden, falls sie in einem geplanten Scan enthalten sind (siehe Abschnitt 9.2.1.3). Auf ähnliche Weise kann für Datenbankdateien auf Zugriffsscans verzichtet werden, falls sie ohnehin regelmäßig durch einen On-Demand-Scan geprüft werden. Es sollten jedoch nicht zu viele Ausnahmen hinzugefügt werden. Nur Dateien, die beim Zugriffsscan die Leistung beeinträchtigen, sollten als Ausnahme definiert werden, und das nur, wenn sie regelmäßig durch einen regulären Scan geprüft werden. Als sicher bekannte Dateien, die false positive Ergebnisse generieren, können ebenfalls der Ausnahmeliste hinzugefügt werden, nachdem ihre Sicherheit verifiziert wurde. Bei der Definition von Ausnahmen muss darauf geachtet werden, dass sie nur für die Clients bzw. Gruppen gelten, die wirklich diese Ausnahme benötigen. Da eine Ausnahme verhindert, dass die Datei vom Dateisystemwächter auf Malware geprüft wird, kann sie weitreichende Auswirkungen haben und sollte nur für so wenige Clients wie möglich gelten. Es können Verzeichnisse, Laufwerke, Dateien und Prozesse von Scans ausgenommen werden. Verzeichnisse, Laufwerke und Prozesse können manuell in das Textfeld eingegeben oder aus einer Ordnerstruktur ausgewählt werden. Die Auswahl kann aus lokalen Ordnern und Dateien erfolgen oder durch Öffnen der Ordnerstruktur auf einem der Clients im Netzwerk. Bei Prozessen muss der vollständige Pfad und der Dateiname in das Textfeld eingegeben werden. Dateiausnahmen sollten als Dateiname eingegeben werden und können mit Platzhaltern (**?** und *****) definiert werden. Diese Platzhalter stellen einzelne Zeichen bzw. Zeichenfolgen dar.

8.2.2. Verhaltensüberwachung

Die Verhaltensüberwachung ist der nächste Schritt des heuristischen Verfahrens. Während der Ausführung von Dateien wird jede Aktion verfolgt. Zeigt die Datei ein Verhalten, das dem von Malware gleicht (z. B. übermäßiges Schreiben in die Registry oder Erstellung von Autostart-Einträgen), kann ihre Ausführung blockiert werden. Außerdem kann die Datei in Quarantäne verschoben werden. Erzeugt die Verhaltensüberwachung false positive Ergebnisse, kann der Whitelist im entsprechenden Bericht im Modul SICHERHEITSEREIGNISSE ein Eintrag hinzugefügt werden.

8.2.3. ExploitProtection

Exploits suchen speziell in Drittanbieter-Software auf dem Client nach Sicherheitslücken. ExploitProtection überprüft das Verhalten der installierten Software auf Unregelmäßigkeiten. Wird ungewöhnliches Verhalten entdeckt, kann es entweder protokolliert oder aber geblockt werden. Es wird empfohlen, verdächtige Prozesse zu blockieren. Jede Aktion der ExploitProtection wird als Bericht im Modul SICHERHEITSEREIGNISSE festgehalten. Wird ein Programm fälschlicherweise als Bedrohung identifiziert, kann anhand des zugehörigen Berichts ein Eintrag in der Whitelist erstellt werden.

8.2.4. BankGuard

Eine spezifischere Form der Verhaltensüberwachung ist BankGuard (auf der Registerkarte WEB verfügbar). BankGuard überwacht die Browser-Systemdateien für Microsoft Internet Explorer, Mozilla Firefox und Google Chrome und schützt vor Malware, die Websites für Online-Banking manipuliert.

8.2.5. Anti-Ransomware

Während herkömmliche Malware ein Gerät infiziert, um es in einem Botnet zu verwenden oder Kreditkartendaten zu entwenden, wollen die Entwickler von Ransomware sich ihre Beute sichern, indem sie den Benutzer direkt unter Druck setzen. Ransomware sperrt das Gerät oder verschlüsselt sogar Daten, bis das Opfer das Lösegeld zahlt. Neben der Erkennung durch Signaturen oder Verhaltensweisen findet die Anti-Ransomware-Funktion auch konkrete Aktionen der Ransomware wie Dateiverschlüsselungen und sperrt sie, bevor sie Schaden anrichten können.

Ist die Anti-Ransomware aktiviert, wird jede Bedrohung protokolliert und ein Bericht an den ManagementServer gesendet. Je nach Einstellungen unter CLIENT-EINSTELLUNGEN > WÄCHTER protokolliert der G DATA Security Client nur die Bedrohung oder sperrt ihre Ausführung und verschiebt sie in Quarantäne. Optional kann der Benutzer im Fall einer Bedrohung auch benachrichtigt werden. Bei Falsch-Positiven kann ein Eintrag der Whitelist hinzugefügt werden.

8.2.6. USB Keyboard Guard

USB Keyboard Guard schützt Clients vor BadUSB-Angriffen. Böswillig umprogrammierte USB-Geräte, wie Kameras, USB-Sticks und Drucker, können als Tastatur dienen, wenn sie an einen Computer angeschlossen werden. Damit diese Geräte keine unbefugten, automatischen Befehle ausführen, muss der Benutzer das USB-Gerät bestätigen, das sich als Tastatur ausgibt. Hat der Benutzer tatsächlich eine Tastatur angeschlossen, kann sie unbesehen bestätigt werden. Gibt sich das Gerät jedoch selbst als

Tastatur aus und hat der Benutzer etwas Anderes angeschlossen, sollte die Nutzung nicht autorisiert werden, da es sich um ein infiziertes Gerät handeln könnte. Ungeachtet der Entscheidung des Benutzers wird im Modul SICHERHEITSEREIGNISSE ein Bericht hinzugefügt. Wurde ein Gerät autorisiert, kann es der Administrator dennoch blockieren, indem er mit der rechten Maustaste auf den Bericht klickt und die Autorisierung zurücknimmt.

USB Keyboard Guard sollte aktiviert sein, um optimal vor infizierten USB-Geräten zu schützen. Im Gegensatz zu anderen Schutzmaßnahmen ist diese Option nicht völlig transparent, da der Endbenutzer das angeschlossene Gerät als Tastatur bestätigen muss. Über die erstellten Berichte beim Autorisieren oder Blockieren eines Geräts hat der Administrator dennoch völlige Kontrolle.

8.3. Leistung

Client-Hardware und -Software sowie die Netzwerkinfrastruktur besitzen nur begrenzte Kapazität. Früher ging die Informationssicherheit immer auf Kosten der Leistung. Je mehr Sicherheitsmaßnahmen implementiert wurden, desto höher war der gemessene Leistungsabfall. Deshalb ist die Leistung für die meisten modernen Client-Server-Sicherheitslösungen der entscheidende Faktor. G DATA bietet optimierte Sicherheitsmodule, die kaum die Client-Leistung beeinträchtigen, selbst wenn sie auf optimale Sicherheit konfiguriert wurden. Durch verschiedene Umstände, wie Hardware und Software, kann sich eine unterschiedliche Gewichtung von Sicherheit und Geschwindigkeit ergeben. Ein Netzwerkaufbau gemäß den definierten Netzwerkzonen und Client-Rollen (siehe Abschnitt 1.1) hilft bei der Entscheidung, welche Clients mehr Sicherheit benötigen und welche Clients sich auf Leistung konzentrieren können. Das richtige Gleichgewicht zu finden, ist schwierig: In manchen Unternehmensnetzwerken sollten so viele Sicherheitsebenen wie physisch möglich aktiviert werden, in anderen sind schnelle Clients wichtiger. Das mehrschichtige Konzept von G DATA bietet den Vorteil, dass die Sicherheitsfunktionen für jeden einzelnen Client optimiert werden können. Verschiedene Optionen ergänzen sich, wodurch eine oder zwei deaktiviert werden können, ohne die Sicherheitsleistung zu beeinträchtigen.

Im Allgemeinen wird empfohlen, auf Nummer sicher zu gehen und zweimal nachzudenken, bevor eine Sicherheitsfunktion aus Leistungsgründen deaktiviert wird. Bei der Installation einer Sicherheitslösung sollte mit dem maximalen, für den jeweiligen Client angemessenen Sicherheitsniveau begonnen werden und dieses erst verringert werden, wenn der Client zu langsam wird. Manche Sicherheitseinstellungen beeinflussen die Leistung mehr als andere. Der Dateisystemwächter benötigt viele Ressourcen, wenn der Client vor allem für Dateivorgänge genutzt wird. Einstellungen wie der Archivscan können die Verarbeitung von großen Dateien verzögern, während Scans bei Lese- und Schreibzugriff die Festplatte erheblich ausbremsen. Clients mit einer weniger leistungsstarken CPU können bei Verwendung beider Scan-Engines verlangsamt werden. Die Deaktivierung einer Engine beschleunigt den Computer. Andere Dateiwächtereinstellungen, wie die Heuristik oder die Verhaltensüberwachung, haben nur geringe Auswirkungen auf die Client-Leistung.

Die Gebrauchstauglichkeit wird noch von anderen Faktoren als der Leistung beeinflusst. Sicherheitssoftware beinhaltet immer ein geringes Risiko, dass reguläre Dateien als Malware erkannt werden. Grund dafür sind die Muster im Heuristikmodul oder in der Verhaltensüberwachung. Wurde der Schutz zu streng konfiguriert, gibt es mehr false positive Ergebnisse. Ist die Sicherheit jedoch zu lax, kann Malware unbemerkt eindringen. Wie bei allen Leistungsproblemen sollte auch gegen false positive

Ergebnisse erst dann etwas unternommen werden, wenn sie tatsächlich auftreten. Wurde eine Datei als Malware erkannt, zeigt der Abschnitt SICHERHEITSEREIGNISSE vom G DATA Administrator, auf welchem Client und durch welches Schutzmodul sie erkannt wurde. Die Einstellungen für das relevante Modul können dann weniger streng konfiguriert werden oder diese spezifische Datei wird auf die Whitelist gesetzt (falls das Sicherheitsmodul diese Maßnahme unterstützt). Da der Client durch die Verringerung der Sicherheitsstufe einem Risiko aussetzt wird, sollte die betroffene Datei zunächst nur auf die Whitelist gesetzt werden. Dadurch wird sie nicht erneut als Malware erkannt, nicht entfernt und nicht in Quarantäne verschoben. Identifiziert ein bestimmtes Sicherheitsmodul Dateien oft fälschlicherweise als bösartig, kann die Sicherheitsstufe verringert werden. Die vollständige Abschaltung eines Moduls sollte nur der allerletzte Ausweg sein. In den meisten Fällen reicht es aus, eine Datei in Quarantäne zu verschieben, anstatt sie zu löschen, oder eine Infektion zu protokollieren, anstatt sie direkt zu bekämpfen. Diese Fälle erfordern jedoch ein administratives Eingreifen. Falls G DATA so konfiguriert wurde, dass Infektionen nicht automatisch bekämpft werden, ist eine manuelle Untersuchung notwendig. Mit Alarmmeldungen kann der Administrator auf derartige Fälle aufmerksam gemacht werden (siehe Abschnitt 6.2). Ist es nicht möglich, die Einschränkungen des Sicherheitsmoduls zu lockern (wenn beispielsweise eine Client-Gruppe absolute Sicherheit benötigt), kann der Zugriff auf Anwendungen, Geräte und Websites mithilfe des PolicyManagers beschränkt werden (siehe Kapitel 14).

8.4. Betriebssystemsicherheit

Sicherheitssoftware verringert zwar die Wahrscheinlichkeit einer Malware-Infektion, doch können zusätzliche Maßnahmen auf Betriebssystemebene konfiguriert werden. Einige Aspekte der Netzwerksicherheit und der lokalen Betriebssystemsicherheit können effizient mithilfe von lokalen Einstellungen oder netzwerkbasierten Gruppenrichtlinien gesteuert werden. Diese Einstellungen können wahlweise auf allen Clients durchgesetzt werden oder es werden nur die am stärksten gefährdeten Netzwerkzonen und Client-Rollen geschützt.

Windows ist standardmäßig so konfiguriert, dass viele Hintergrunddienste unabhängig von ihrer Wichtigkeit ausgeführt werden. Einige unterstützen wichtige Windows-Funktionen, andere werden nur für sehr spezifische Konfigurationen oder Software-Suiten verwendet. Jeder Dienst kann jedoch einen Angriffsvektor darstellen. Angreifer suchen ständig nach Schwachstellen in Windows-Diensten, um eine Sicherheitslücke zu nutzen und auf das System zuzugreifen. Eine Maßnahme kann das Patchen der betroffenen Dienste sein. Dies kann jedoch erst erfolgen, wenn Microsoft oder ein Software-Anbieter die Schwachstelle entdeckt hat und einen Patch herausgibt. Ungenutzte Dienste können im Voraus deaktiviert werden, so dass diese potenzielle Schwachstelle für Hacker geschlossen ist. Dienste zu deaktivieren, kann sich auch positiv auf die Rechnerleistung auswirken. Mit dem Befehl **services.msc** wird auf einem Windows-Computer das Fenster DIENSTE geöffnet, der alle auf dem System installierten Dienste anzeigt, ob sie nun aktiviert und ausgeführt werden oder nicht. Dienste zu deaktivieren, wirkt sich nicht auf der Stelle positiv aus. Zuvor sollte geprüft werden, dass der betroffene Client nicht auf diesen Dienst angewiesen ist.

Microsoft hat die Autostart-Funktion in neuen Versionen seines Betriebssystems durch ein Fenster ersetzt, in dem der Benutzer eine bestimmte Aktion auswählen kann, wie z. B. Stammordner eines Datenträgers auswählen oder darin enthaltene Daten zu importieren, um das Risiko einer Malware-Verbreitung über Wechseldatenträger (z. B. USB-Sticks oder CD-ROMs) zu verringern. Dadurch wird die

oft verwendete Konfigurationsdatei „autorun.inf“ umgangen. Die Verbreitung von Malware über autorun.inf kann so zwar effektiv gestoppt werden, doch der Benutzer kann diese Einstellung umgehen. In dem Fenster, das beim Anschließen eines Wechseldatenträgers angezeigt wird, kann der Benutzer eine Standardaktion auswählen, die für alle Medien dieser Art ausgeführt wird. Wird also zu einem späteren Zeitpunkt ein infizierter USB-Stick angeschlossen, wird er wie jeder andere Datenträger ausgeführt. Ist eine Sicherheitslösung installiert, kann selbst ausgeführte Malware keinen Schaden anrichten. In Unternehmensnetzwerken wird durch die Deaktivierung der Autostart-Funktion jedoch die Sicherheit erhöht. In kleineren Netzwerken kann die Autostart-Funktion mithilfe von lokalen Registrierungseinstellungen deaktiviert werden: Im Registrierungs-Editors wird der DWORD-Wert **NoDriveTypeAutoRun** mit dem hexadezimalen Wert **0xFF** in den Schlüssel „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer“ eingefügt, um die Autostart-Funktion für alle Laufwerksarten zu deaktivieren. Alternativ ist ein Hotfix von Microsoft verfügbar, um die Einstellung automatisch zu ändern[10]. In Unternehmensnetzwerken steht eine Gruppenrichtlinie zur Verfügung, um die Autostart-Funktion für bestimmte Computer oder Benutzer zu deaktivieren.

Heruntergeladene Dateien und E-Mail-Anhänge sind eine weitere gängige Infektionsquelle. Aus diesem Grund warnen Browser und E-Mail-Clients die Endbenutzer normalerweise, bevor eine Datei heruntergeladen wird. Dadurch wird theoretisch über das Risiko beim Download von Dateien aus öffentlichen Quellen informiert. In der Praxis werden die Meldungen jedoch häufig nicht einmal gelesen. Sicherheitslösungen erfassen Malware durch Webschutz, Blacklists und andere Lösungen, lange bevor die Datei die Festplatte erreicht. Und selbst dann wird sie vom Dateisystemwächter erkannt und blockiert. Es kann jedoch sein, dass das Risiko, Malware könnte über einen Client-Browser eindringen, vollkommen ausgeschlossen werden muss. Mithilfe von Sicherheitszonen können Datei-Downloads für alle Browser blockiert werden, die den integrierten Windows Anlagen-Manager unterstützen (Microsoft Internet Explorer, Google Chrome). Dadurch können URL-Aktionen so konfiguriert werden, dass sie in bestimmten Sicherheitszonen, beispielsweise bei der Ausführung eines Downloads, nicht zulässig sind[11]. Andere Browser ignorieren möglicherweise die Zoneneinstellungen. In diesem Fall kann es hilfreich sein, den Dateispeicherungszugriff zu beschränken und die Benutzerkontensteuerung oder eine angemessene Gruppenrichtlinie zu aktivieren.

Zu den elementaren Schutzmaßnahmen gehört es auch, die Berechtigungsstufe für Endbenutzer auf die niedrigste Stufe zu setzen. Benötigt ein Endbenutzer keine erweiterten Systemberechtigungen, um mit dem Client-Computer zu arbeiten, sollten diese Berechtigungen auch nicht gewährt werden – so wird Schaden durch Malware verhindert. Dazu gehört auch, dass der Endbenutzer sich nicht mit einem Administratorkonto am Client-Computer anmelden kann und dass Gruppenrichtlinien den Zugriff auf lokale und Netzwerkressourcen einschränken. Andere Aktionen zu blockieren, wie die Anzeige von Wechseldatenträgern oder die Verwendung von bestimmten Anwendungen, können einfach mithilfe des PolicyManager-Moduls von G DATA konfiguriert werden (siehe Kapitel 14).

Bei lokalen Sicherheitseinstellungen gibt es nicht die eine Konfiguration, die für alle passt. Jede Netzwerkzone hat andere Anforderungen an die Clients und jeder einzelne Benutzer kann weitere Änderungen der Sicherheitsrichtlinien erfordern. Ein guter Ausgangspunkt für Netzwerke mit Active

[10] Siehe http://support.microsoft.com/kb/967715.
[11] Siehe http://msdn.microsoft.com/library/ms537183.aspx.

Directory sind Gruppenrichtlinien. Mit dieser integrierten Funktion können umfassende Regeln für lokale und Netzwerkressourcen sowie für die Verwaltung von Berechtigungen konfiguriert werden. Bei Netzwerken ohne Active Directory können die Einstellungen lokal angepasst werden.

8.5. Schutz von Web-Proxys

Echtzeitschutz ist nicht allein auf Sicherheitsmodule auf den Clients begrenzt. Der Internetdatenverkehr kann gescannt werden, noch bevor er den Client erreicht. Dazu bietet G DATA ein Sicherheits-Plug-in für den beliebten Web-Proxyserver Squid. Das Linux Web Security Gateway-Modul ist optional verfügbar.

Das Linux Web Security Gateway kann im Rahmen des G DATA Security Clients für Linux installiert werden (siehe Abschnitt 4.8.3). Nach der Installation verbindet es sich automatisch mit dem übergeordneten ManagementServer. Die Einstellungen können über den G DATA Administrator im SQUID-Modul verwaltet werden. Durch das Aktivieren des Virenschutzes wird der gesamte Web-Datenverkehr, der den Squid-Proxy passiert, auf Viren gescannt. Dies ist die empfohlene Einstellung für grundlegenden Schutz. Wird die Option AntiPhishing aktiviert, wird automatisch auch in der Cloud geprüft, ob der Datenverkehr verdächtig ist. Durch Aktivieren der Option BERICHTE ERSTELLEN wird bei jedem Virenfund ein Bericht zum Modul SICHERHEITSEREIGNISSE hinzugefügt Diese Option sollte aktiviert sein, kann aber auch deaktiviert werden, falls zu viele Ereignisse erzeugt werden, die kein Eingreifen erfordern.

Die Blacklist ist ein verfeinerter Kontrollmechanismus. Statt nur den vireninfizierten Datenverkehr zu blockieren, kann der Administrator auch spezifische Webdomänen, Client-IP-Adressen und MIME-Typen zur Blacklist hinzufügen. Ein Szenario ist das Blockieren spezifischer Websites im gesamten Netzwerk. Die Wirkung ist ähnlich der des PolicyManager-Moduls WEB-INHALTSKONTROLLE auf dem Client (siehe Abschnitt 14.3). Mit der MIME-Typ-Option können jedoch auch spezifischer Dateitypen, beispielsweise ZIP-Archive (durch die Eingabe von **application/zip**) blockiert werden[12]. Solche Schutzmaßnahmen sind weitreichend und nicht immer anwendbar, bieten jedoch eine Sicherheitsschicht für Netzwerk-Clients, die ansonsten ungeschützt wären.

[12] Eine Liste mit allen MIME-Typen ist unter https://www.sitepoint.com/web-foundations/mime-types-complete-list/ einsehbar.

9. On-Demand-Schutz

Zusätzlich zum Echtzeitschutz können Client-Computer auch auf Abruf, also „on demand“, geschützt werden. On-Demand-Scans werden einmal oder regelmäßig ausgeführt, um einen vordefinierten Bereich des Client-Computers auf Malware zu prüfen. Der On-Demand-Schutz sollte zusätzlich zum Echtzeitschutz konfiguriert werden, da letzterer nur Dateien scannt, die momentan geöffnet sind. On-Demand-Scans erkennen Malware in allen Dateien auf dem Client-Computer, ungeachtet davon, ob sie gelesen oder geschrieben werden. Durch die Planung eines regelmäßigen On-Demand-Scans für einen Client-Computer kann die gesamte Festplatte gescannt werden, um zu prüfen, ob Malware inaktive Dateien infiziert hat. Mithilfe der G DATA Software können zwei Arten von On-Demand-Scans geplant werden: ein Leerlauf-Scan oder einzelne bzw. regelmäßige Scans. Der Leerlauf-Scan wird für den On-Demand-Schutz empfohlen, da er nicht geplant werden muss: Er scannt automatisch Clients, wenn sie nicht in Gebrauch sind. Alternativ können Clients mithilfe von Scans zu einem vordefinierten Zeitpunkt gescannt werden.

9.1. Leerlauf-Scan

Ein normaler Komplett-Scan, der zu einem bestimmten Zeitpunkt des Tages geplant ist, erfordert erhebliche Computerressourcen. Daher ist es wenig praktikabel, ihn auszuführen, während ein Benutzer angemeldet ist. Ein Komplett-Scan außerhalb der Geschäftszeiten verhindert Produktivitätsunterbrechungen, funktioniert aber nur mit einem eingeschalteten Client. Die Konfiguration eines Leerlauf-Scans ist also die perfekte Lösung: Ist der Client eingeschaltet, aber nicht in Gebrauch, startet der G DATA Security Client einen automatischen Scan im Hintergrund. Dabei werden vordefinierte Laufwerke, Dateien und Ordner gescannt. Kehrt der Benutzer an den Client zurück, pausiert der Scan. Er erzielt also die Funktion und Sicherheitsstufe eines normalen Scans, verhindert jedoch potenzielle Leistungseinbußen.

Bei Clients, die nicht immer mit dem Unternehmensnetzwerk verbunden sind, kann ein Leerlauf-Scan ein Ersatz für geplante Scans sein. Ein Laptop, der sich nach längerer Zeit wieder mit dem Netzwerk verbindet, erhält neu geplante Scans, die sofort ausgeführt werden, wenn sie überfällig sind. Dies kann die Rechnerleistung beeinträchtigen. Werden für derartige Clients Leerlauf-Scans aktiviert und Komplett-Scans deaktiviert, ist der Client vollständig geschützt, ohne beim Start überlastet zu werden.

Das Infobereichssymbol vom G DATA Security Client muss bei allen Sitzungen aktiviert sein, um Clients im Leerlauf zu ermitteln. Der Leerlaufstatus ergibt sich aus mehreren Parametern. Der Scan wird nur gestartet, wenn der Endbenutzer den Client für mindestens eine Minute nicht genutzt hat, und niemals in den ersten zehn Minuten nach dem Einschalten. Ist der Benutzer nicht am Computer, generieren aber andere Hintergrundaufgaben CPU- oder E/A-Aktivität, pausiert der Leerlauf-Scan. Andere geplante Aufträge werden ausgeführt, bevor der Leerlauf-Scan startet. Ändert sich einer der Parameter während des Leerlauf-Scans (der Benutzer kehrt an den Client zurück oder ein geplanter Auftrag beginnt), pausiert der Leerlauf-Scan. Sobald die Parameter erneut zutreffen, wird der Scan ab der pausierten Stelle fortgesetzt. Für den Endbenutzer funktioniert ein Leerlauf-Scan genau wie jeder andere geplante Scan. Er läuft im Hintergrund ab und benachrichtigt den Benutzer bei Malware-Fund (falls diese Einstellung aktiviert wurde). Leerlauf-Scans erstellen keinen normalen Bericht, doch jeder Malware-Fund wird wie

üblich im Modul SICHERHEITSEREIGNISSE gemeldet. Nach Abschluss des Leerlauf-Scans aller festgelegten Ordner wird er nach sieben Tagen automatisch erneut gestartet.

Der Leerlauf-Scan kann auf der Registerkarte ALLGEMEIN des Moduls CLIENT-EINSTELLUNGEN aktiviert werden. Wie andere Einstellungen auch kann er für jeden Client aktiviert bzw. deaktiviert werden. Der Leerlauf-Scan sollte für alle Netzwerk-Clients aktiviert und nur dann deaktivier werden, wenn er Leistungsprobleme oder andere Schwierigkeiten verursacht. Der Analyseumfang kann pro Client definiert werden und reicht von allen lokalen Festplatten bis hin zu einzelnen Ordnern. Bei risikobehafteten Clients kann der Leerlauf-Scan so konfiguriert werden, dass er sensible Ordner überwacht. Alternativ kann er manche Aufgaben eines Komplett-Scans übernehmen und alle lokalen Festplatten scannen. Die Einstellungen für den Leerlauf-Scan entsprechen denen des Wächters und werden von der Registerkarte WÄCHTER übernommen. Dies betrifft die Engine-Einstellungen und die Optionen REAKTION AUF INFIZIERTE DATEIEN, INFIZIERTE ARCHIVE und SCANMODUS sowie die Scanner-Spezifikationen NETZWERKZUGRIFFE PRÜFEN, HEURISTIK, ARCHIVE, E-MAIL-ARCHIVE ÜBERPRÜFEN, PRÜFE SYSTEMBEREICHE, AUF DIALER PRÜFEN und BENUTZER BEI VIRENFUND BENACHRICHTIGEN. Da der Leerlauf-Scan ein besonderer Scan ist, werden Ausnahmen aus der Ausnahmenliste für Scans von der Registerkarte ALLGEMEIN übernommen.

9.2. Scans

Geplanter On-Demand-Schutz wird als einzelner oder regelmäßiger Scan ausgeführt. Einzel-Scans werden nur einmal ausgeführt, während regelmäßige Scans gemäß einem Zeitplan wiederholt werden. Beide Scan-Arten können im Modul AUFTRÄGE geplant und verwaltet werden. Wie bei anderen Modulen vom G DATA Administrator gelten die geplanten Aufträge auch für in der Ansicht CLIENTS ausgewählte Clients oder Gruppen. Das Modul zeigt eine Liste der aktuell definierten Aufträge an. Standardmäßig werden alle Auftragsarten, also Backups, PatchManager usw., angezeigt. Für jeden Auftrag werden verschiedene Eigenschaften aufgeführt. Bei Client-Aufträgen wird der Client angezeigt, für den sie definiert wurden (bei Gruppen der Gruppenname). Die Spalte STATUS zeigt den aktuellen Status des Auftrags an. Bei Gruppenaufträgen kann der Status pro Client überprüft werden, indem links der entsprechende Client ausgewählt wird. Wurde ein Scan mindestens einmal ausgeführt, kann die Liste erweitert werden, um verknüpfte Scanprotokolle anzuzeigen. Durch Doppelklicken auf ein Protokoll wird eine detaillierte Ergebnisliste angezeigt. In der Spalte INTERVALL wird das definierte Scanintervall angezeigt, etwa EINMAL für einen Einzel-Scan oder TÄGLICH für einen regelmäßigen Scan, der jeden Tag ausgeführt wird. Unter UMFANG wird schließlich der Scanumfang angezeigt, der für den Auftrag definiert wurde.

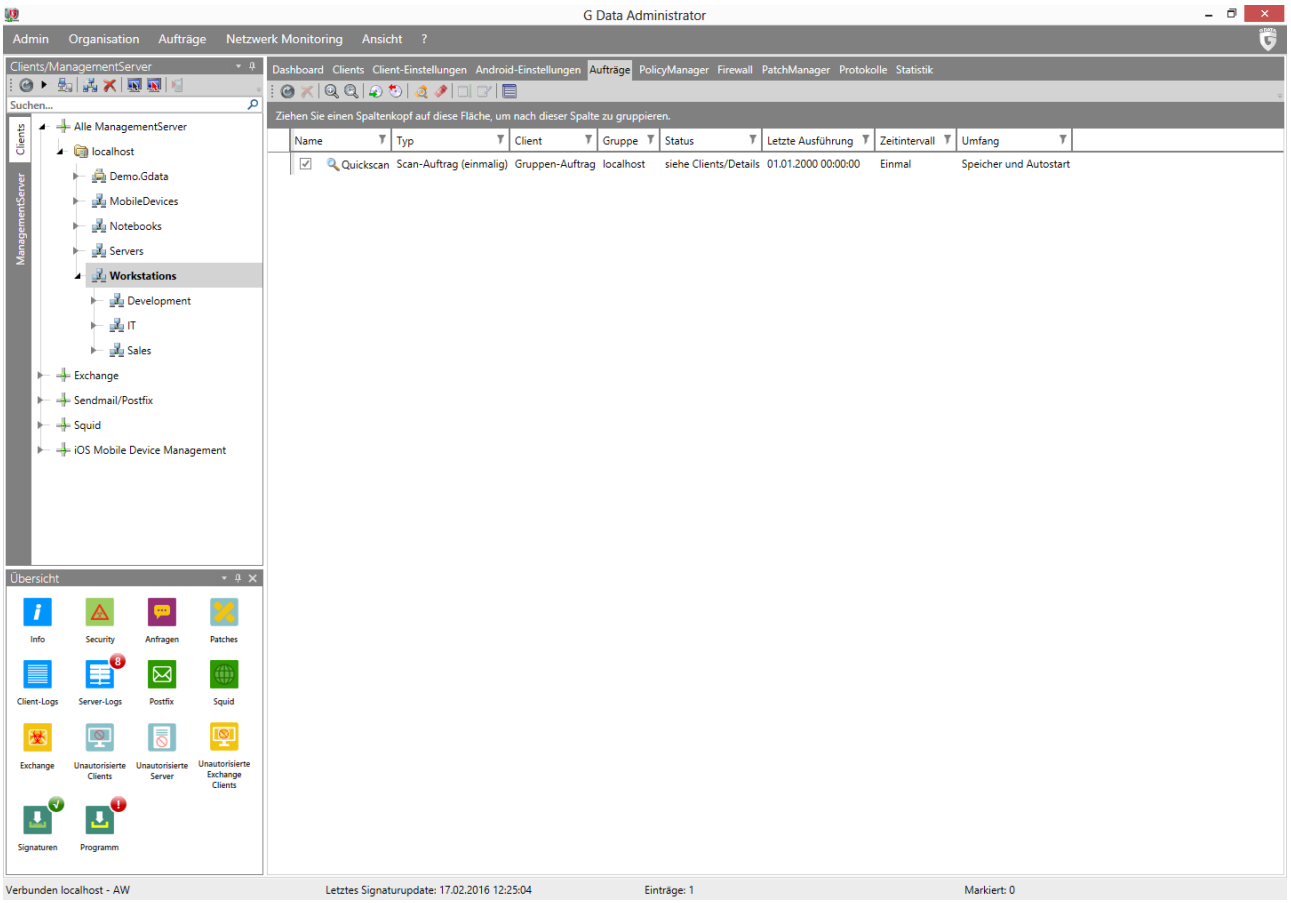

Abbildung 36: G DATA Administrator – Aufträge

Einzelne und regelmäßige Scans können in der Taskleiste durch Klick auf die entsprechenden Schaltflächen definiert werden oder über das Menü AUFTRÄGE und die Optionen HINZUFÜGEN > EINMALIGER SCAN oder PERIODISCHER SCAN (weitere Informationen zum Planen von Scans finden Sie in Abschnitt 9.2.1 und 9.2.2). Nach der Definition des Auftrags wird er sofort in der Liste AUFTRÄGE angezeigt. Die Spalte STATUS enthält den aktuellen Status. Wurde der Auftrag mindestens einmal ausgeführt, werden Datum und Uhrzeit der letzten Ausführung und das Scan-Protokoll angezeigt (durch Klick auf das Plus-Symbol ganz links). Wurde während eines geplanten Scans Malware gefunden, wird automatisch die bei der Definition des Auftrags definierte Aktion ausgeführt. Das Scan-Protokoll zeigt einen Eintrag über die Infektion und dem Modul SICHERHEITSEREIGNISSE wird ein Bericht hinzugefügt (siehe Abschnitt 6.2).

Für einzelne und regelmäßige Scans können einige allgemeine Optionen auf der Registerkarte JOBPLANUNG des Scan-Fensters eingestellt werden. Dem Endbenutzer kann erlaubt werden, einen Scan zu pausieren oder abzubrechen. Unterbricht ein geplanter Auftrag die Arbeit eines Endbenutzers, kann das Pausieren erlaubt werden, um die Arbeit ohne Leistungseinbußen fortzusetzen. Diese Option sollte jedoch mit Bedacht ausgewählt werden: Der Abbruch eines wichtigen geplanten Scans kann die Systemsicherheit gefährden. Der Endbenutzer kann benachrichtigt werden, wenn während eines geplanten Scans ein Virus gefunden wurde. Bei Scans des Dateisystemwächters kann dies zwar nützlich sein (siehe Abschnitt 8.2.1), doch muss der Endbenutzer nicht unbedingt während eines geplanten Scans benachrichtigt werden, da sich der Scanner automatisch um die infizierte Datei kümmert und die Infektion dem Modul SICHERHEITSEREIGNISSE vom G DATA Administrator gemeldet wird. Während des Scans kann der G DATA Security Client alle zwei Minuten seinen Fortschritt dem ManagementServer melden (und so die Details

des Scans im Modul AUFTRÄGE aktualisieren). Dies kann hilfreich sein, um den genauen Fortschritt eines Scans mitzuverfolgen, ist bei wiederkehrenden Scans jedoch nur selten nützlich. Nur wenn ein Einzel-Scan sofort ausgeführt wird, kann die direkte Mitverfolgung der Funde notwendig sein. Clients können nach dem Abschluss eines Scans automatisch ausgeschaltet werden. Automatisches Abschalten ist jedoch nicht möglich, wenn bei Scan-Abschluss ein Endbenutzer am Client angemeldet ist. Hierdurch soll Datenverlust oder anderes, unerwartetes Verhalten verhindert werden. Eine automatische Abschaltung ist meist dann hilfreich, wenn Scans nach einem normalen Arbeitstag oder an Wochenenden geplant sind, also wenn die Clients nach dem Scan nicht direkt verwendet werden. Periodische Scans können hinausgezögert werden, wenn der Client zum geplanten Zeitpunkt nicht eingeschaltet ist. Diese Option stellt sicher, dass kein Auftrag ausgelassen wird. Wird ein Scan übersprungen, könnte eine infizierte Datei bis zum nächsten Scan auf dem System verbleiben und möglicherweise auf andere Systeme übertragen werden. Diese Option sollte nur für regelmäßig ausgeführte Aufträge deaktiviert werden, damit der nächste Auftrag kurz nach dem übersprungenen Auftrag ausgeführt wird. Beinhaltet der Scan eine oder mehrere Netzwerkfreigaben, sollten sie als UNC-Pfad statt als zugeordnete Netzlaufwerke eingegeben werden. Falls das Client-Konto (z. B. Client001$) keine Berechtigung zum Zugriff auf eine Freigabe hat, muss in BENUTZERKONTEXT (OPTIONAL) ein BENUTZERNAME und ein KENNWORT für ein Konto mit den passenden Berechtigungen eingegeben werden.

9.2.1. Periodische Scans

Vor der Planung eines periodischen Scans wird empfohlen, den Scan-Zeitplan als Ganzes zu betrachten. Jeder Netzwerk-Client sollte regelmäßig gescannt werden, aber die Planung eines Einzel-Scans, der jeden Computer im Netzwerk enthält, bietet keine optimale Sicherheit. Geplante Scans für Server sollten sich beispielsweise von denen für Clients unterscheiden, und verschiedene Client-Rollen könnten andere Scan-Einstellungen erfordern. Für einen Client können mehrere Scans geplant werden: z. B. ein täglicher Schnell-Scan und ein wöchentlicher Komplett-Scan. Der Scan-Zeitplan als Ganzes sollte sicherstellen, dass jeder Client regelmäßig gescannt wird. Zusätzlich zum Echtzeitschutz garantieren regelmäßige Scans, dass die Client-Computer vollständig Malware-frei sind. Scans können je nach Anzahl der zu scannenden Dateien jedoch auch zu Leistungseinbußen führen. Daher wird kein täglicher Scan der kompletten Festplatte empfohlen: Er könnte sehr lange dauern, viel CPU-Leistung erfordern und fast konstant auf die Festplatte zugreifen. Für die meisten Clients ist der Leerlauf-Scan die beste Option (siehe Abschnitt 9.1). Wird kein Leerlauf-Scan verwendet, findet ein wöchentlicher Komplett-Scan und ein täglicher Schnell-Scan kombiniert mit dem Client-Echtzeitschutz potenzielle Malware-Infektionen und entfernt sie. Bei Clients mit höherem Infektionsrisiko (z. B. Clients für Downloads aus dem Internet) kann öfter ein Komplett-Scan geplant werden, falls es die Client-Leistung erlaubt. Server, wie z. B. Datei- oder Datenbankserver, könnten stark ausgelastet sein, so dass fast keine CPU-Zyklen für einen Malware-Scan zur Verfügung stehen. Bei dieser Art von Computern könnte es notwendig sein, Scans außerhalb der Geschäftszeiten oder während eines festgelegten Wartungsfensters zu planen.

Für fast jedes Unternehmensnetzwerk sollten mehrere Scans konfiguriert werden. Sie sollten periodisch ausgeführt werden und optional von Einmal-Scans ergänzt werden, um Ausnahmen oder akute Fälle abzudecken. In den folgenden Abschnitten werden die verschiedenen Arten von periodischen Scans erläutert, die als Vorlage für die spezifischen Bedürfnisse eines Unternehmensnetzwerks dienen können. Es gibt keinen Scan, der in jeder Situation geeignet ist. Bei Bedarf müssen die Einstellungen im Unternehmensnetzwerk bis hin zur Netzwerkzone oder auf einzelne Clients angepasst werden. Nachdem

der Auftrag einige Male ausgeführt wurde, sollte überprüft werden, ob er die erwarteten Ergebnisse liefert und die Client-Leistung nicht zu sehr beeinträchtigt.

9.2.1.1. Komplett-Scan

Die erste und wohl wichtigste Art des periodischen Scans ist der Komplett-Scan. Zusätzlich zum Echtzeitschutz sollte jeder Netzwerk-Client regelmäßig durch einen geplanten Scan geprüft werden. Ein Komplett-Scan findet Malware, die nicht durch den Client-Echtzeitschutz erkannt wird. Auch wenn ein Dateisystemwächter jede Malware erkennt, die gelesen, geschrieben oder ausgeführt wird, scannt er nicht proaktiv die Dateien, die auf der Festplatte gespeichert wurden. Wurde eine Datei auf der Festplatte gespeichert, während der Wächter (noch) nicht aktiviert war, erkennt er sie erst beim Versuch, sie zu öffnen oder auszuführen. Da ein Komplett-Scan die gesamte Festplatte scannt, erkennt er Malware, bevor sie ausgeführt wird. Je häufiger ein Komplett-Scan ausgeführt wird, desto höher ist die Sicherheitsstufe und Gewissheit, dass sich keine infizierten Dateien im System befinden. Da der Scan jedoch alle Dateien auf den Festplatten des Systems scannt, schlägt sich ein Komplett-Scan stark auf die Leistung nieder. In den meisten Systemen werden aktive Anwendungen ausgebremst und die Tätigkeiten des Endbenutzers beeinträchtigt. Aus Leistungsgründen ist in den meisten Fällen kein täglicher Komplett-Scan möglich. Clients mit geringem oder mittlerem Risiko können einmal wöchentlich nach den Geschäftszeiten oder am Wochenende gescannt werden. Clients mit hohem Risiko könnten öfter gescannt werden, aber idealerweise nur, wenn der Computer nicht in Gebrauch ist. Auch für Server sollten Komplett-Scans geplant werden. Falls dabei die Leistung ein Problem darstellt, kann der Scan während eines regelmäßigen Wartungsfensters des Servers geplant werden.

Im Modul AUFTRÄGE vom G DATA Administrator kann ein Komplett-Scan als periodischer Scan festgelegt werden. Hierbei müssen die entsprechenden Clients oder Gruppen für den Scan in der Ansicht CLIENTS ausgewählt werden. Das Fenster PERIODISCHER SCAN öffnet sich auf der Registerkarte JOBPLANUNG. Nun werden Tag und Uhrzeit ausgewählt, wann der Scan für die ausgewählten Clients ausgeführt werden soll. Da ein Komplett-Scan viele Ressourcen benötigt und einige Zeit dauern kann, muss der Auftrag so geplant werden, dass er sich mit keinen anderen Aufgaben überschneidet (also periodische oder Einzel-Scans, Backups oder PatchManager-Aufgaben). Auf der Registerkarte SCANNER werden die Parameter festgelegt, mit denen der Scan ausgeführt werden soll. Da ein Komplett-Scan beträchtliche Client-Ressourcen erfordert und immer dann ausgeführt werden sollte, wenn der Client nicht in Gebrauch ist, müssen die Scan-Einstellungen nicht aus Leistungsgründen optimiert werden. Die Einstellungen sollten dennoch für die Clients optimiert werden, für die der Auftrag geplant ist. Die sicherste Scan-Engine-Option ist die Verwendung beider Scan-Engines. Selbst wenn die Client-Leistung während eines Komplett-Scans beeinträchtigt wird, empfiehlt sich die Verwendung beider Engines. Dadurch wird eine optimale Malware-Erkennung sichergestellt. Welche Aktion bei der Erkennung einer infizierten Datei durchgeführt wird, hängt vom Administrator ab. Im Allgemeinen wird eine Desinfektion empfohlen; ist dies nicht möglich, wird die Datei in Quarantäne verschoben. Dadurch wird verhindert, dass false positive Erkennungen sofort gelöscht werden, und die Dateien in Quarantäne könne weiter untersucht werden. Auch infizierte (E-Mail-)Archive können in Quarantäne verschoben werden, erfordern jedoch mehr Aufmerksamkeit. Selbst wenn nur eine Datei oder E-Mail innerhalb eines Archivs infiziert ist, wird das komplette Archiv verschoben. Auch nicht infizierte Dateien, die zusammen mit einer infizierten Datei archiviert wurden, werden in Quarantäne verschoben. Das Löschen eines vollständigen Archivs ist eine noch drastischere Option und wird daher nicht empfohlen. Infizierte Archive können protokolliert

werden und das Modul SICHERHEITSEREIGNISSE muss regelmäßig überprüft werden. Alle Dateien sollten gescannt werden. Durch die Änderung der zu scannenden Dateitypen in NUR PROGRAMMDATEIEN UND DOKUMENTE werden potenziell infizierte Dateien übergangen. Die Scanner-Priorität kann auf „Hoch“ gesetzt werden, falls der Client während des Scans nicht verwendet wird. Dadurch wird die Scan-Dauer erheblich reduziert. Anderenfalls sollte die niedrige oder mittlere Einstellung verwendet werden. Die spezifischen Überprüfungen, wie HEURISTIK, E-MAIL-ARCHIVE, SYSTEMBEREICHE, Dialer und Rootkits, sollten aktiviert werden, um maximalen Schutz zu erzielen. In den Scan können Archive einbezogen werden, aber da sie meist unveränderbar sind, könnten sie durch einen weniger häufigen periodischen Scan abgedeckt werden (siehe Abschnitt 9.2.1.3).

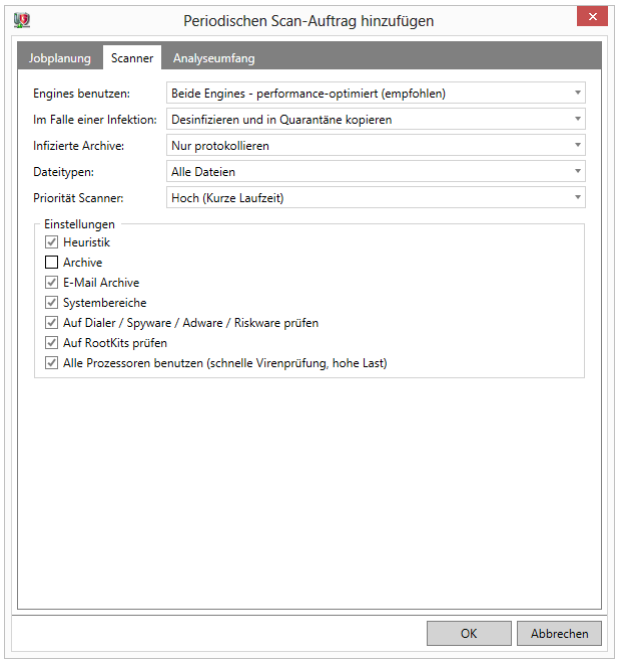

Abbildung 37: G DATA Administrator – Aufträge, neuer periodischer Scan (Komplett-Scan)

Ein Komplett-Scan sollte alle Festplatten umfassen. Durch die Auswahl von FOLGENDE VERZEICHNISSE PRÜFEN können einer oder mehrere zu scannende Ordner ausgewählt werden, um die im Komplett-Scan enthaltenen Ordner differenziert zu steuern. Mit dieser Option können zwar nicht zu scannende Ordnern ausgeschlossen werden, LOKALE FESTPLATTENLAUFWERKE PRÜFEN sollte aber grundsätzlich aktiviert bleiben und eventuelle Ausnahmen sollten im Modul CLIENT-EINSTELLUNGEN definiert werden (siehe Abschnitt 9.3). Der komplette Festplattenscan umfasst einen Arbeitsspeicher- und Autostart-Scan. Da Komplett-Scans meist nicht täglich ausgeführt werden, wird empfohlen, einen zusätzlichen Arbeitsspeicher- und Autostart-Scan festzulegen, der häufiger als der Komplett-Scan läuft (siehe Abschnitt 9.2.1.3).

9.2.1.2. Schnell-Scan

Die zweite Art der wiederkehrenden Scans ist der schnelle Datei-Scan. Dieser Scan sollte so konfiguriert werden, dass er täglich für alle Netzwerk-Clients ausgeführt wird. Auch Server können in den Auftrag einbezogen werden, aber nur, wenn ausreichende Ressourcen zur Verfügung stehen. Bei einem Schnell-Scan werden die Dateien mit dem höchsten Infektionsrisiko überprüft und die Dateien übersprungen, die nicht ausgeführt werden können (und somit keine Gefahr für den Client sind). Weniger Dateien zu scannen, verkürzt die Scan-Dauer erheblich und behält eine ordnungsgemäße Sicherheitsstufe bei. Wie

bei einem Komplett-Scan kann ein Schnell-Scan durch die Auswahl von PERIODISCHER SCAN konfiguriert werden. Ein Schnell-Scan sollte täglich ausgeführt werden (Wochenenden können für Clients ausgelassen werden, die nur in der Woche eingeschaltet und genutzt werden). Der Zeitpunkt, an dem der Auftrag ausgeführt werden soll, ist frei wählbar. Schnell-Scan sind ressourcenschonender als Komplett-Scans, können aber dennoch Leistungseinbußen verursachen (je nach Einstellung auf der Registerkarte SCANNER). Eine Möglichkeit ist die Planung eines Scans während der Mittagspause oder außerhalb der Geschäftszeiten (falls die Clients nicht ausgeschaltet werden). Je nach Konfiguration der Client-Hardware und der Einstellungen für Schnell-Scans könnte ein typischer Endbenutzer die verringerte Leistung nicht bemerken, wodurch die Planung des Scans zu jeder Tageszeit möglich ist.

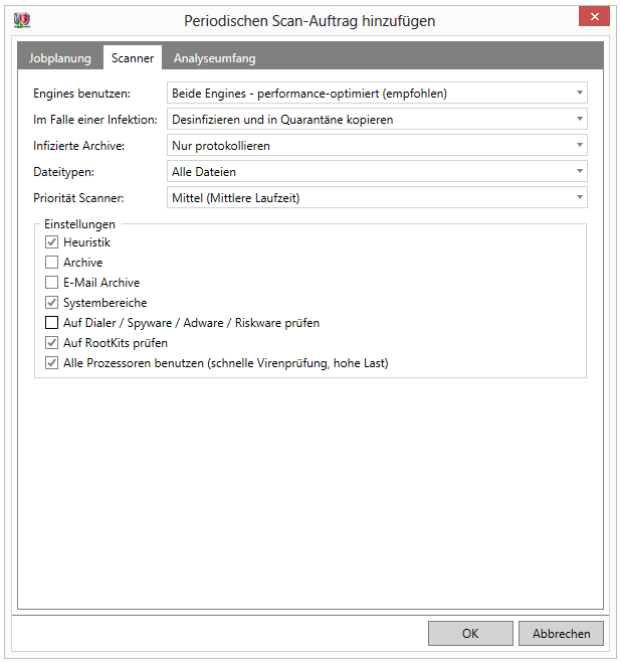

Abbildung 38: G DATA Administrator – Aufträge, neuer periodischer Scan (Schnell-Scan)

Auf der Registerkarte SCANNER können die Arten der auszuführenden Malware-Scans konfiguriert werden. Bei einem Schnell-Scan hängen diese Einstellungen vor allem von der erforderlichen Geschwindigkeit ab. Ein Schnell-Scan soll ein ressourcenschonender täglicher Scan sein, der ausführbare Dateien auf Malware prüft und den Client nicht zu sehr belastet. Die Verwendung beider Scan-Engines wird empfohlen, um optimale Leistung zu erzielen. Führt die Hardware- oder Software-Konfiguration eines Clients während des Schnell-Scans zu Leistungsproblemen, kann der Scan mit nur einer Engine ausgeführt werden. Dadurch verringert sich die Erkennungsrate ein wenig. Wie bei einem Komplett-Scan kann die durchzuführende Aktion bei Fund einer infizierten Datei vom Administrator bestimmt werden. Empfohlen wird eine Desinfektion/Protokollierung. Bei einem Schnell-Scan sollten die DATEITYPEN so gewählt werden, dass NUR PROGRAMMDATEIEN UND DOKUMENTE einbezogen werden. Dadurch werden nur die Dateien gescannt, die durch Ausführen oder Öffnen tatsächlich das System infizieren können. Andere Dateien werden ignoriert, was Zeit spart. Die Scanner-Priorität hängt von den für den Scan-Vorgang verfügbaren Ressourcen ab. Wird ein Schnell-Scan ausgeführt, während ein Endbenutzer wahrscheinlich am Client arbeitet, sollte eine mittlere oder niedrigere Priorität eingestellt werden, um eine normale Leistung zu gewährleisten. Mit dieser Einstellung kann der Scan jedoch länger dauern. Die Priorität kann auf „Hoch“ gesetzt werden, um das schnellstmögliche Ergebnis zu liefern, allerdings beeinträchtigt dies die Rechnerleistung. Ebenso kann die Option ALLE PROZESSOREN BENUTZEN den Scan beschleunigen, was sich

jedoch deutlich in der Leistung bemerkbar macht. Durch Aktivieren der Option HEURISTIK wird der Scan mithilfe der Mustertechnologie ausgeführt, um Malware-Muster zu erkennen. Bei einem Schnell-Scan können ARCHIVE durch Deaktivierung des Kontrollkästchens ignoriert werden: Da sie nicht ausgeführt werden können, müssen sie nicht in einem Schnell-Scan überprüft werden. Das Gleiche gilt für E-MAIL-ARCHIVE. In beiden Fällen muss der Dateisystemwächter für die Clients aktiviert sein, damit die in den Archiven enthaltene Malware bei der Extraktion blockiert wird. Während eines Schnell-Scans sollten SYSTEMBEREICHE geprüft werden. Auch AUF ROOTKITS PRÜFEN sollte aktiviert sein. Beide Optionen schlagen sich nur geringfügig auf die Leistung oder Zeit nieder, sind aber dennoch ein wichtiger Teil des Client-Systems. Zu guter Letzt kann der Scan für Dialer/Spyware/Adware/Riskware aktiviert werden, wenn sie vom Administrator als Malware angesehen werden. Eine Deaktivierung spart Zeit.

Ein Schnell-Scan sollte alle Client-Dateien umfassen. Durch Auswahl der Option LOKALE FESTPLATTENLAUFWERKE PRÜFEN wird der Scan auf der gesamten Festplatte ausgeführt. Ein Schnell-Scan kann auf vordefinierte Ordner, wie den Ordner „Programme“ oder den Windows-Systemordner, beschränkt werden. Dadurch wird die Scan-Dauer reduziert, es entsteht jedoch ein Sicherheitsrisiko, da sich ausführbare Malware-Dateien in jedem Ordner verbergen könnten. Tatsächlich wird oft versucht, der Erkennung durch Verwendung unüblicher Ordner zu entgehen.

9.2.1.3. Andere periodische Scans

Zusätzlich zu den typischen Komplett- und Schnell-Scans gibt es mehrere andere häufige Scan-Arten. Vor allem sollte ein Arbeitsspeicher- und Autostart-Scan geplant werden. Dadurch werden oft angegriffene Windows-Autostart-Bereiche und die aktuell im Arbeitsspeicher ausgeführten Programme überprüft. Diese Maßnahme ist relativ ressourcensparend und kann für alle Netzwerk-Clients geplant werden, indem ein neuer periodischer Scan mit der Einstellung des ANALYSEUMFANGS auf SPEICHER UND AUTOSTART PRÜFEN definiert wird. Normalerweise wird ein Arbeitsspeicher- und Autostart-Scan beim Systemstart ausgeführt. Er kann jedoch auch als stündlicher oder täglicher Auftrag geplant werden. Der Systemstart ist ein guter Zeitpunkt für andere ressourcensparende Scans. Große Scans sollten vermieden werden: Systeme werden normalerweise von einem Endbenutzer eingeschaltet und sollten daher so schnell wie möglich einsatzbereit sein. Eine Startverzögerung durch einen Malware-Scan ist meist nicht akzeptabel. Enthält ein Client jedoch risikobehaftete Dateien oder Ordner, die gescannt werden sollen, kann die Planung eines Auftrags für zusätzliche Sicherheit sorgen, indem die Dateien nach dem Start und vor der Verwendung überprüft werden.

Mit periodischen Scans können Dateitypen und Ordner erfasst werden, die nicht von den regulären Schnell- oder Komplett-Scans überprüft werden. Große Archivdateien werden normalerweise selten geändert. Selbst wenn ein Archiv eine infizierte Datei enthält, ist der Client dennoch sicher: Solange der Dateisystemwächter aktiviert ist, wird die Archivdatei direkt bei Extraktion blockiert. Aufgrund der verschiedenen Schutzebenen können Archivdateien aus Zeitgründen vom dem regulären Komplett-Scan ausgeschlossen werden. Zum Scannen von Archiven kann ein separater periodischer Scan geplant werden. Während der Komplett-Scan normalerweise wöchentlich durchgeführt wird, könnte ein Archiv-Scan so geplant werden, dass er alle zwei Wochen oder einmal monatlich stattfindet. Alternativ können periodische Scans zwischen Komplett- und Schnell-Scans geplant werden, um einen bestimmten Ordner auf Malware zu prüfen. Besonders risikobehaftete Clients können von einem zusätzlichen Scan profitieren (oder einer erhöhten Scan-Häufigkeit des regulären Komplett-Scans).

9.2.2. Einzel-Scans

Scans können so geplant werden, dass sie nur einmal ausgeführt werden. Im Gegensatz zu periodischen Scans werden Einzel-Scans einmal ausgeführt. Anschließend wird ein Bericht gespeichert und der Auftrag wird nicht wiederholt. Einzel-Scans können ein leistungsstarkes Hilfsmittel sein, um Malware zu finden und zu säubern. Bei der Arbeit mit einem Malware-Infektionsbericht (siehe Kapitel 10) kann ein Einzel-Scan für einen bestimmten Ordner schnell darüber Aufschluss geben, ob eine Malware-Infektion vollständig behoben wurde. Wurde eine Infektion beseitigt, kann mit einem Einzel-Scan im Arbeitsspeicher oder Autostart-Bereich des Clients sichergestellt werden, dass keine Spuren hinterlassen wurden.

Wie bei periodischen Scans können auch Einzel-Scans einfach im Modul AUFTRÄGE vom G DATA Administrator verwaltet werden. Die Einstellungen unter JOBPLANUNG sind dabei etwas einfacher als die für periodische Scans. Einzel-Scans können im Voraus mit und ohne Startzeit festgelegt werden. Sie lassen sich bei Bedarf auch direkt ausführen. Ist keine Uhrzeit angegeben, wird der Auftrag für keine bestimmte Zeit geplant, aber in der Übersicht AUFTRÄGE angezeigt. Durch Auswahl des Auftrags und Klicken auf die Symbolleistenschaltfläche SOFORT (ERNEUT) AUSFÜHREN kann er jederzeit ausgeführt werden. Unter EINSTELLUNGEN kann der Administrator die verschiedenen Scan-Parameter definieren. Der Endbenutzer kann den Scan anhalten oder abbrechen. Dies ist zwar bei umfangreicheren Scans hilfreich, während Einzel-Scans naturgemäß so schnell wie möglich ohne Unterbrechung fertig gestellt werden sollten. Ebenso ist es oft nicht notwendig, den Endbenutzer bei Virenfund zu benachrichtigen: Überwacht der Administrator den Auftrag, kann er schnell auf mögliche Malware-Infektionen reagieren. Optional kann der Client direkt nach Abschluss des Scans abgeschaltet werden. Sind nach dem Scan weitere Aktionen notwendig, ist eine Abschaltung weniger praktikabel. Nur wenn der Scan als letzte Aufgabe des Tages ausgeführt wird, kann ein Client automatisch ausgeschaltet werden. Und zu guter Letzt sollte der Client seinen Scan-Fortschritt regelmäßig dem ManagementServer melden, damit ihn der Administrator mitverfolgen kann.

Die SCANNER-EINSTELLUNGEN eines einzelnen Scans sollte an die Umstände angepasst werden. In den meisten Fällen sind beide Scan-Engines sowie die Heuristik und die Rootkit-Überprüfung notwendig, um ein optimales Ergebnis zu erzielen. Die zu scannenden Dateitypen und Bereiche hängen vom Ort der (möglichen) Infektion ab: Alle Dateien, Programmdateien und Dokumente, Archive, E-Mail-Archive und Systembereiche. Alle möglichen infizierten Orte sollten einbezogen werden. In den meisten Fällen ist es am praktischsten, einen vorhandenen Komplett-Scan für die betroffenen Clients auszuwählen und auf SOFORT (ERNEUT) AUSFÜHREN zu klicken, um den Scan außerhalb des Zeitplans auszuführen. Ein kompletter Festplattenscan ist am sichersten, könnte sich jedoch mit einem Komplett-Scan überschneiden. In jedem Fall sollte ein Arbeitsspeicher- und Autostart-Scan durchgeführt werden, um jegliche Malware-Spuren im Arbeitsspeicher aufzudecken.

9.3. Ausnahmen

Es gibt viele Gründe, um Dateien und Ordner aus On-Demand- oder Leerlauf-Scans auszuschließen[13]. Einige Dateien könnten fälschlicherweise als Malware erkannt werden und müssen daher als Ausnahme konfiguriert werden. Ein Schnell-Scan schließt standardmäßig viele Dateitypen und möglicherweise

[13] Weitere Informationen über den Ausschluss von Dateien aus Echtzeit-Scans finden Sie in Abschnitt 8.2.1.

sogar Ordner mit geringem Risiko aus. Ein Komplett-Scan kann Archive oder Datenbankdateien ausschließen, die in einem separaten Scan überprüft werden. Leistung, Uhrzeit oder false positive Ergebnisse können alle gute Gründe sein, um eine Ausnahme zu definieren. Es muss jedoch mit Bedacht entschieden werden, welche Festplatten, Ordner, Dateien oder Dateitypen vom Scan ausgeschlossen werden. Fast alle Datentypen können potenziell Malware enthalten. Jede Datei auf jeder Festplatte sollte mindestens einmal in einem periodischen Scan enthalten sein, egal, ob dies ein schneller, kompletter oder benutzerdefinierter Scan ist. Dabei ist es nicht immer hilfreich, eine Datei mehr als einmal durch verschiedene Aufträge scannen zu lassen. Verschiedene periodische Scans können die gleiche Datei mehrmals durchsuchen, doch das mehrmalige Scannen von großen Teilen der Client-Festplatten ist unnötig.

Wie bei allen Einstellungen gelten auch Ausnahmen für die in der Ansicht CLIENTS ausgewählten Clients oder Gruppen. Die Entscheidung, welche Clients und auf welcher Registerkarte Ausnahmen festgelegt werden, ist sehr wichtig, da hierdurch der Ausnahmeumfang festgelegt wird. Ausnahmen sollten für so wenig Clients wie möglich definiert werden, da unnötige Ausnahmen eine Malware-Infektion begünstigen können. Ordner und Laufwerke können als Ausnahme für einen bestimmten Auftrag definiert werden, indem sie in einem neu erstellten Scan nicht enthalten sind. Ordner, die nur nicht zu scannende Dateien enthalten, können aus einem regulären Schnell- oder Komplett-Scan ausgeschlossen werden, sollten jedoch in einem zweiwöchigen oder monatlichen Auftrag enthalten sein. Alternativ können in der Ausnahmeliste auf der Registerkarte ALLGEMEIN Dateitypen und Ordner als globale Ausnahmen definiert werden, die in keinem Auftrag oder Leerlauf-Scan enthalten sind. Da die in dieser Liste definierten Ausnahmen weitreichend sind, sollten sie nur bei einem ernsthaften Problem hinzugefügt werden, wenn z. B. eine wichtige Datei fälschlicherweise als Malware erkannt wird.

9.4. Lokale Scans

On-Demand-Schutz gibt es nicht nur als zentral verwaltete Maßnahme. Oft ist es hilfreich, wenn der Endbenutzer lokale Scans ausführen darf. Der zentral konfigurierte Wächter scannt zwar bereits Dateien und kümmert sich um mögliche Infektionen, doch können Benutzer, die mit Dokumenten aus nicht verifizierten Quellen arbeiten müssen (z. B. Downloads aus dem Internet oder Dateien von Wechseldatenträgern), mit lokalen Scans die Dateisicherheit zusätzlich verifizieren. Die Berechtigung zum Starten von lokalen Scans kann mit den CLIENT-FUNKTIONEN gewährt werden (siehe Abschnitt 7.4).

Für Windows-Benutzer kann ein lokaler Scan gestartet werden, indem mit der rechten Maustaste auf das Infobereichssymbol von G DATA Security Client geklickt und das entsprechende Scan-Ziel aus dem Menü VIRENPRÜFUNG ausgewählt wird. Im G DATA Security Client für Linux oder Mac wird die Oberfläche durch Klicken auf das G DATA Symbol und Auswahl der Scan-Ziele unter VIRENPRÜFUNG geöffnet. Alternativ kann unter Linux das Eingabeaufforderungstool „gdavclientc-cli“ zur Durchführung eines Scans verwendet werden.

10. Umgang mit einer Malware-Infektion

Egal, wie gut der Endbenutzer über die Risiken von zweifelhaften Websites oder das Öffnen von E-Mail-Anhängen Bescheid weiß: Irgendwann gelangt Malware auf einen Client und versucht ihn zu infizieren. Die verschiedenen Ebenen der G DATA Sicherheitslösung arbeiten zusammen, um die Bedrohung zu blockieren und das System oder Netzwerk vor Schaden zu schützen. Im Modul SICHERHEITSEREIGNISSE wird ein Bericht hinzugefügt und der Administrator optional automatisch benachrichtigt[14]. Obwohl Malware vollständig automatisch blockiert wird, heißt das nicht, dass eine Bedrohung ignoriert werden darf. Der Administrator muss sich über die Bedrohung informieren: Wo kam sie her, was kann sie tun, und wie hoch ist das Risiko, dass sie erneut auftritt?

Der Vorteil einer automatischen Malware-Blockierung ist, dass keine sofortige Aktion auf dem Client ausgeführt werden muss. Eine einzelne Malware-Infektion kann jedoch nur die Spitze des Eisbergs sein: Insbesondere Unternehmensnetzwerke werden oft von ausgetüftelten Bedrohungen angegriffen, die aus mehreren Angriffen mit unterschiedlichen Vektoren bestehen. Der G DATA Administrator bietet hervorragende Protokollierungsfunktionen und Statistikmodule, um Infektionen zu bewerten und zu entscheiden, ob weitere Maßnahmen notwendig sind. Der Ausgangspunkt für jede weitere Analyse ist das Modul SICHERHEITSEREIGNISSE, doch auch andere G DATA Sicherheitsmodule können bei der Untersuchung einer Malware-Infektion und der Vermeidung weiterer Probleme hilfreich sein.

In Unternehmen mit Verfahren zum Risikomanagement oder ähnlichen Maßnahmen kann eine Malware-Infektion mehrere Ereignisse auslösen. Die automatisierte Erkennung, die Behebung und die erweiterte Behebung können zusammengefasst oder geändert werden, um sie an vorhandene Verfahren anzupassen, während die nach der Infektion gesammelten Informationen einen Missbrauch des Angriffsvektors verhindern können.

10.1. Automatische Erkennung und Entschärfung

Die Erkennung von Malware läuft komplett automatisch ab. Erkennt eine der Sicherheitsebenen von G DATA während eines geplanten Scans oder als Ergebnis eines Echtzeit-Sicherheitsmoduls eine Bedrohung, führt sie die zuvor definierte Maßnahme automatisch durch und fügt einen Bericht zum Modul SICHERHEITSEREIGNISSE hinzu. Darum muss die Aktion zuvor festgelegt werden. Zwei Entschärfungswege sollten verfolgt werden: Die Entfernung der Infektion als solche und die Verhinderung einer weiteren Verbreitung im Netzwerk. Die erste Methode kann direkt im G DATA Administratormodul CLIENT-EINSTELLUNGEN konfiguriert werden. Die zweite Methode erfordert eine umfassende Übersicht über die Netzwerk-Clients und ihre Sicherheitseinstellungen (siehe Abschnitt 10.2).

Für jede einzelne Sicherheitsebene kann festgelegt werden, wie sie mit einer Malware-infizierten Datei umgehen soll. Beim Echtzeit-Dateisystemschutz bietet die Registerkarte WÄCHTER die entsprechenden Optionen unter AKTION BEI VIRENFUND. Auf derselben Registerkarte kann die Komponente VERHALTENSÜBERWACHUNG konfiguriert werden. Der E-Mail-Scan lässt sich auf der Registerkarte E-MAIL konfigurieren, während im Modul AUFTRÄGE auf der Registerkarte SCANNER verschiedene Reaktionen für

[14] Alarmmeldungen sollten konfiguriert werden, also E-Mails, die bei einer Malware-Infektion oder eines anderen auslösenden Ereignisses an den Administrator gesendet werden. Weitere Informationen über die (automatische) Überwachung finden Sie in Kapitel 6.

geplante Scans eingestellt werden können. Einige Maßnahmen, wie die Desinfektion und das Verschieben einer Datei in Quarantäne, können miteinander kombiniert werden.

10.1.1. Zugriff blockieren

Die erste Aktion, die bei einer Malware-Erkennung durchgeführt werden sollte, ist die Blockierung der betroffenen Datei, um ihre Ausführung und eine Infektion des Systems zu verhindern. Das ist das absolute Minimum. Wird eine infizierte Datei nicht blockiert, infiziert sie das System. Je nach Art der Malware verursacht dies Instabilität, Leistungsverlust, Datenverlust oder Schlimmeres. Alle G DATA Sicherheitsmodule bieten die Möglichkeit, infizierte Dateien zu blockieren (oder, bei der Verhaltensüberwachung, den Prozess anzuhalten, sobald er verdächtig wird). Wurde eine Datei oder ein Prozess blockiert, sendet der Client einen Bericht an den ManagementServer, wo er die optional konfigurierte Benachrichtigungsprozedur auslöst.

Die Blockierung von Malware verhindert zu dem Zeitpunkt zwar erfolgreich eine Infektion, lässt die Datei selbst aber unverändert. Sie verbleibt auf der Festplatte und könnte später erneut versuchen, das System zu infizieren. Sind die Clients mit G DATA Sicherheitsmodulen geschützt, stellt dies kein Problem dar. Andere Clients, die ungeschützt auf die Datei zugreifen, können sich jedoch infizieren. Deshalb sollte nach der Blockierung einer Datei immer eine zusätzliche Aktion ausgeführt werden: entweder eine Desinfektion, ein Verschieben in Quarantäne oder das Löschen der Datei.

10.1.2. Desinfektion

Malware kann als isolierte Datei auftreten, die ausschließlich zur Infektion von Systemen erstellt wurde. In anderen Fällen besteht sie aus einer oder mehreren Komponenten, die sich an rechtmäßige Dateien anhängen. Dies kann mehrere Zwecke verfolgen. Ein Benutzer öffnet eine infizierte Datei eher, wenn sie nicht infiziert aussieht. Durch das Verstecken eines Malware-Moduls in einem Word-Dokument oder einer ausführbaren Datei eines Drittanbieters ist es wahrscheinlicher, dass ein Endbenutzer sie versehentlich ausführt. Des Weiteren ist die Erkennung von Malware schwieriger, wenn sie in eine harmlose Datei eingebunden ist. Und letztlich bedeutet Malware, die bereits auf dem Client befindliche Dokumente oder Programme manipuliert, ein größeres Risiko für den Endbenutzer, da sie Dateien löschen, verbergen oder verschlüsseln könnte.

Bei der Desinfektion wird versucht, die Malware aus einer Datei zu entfernen, die sie infiziert hat. Nach einer erfolgreichen Säuberung kann die Datei ohne weiteres Infektionsrisiko des Systems wieder verwendet werden. Bei den Sicherheitsmodulen, die diese Option anbieten, ist die Desinfektion die empfohlene Einstellung. Wird Malware erkannt, bewertet das Sicherheitsmodul die Datei und überprüft, ob eine Desinfektion möglich ist. Nicht alle Dateien können gesäubert werden: Manchmal beschädigt Malware Dateien auf irreparable Weise. Besonders schwierig ist die Säuberung von Dateien, die durch Malware manipuliert wurden, aber selbst keine Malware enthalten, wie z. B. verschlüsselte Dokumente. Aus diesem Grund konzentrieren sich die Echtzeitschutzmodule auf die Verhinderung einer Infektion. Die Desinfektion ist eine sehr gute Möglichkeit, eine Infektion zu verhindern, sollte jedoch mit einer Alternative kombiniert werden, falls die Desinfektion fehlschlägt. Bei allen Modulen kann die Desinfektion mit einer anderen Entschärfungsmethode kombiniert werden: Blockieren des Dateizugriffs, Verschieben der Datei in Quarantäne und Entfernen der Datei.

10.1.3. Quarantäne

Die Funktion „Quarantäne“ wird besonders in Kombination mit einer Desinfektion empfohlen. Der geschützte Quarantäne-Ordner funktioniert als Tresor für infizierte Dateien. Jedes Sicherheitsmodul kann die erkannte Malware in Quarantäne verschieben, wo sie umbenannt wird, damit sie nicht zur Ausführung kommt. Der Zugriff auf die Quarantäne ist für Administratoren und Benutzer (falls aktiviert) möglich. Jede Datei in Quarantäne besitzt einen eigenen Bericht im Modul SICHERHEITSEREIGNISSE. Die Liste der Berichte kann über die entsprechende Symbolleistenschaltfläche auf Quarantäneberichte beschränkt werden. Die betroffenen Dateien können gesäubert und aus der Quarantäne wiederhergestellt werden. Löschen ist ebenfalls möglich, indem auf die Symbolleistenschaltflächen geklickt oder aus dem Kontextmenü des Berichts die entsprechende Option ausgewählt wird. Dateien in Quarantäne dürfen nicht ausgeführt werden, bevor sie desinfiziert wurden. Kann eine Datei nicht desinfiziert werden, sollte sie nicht ausgeführt werden, sondern stattdessen in Quarantäne belassen oder gelöscht werden. Die einzige Ausnahme ist eine false positive Erkennung: Wurde eine Datei fälschlicherweise als Malware gekennzeichnet, sollte sie zur Ausnahmeliste des jeweiligen Moduls hinzugefügt und aus der Quarantäne wiederhergestellt werden. Werden verdächtige Dateien auf die Whitelist gesetzt, ist besondere Sorgfalt erforderlich: Das versehentliche Zulassen von Malware auf einem infektionsfreien Client kann schwerwiegende Systemprobleme und Datenverluste verursachen. Dateien in Quarantäne können zur weiteren Analyse an G DATA gesendet werden. Im Falle einer (vermuteten) Vireninfektion kann hierdurch die zukünftige Erkennungsrate verbessert werden. Aufgrund der großen Menge an Dateiübertragungen sind jedoch keine individuellen Antworten möglich.

10.1.4. Datei entfernen

Die Entfernung einer infizierten Datei ist die gründlichste Entschärfungsmethode. Jede Malware wird automatisch gelöscht und kann den Client nicht infizieren oder auf andere Computer verteilt werden. Unternehmen, die auf eine maximale Sicherheit bestehen, können ungeachtet der praktischen Folgen die Sicherheitsmodule so konfigurieren, dass alle infizierten Dateien sofort gelöscht werden. Das ist jedoch nicht die empfohlene Einstellung. Je nach Modul und Scanner-Einstellungen könnten Dateien fälschlicherweise als Malware erkannt werden. Das sofortige Löschen dieser Dateien könnte somit zu Datenverlust führen. In allen Fällen ist die empfohlene Aktion das Verschieben der Datei in Quarantäne, optional kombiniert mit der Desinfektion.

10.2. Erweiterte Entschärfung

Neben den automatischen Maßnahmen, die jedes Sicherheitsmodul ausführt, gibt es mehrere Aktionen, die ein Administrator vornehmen kann. Zunächst kann auf der Client-Seite der Endbenutzer über die Infektion informiert werden. Der Benutzer könnte versehentlich eine infizierte Website, Datei oder andere Ressource geöffnet haben. Die Virenwarnung zeigt ihm, dass der Zugriff auf die Ressource untersagt ist und die Datei in Quarantäne verschoben oder entfernt wurde.

Das Warnfenster kann im Modul CLIENT-EINSTELLUNGEN aktiviert werden, indem die Option BENUTZER BEI VIRENFUND BENACHRICHTIGEN auf der Registerkarte WÄCHTER angeklickt wird. Der Endbenutzer sollte über die Blockierung von Malware unterrichtet werden. Dadurch erfahren sie, dass sie die betroffene Ressource zukünftig meiden müssen. Eventuell können sie dem Administrator weitere Details über den

Infektionsversuch bereitstellen. Bei unerfahrenen Endbenutzern könnte die Meldung jedoch Verwirrung oder Sorge verursachen und zu Support-Anrufen führen. Für diese Benutzer kann die Virenbenachrichtigung deaktiviert werden. Alternativ kann der betroffene Client über die Funktion NACHRICHTEN im Modul CLIENTS manuell benachrichtigt werden. Dadurch kann die an den Endbenutzer gesendete Information besser angepasst werden. Dieser Vorgang ist allerdings nicht automatisierbar. Dadurch vergeht einige Zeit zwischen der Infektion und dem Moment, in dem der Administrator manuell die Nachricht sendet.

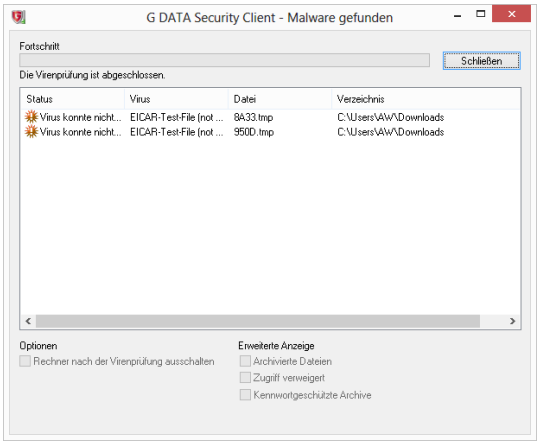

Abbildung 39: G DATA Security Client – Malware gefunden

Ähnliche Argumente für und gegen einen Eingriff durch den Benutzer gelten bei der Frage, ob Benutzer den lokalen Quarantäneordner öffnen dürfen. Diese Option kann im Modul CLIENT-EINSTELLUNGEN aktiviert werden. Damit kann der Benutzer eine vereinfachte Version der Quarantäneberichte anzeigen, die normalerweise nur im Modul SICHERHEITSEREIGNISSE verfügbar sind. Der G DATA Security Client bietet im Kontextmenü des Infobereichs das Fenster QUARANTÄNE. Die Funktion „Quarantäne“ zeigt Datum und Uhrzeit der Infektion, Virusnamen, Dateinamen und Verzeichnis, in dem die Malware gefunden wurde. Der Benutzer kann die betroffenen Dateien desinfizieren, zurück verschieben oder löschen. Im Falle einer false-positive Erkennung kann der Endbenutzer die Datei in Quarantäne ohne Eingreifen des Administrators wiederherstellen. Gleichzeitig zeigt dies, wie riskant die Funktion ist: Möglicherweise noch infizierte Dateien könnten ohne weitere Säuberungsmaßnahmen zurück ins System verschoben werden. Diese Option sollte für alle Clients deaktiviert bleiben. Muss ein Endbenutzer oder der Administrator auf die Quarantäne auf einem Client zugreifen, kann die Option allein für diesen Client aktiviert werden. Dabei muss ein Kennwort abgefragt werden (durch Aktivierung der Option KENNWORTSCHUTZ FÜR DIE ÄNDERUNG VON OPTIONEN im Modul CLIENT-EINSTELLUNGEN).

Auf Serverseite kann der Administrator verschiedene Maßnahmen durchführen, sobald eine Vireninfektion gemeldet wird. Die erste Maßnahme ist es sicherzustellen, dass sich eine mögliche Infektion nicht auf andere Netzwerk-Clients ausbreiten kann. Die Art und Weise, wie eine Verbreitung verhindert wird, hängt von der Schwere der Infektion ab. Bei einfachen, überschaubaren Malware-Infektionen reicht es aus, die Datei in Quarantäne zu verschieben oder zu löschen. Wenn ein Ausbruch das Potential besitzt, weitere Netzwerk-Clients zu infizieren, insbesondere solche, die nicht von einer Sicherheitslösung geschützt sind, sollte der infizierte Client so bald wie möglich vom Netzwerk getrennt werden, indem man seinen Zugriff auf Netzwerkebene (vorübergehend) aufhebt oder ihn physisch trennt. Hierbei muss der Administrator die Untersuchung und Entschärfung der Infektion vor Ort fortsetzen, weshalb diese Maßnahme nur bei akuten Fällen empfohlen wird. In jedem Fall sollte ein

sofortiger Komplett-Scan des betroffenen Clients geplant werden (siehe Abschnitt 9.2.2), in dem Festplatten, Speicher und Autostart auf Spuren von Malware geprüft werden. Bei Verwendung des PatchManager-Moduls (siehe Kapitel 15) sollte der Client auf veraltete Software geprüft werden. Fehlende Patches müssen so schnell wie möglich bereitgestellt werden. Das PolicyManager-Modul hilft dabei, Anwendungen, Geräte oder Webinhalte zu sperren, und lässt sich als Teil einer Unternehmensrichtlinie für Inhalte konfigurieren. Eine Malware-Infektion lässt sich als Ausgangspunkt für eine neue Richtlinie nutzen: Wenn der Angriffsvektor bekannt ist (etwa eine bestimmte Website, ein infiziertes USB-Laufwerk oder ein anderer Wechseldatenträger), kann der PolicyManager diesen in Zukunft blockieren (siehe Kapitel 14).

10.3. Analyse

Nach der ersten Entschärfungsmaßnahme sollte die Malware-Infektion analysiert werden. Diese Vorgehensweise beinhaltet kein striktes Protokoll oder vordefinierte Aktionen. Der Schwerpunkt liegt darauf, Informationen über die Malware zu gewinnen, um künftige Infektionen zu verhindern. Aufgrund von zeitlichen Beschränkungen haben manche Administratoren möglicherweise keine Zeit dafür, andere hingegen werden alle Aspekte der Infektion untersuchen sowie Fakten und Hinweise sammeln. Dabei ist eine Sache wichtig: Die Malware wurde bereits einmal blockiert und wird automatisch blockiert, wenn sie erneut versucht, das System zu infizieren. Die Durchführung einer zusätzlichen Analyse und das Sammeln weiterer Informationen helfen dabei, den Schutzvorgang zu optimieren, sind aber nicht erforderlich. Je mehr Informationen gefunden werden, desto spezifischer sind die zusätzlichen Maßnahmen, die der Administrator ergreifen kann. So kann er beispielsweise bestimmte Websites oder Programme auf die Blacklist setzen oder zusätzliche Scans konfigurieren.

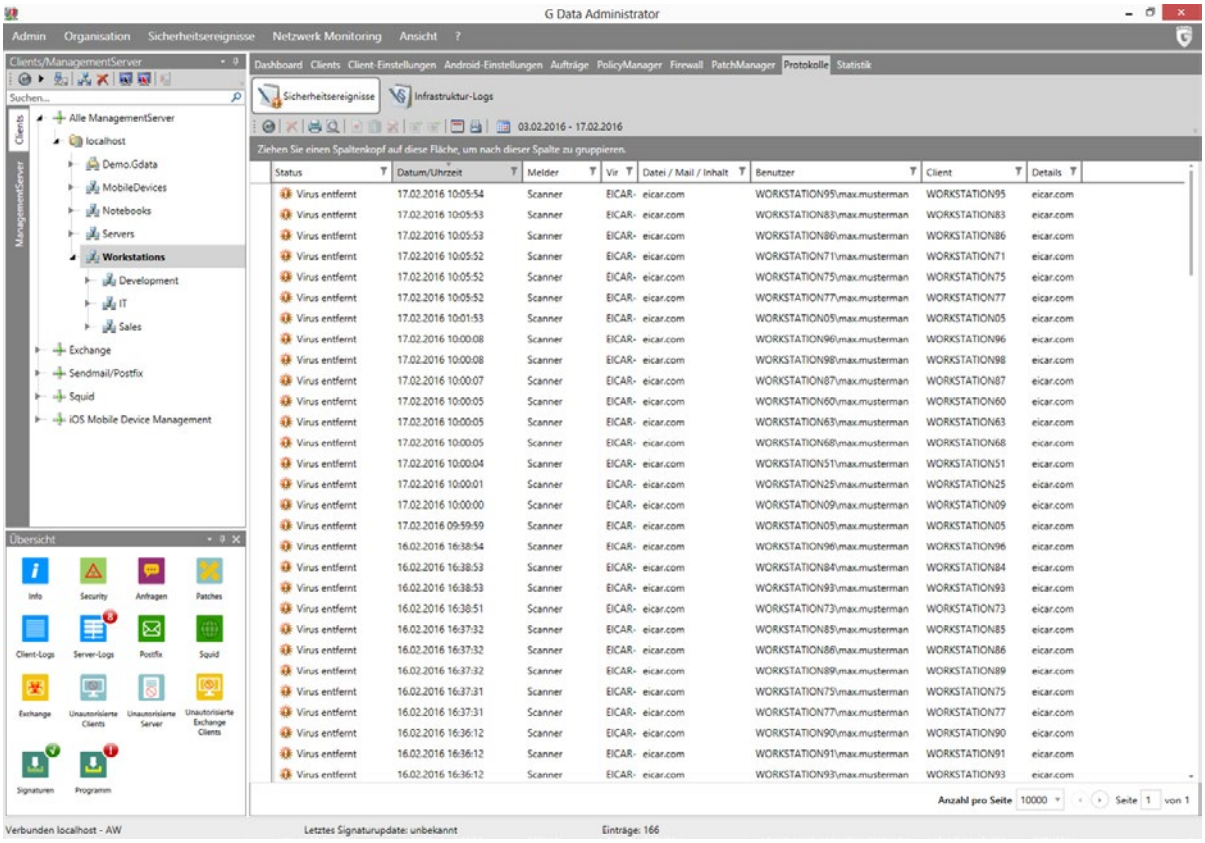

Abbildung 40: G DATA Administrator – Sicherheitsereignisse

Ausgangspunkt für die Untersuchung einer Infektion ist das Modul SICHERHEITSEREIGNISSE. Der Dateiname der infizierten Datei wird zusammen mit dem Ordner, in dem sie gefunden wurde, und dem Namen des Virus aufgeführt. In der Spalte MELDER wird angezeigt, welches Sicherheitsmodul das Virus erkannt hat. Dies hilft bei der Feststellung, wie das Virus versucht hat, den Client anzugreifen. Beispielsweise beziehen sich Berichte des Moduls „Wächter“ auf Dateien, die in das Dateisystem geschrieben oder daraus gelesen wurden. Die meisten Wächter-Erfassungen werden durch Dateien ausgelöst, die von einem externen Gerät (etwa einem USB-Stick) gelesen oder von einem Prozess geschrieben werden (etwa beim Herunterladen einer Datei im Browser). Je nach dem Modul, das das Virus gemeldet hat, können zusätzliche Maßnahmen geplant werden, etwa ein zusätzlicher geplanter Scan, das Hinzufügen einer Website zur Blacklist von PolicyManager oder die Anpassung der WÄCHTER-Einstellungen.

Der Virusname ist ein wichtiger Einstieg in die Informationsfindung. Sowohl der vollständige Virusname als auch seine Familien- oder Kategorienkomponenten können dabei helfen, entscheidende Tipps zum Umgang mit einer Infektion zu finden. Das Modul SICHERHEITSEREIGNISSE zeigt den Virennamen so an, wie er vom Sicherheitsmodul und von der Scan-Engine gemeldet wurde. Der erste Teil des Namens bezieht sich oft auf die Art der Malware: Trojaner, Adware, Generic oder andere. Dies verdeutlicht die Hauptfunktion der Malware und kann möglicherweise klären, wie sie das System infiziert hat. Bei manchen Viren folgt auf den Malwaretyp eine Plattformbezeichnung wie JS (JavaScript) oder VBS (VBScript). Die Plattform definiert die Programmier- oder Skriptsprache, in der die Malware geschrieben wurde oder die sie ausnutzt. Das ist zwar eine wertvolle Information, sie kann aber nicht direkt zum Schließen von Angriffsvektoren genutzt werden. Eine komplette Plattform von der Ausführung auf einem Client-PC zu sperren, ist eine drastische Maßnahme, die üblicherweise eine große Anzahl legitimer Programme beeinträchtigt. Es ist aber (sogar vor der Entdeckung einer Infektion) empfehlenswert, sich die konkreten Sicherheitsoptionen einer Plattform anzusehen und ihre Sicherheitslücken im Auge zu behalten. Zusätzlich zur Plattform enthalten manche Virusnamen einen ausdrücklichen Verweis auf den Bug, den sie ausnutzen. Beispielsweise nutzt Exploit.CVE-2016-1345.Gen die Sicherheitslücke aus, die in der Datenbank „Common Vulnerabilities und Exposures“ (CVE) unter dem Eintrag 2016-1345 beschrieben ist. Einträge in der CVE-Datenbank können extrem hilfreich dabei sein, Informationen über bekannte Sicherheitslücken und die Methoden zu ihrer Entschärfung herauszufinden. Das Ministerium für Innere Sicherheit der Vereinigten Staaten pflegt eine CVE-Datenbank unter http://nvd.nist.gov, die kostenlosen Zugriff auf die aktuellsten CVE-Rundschreiben gibt. Der restliche Virusname besteht üblicherweise aus einem Freiformnamen, der von einer der identifizierenden Eigenschaften dieser konkreten Malware übernommen wurde. Der Name variiert oft von einem Antivirusanbieter zum anderen, kann aber dabei helfen, eine Online-Suche nach zusätzlichen Informationen zu starten.

11. Mobile Device Management

Unternehmensnetzwerke bestehen nicht nur aus PCs. Um die gestiegene Vernetzung zu unterstützen, haben viele Unternehmen damit begonnen, ihren Mitarbeitern Mobilgeräte wie Tablets und Smartphones auszuhändigen. Andere erlauben ihren Mitarbeitern, bei der Arbeit ihre eigenen Geräte zu nutzen. Ressourcen und Informationen auf Mobilgeräten verfügbar zu machen, ermöglicht es den Mitarbeitern, auch außerhalb ihrer traditionellen Arbeitsumgebung produktiv zu sein. Dies bringt aber auch Risiken mit sich. Mobile Angriffe können die Gerätesicherheit gefährden und zu Datendiebstahl oder beschädigten Geräten führen. Diese Art von Bedrohung gilt noch mehr für Netzwerke, mit denen sich auch nicht verwaltete Geräte verbinden dürfen. Privaten Mitarbeitergeräten den Zugriff auf Unternehmensressourcen zu erlauben, könnte eine mögliche Option zur Erhöhung der Produktivität bei gleichzeitiger Senkung der Gerätekosten sein. Dies erfordert jedoch eine strikte Sicherheitsrichtlinie, um Malware-Infektionen im Unternehmensnetzwerk zu verhindern.

Mobile Device Management ist in jeder G DATA Lösung enthalten. Mobilgeräte werden über die gleiche Schnittstelle wie andere Clients verwaltet: Der G DATA Administrator führt die Mobilgeräte in seiner Ansicht CLIENTS auf und die Konfiguration erfolgt mit demselben modularen System, mit dem auch die Windows- und Linux-Clients verwaltet werden.

11.1. Android

Ähnlich wie beim Schutz von PCs werden auch Android-Geräte mit einer agentenbasierten G DATA Lösung geschützt. Mit der App „Internet Security für Android“ lassen sich Malware-Schutz, Berechtigungen, Diebstahlschutzoptionen und Kontakte zentral verwalten.

11.1.1. Verwalten von Android-Geräten

Android-Geräte werden mit der entsprechenden Funktion in der Symbolleiste der Ansicht CLIENTS bereitgestellt und erscheinen automatisch, sobald die Client-App installiert wurde und ihre erste Verbindung mit dem ManagementServer hergestellt hat. Weitere Informationen zur Installation von Android-Geräten finden Sie in Abschnitt 4.8.4. Der Gerätename kann auf der Registerkarte ANDROID-EINSTELLUNGEN geändert werden. Eine zusätzliche ANMERKUNG hilft dabei, die verschiedenen Clients zu unterscheiden. Da Android-Geräte in der Liste als Clients erscheinen, können sie in Gruppen verschoben werden. Idealerweise lassen sich alle Geräte in derselben Gruppe mit derselben Richtlinie verwalten, und alle Geräte, die diese Richtlinie nutzen, werden derselben Gruppe hinzugefügt. Wie bei normalen Clients können je nach Netzwerkzonen und Client-Rollen mehrere Arten von Gruppen definiert werden (siehe Abschnitt 7.1). Eine logische Klassifizierung würde darin bestehen, die Android-Geräte je nach Unternehmensabteilung zu einer Gruppe hinzuzufügen. Bei Nutzungsszenarien, die Abteilungsgrenzen überschreiten, ist die Gruppierung der Geräte je nach ihrer Nutzung eine Alternative.

Besonders in einer Umgebung, in der jeder sein eigenes Gerät mitbringt, ist es wichtig, eine Verwaltungszuständigkeit festzulegen. Bei Geräten, die vom Unternehmen ausgegeben wurden, sollte die volle Zuständigkeit für die Geräteverwaltung bei den Administratoren des Unternehmensnetzwerks liegen. Bei Geräten, die von den Mitarbeitern erworben wurden, lässt sich die Grenze aber möglicherweise nicht so klar ziehen: Können Mitarbeiter dazu gezwungen werden, Geräte zu sichern, die nicht dem Unternehmen gehören? Die G DATA Geräteverwaltung löst dieses Problem mit

Konfigurationsprofilen. Für jedes Gerät bzw. jede Gruppe lässt sich unter ANDROID-EINSTELLUNGEN > RICHTLINIEN ein TELEFON-TYP definieren. Je nach TELEFON-TYP wird ein spezifisches Konfigurationsprofil auf das Gerät angewendet. Bei der Wahl von UNTERNEHMEN verwendet das Gerät Einstellungen aus dem Unternehmensprofil, das über den G DATA Administrator verwaltet wird. Endbenutzer haben keinen Zugriff auf die Einstellungen. Dies ist die empfohlene Einstellung für Unternehmensgeräte. Wenn PRIVAT eingestellt ist, nutzt das Gerät sein lokales Konfigurationsprofil und die Endbenutzer dürfen Einstellungen auf dem Gerät selbst konfigurieren. Diese Einstellung sollte verwendet werden, wenn das Gerät nicht vom Unternehmen ausgegeben wurde und kein Rechtsanspruch auf die Verwaltung des Geräts besteht. Die Einstellung GEMISCHT lässt die Benutzer frei zwischen den Konfigurationsprofilen „Unternehmen“ und „Privat“ wechseln.

Besonders bei der Verwendung des Unternehmensprofils sollten die Endbenutzer darüber informiert werden, dass ihr Gerät per Fernzugriff verwaltet wird und der Administrator sich für die Ergreifung weitreichender Maßnahmen entscheiden kann, etwa die Blockierung des Zugangs zum Gerät oder sogar die Löschung der Daten auf dem Gerät (im Zusammenhang mit Diebstahlschutzmaßnahmen, siehe Abschnitt 11.1.6). Zu diesem Zweck bietet das Modul CLIENTS die Möglichkeit, dass Internet Security einen Endbenutzer-Lizenzvertrag (EULA) anzeigt, dem der Endbenutzer zustimmen muss. Im Menü CLIENTS können Administratoren die EULAs unter EULAVERWALTUNG verfassen und verwalten. Es können beliebig viele Verträge erstellt werden. Wenn ein Android-Client ausgewählt ist, kann ein EULA zugewiesen oder entfernt werden, indem die Option ZUGEWIESENE EULA ÄNDERN oder ZUGEWIESENE EULA LÖSCHEN aus dem Menü CLIENTS ausgewählt wird.

Vor der Konfiguration spezifischer Richtlinien zur Geräteverwaltung sollten der Update-Plan und die Synchronisation definiert werden. Beide Einstellungen hängen vom Nutzungsmuster für das Gerät ab. Geräte, die oft mit einem drahtlosen Netzwerk verbunden werden, können so konfiguriert werden, dass sie ihre Virensignaturen automatisch aktualisieren und alle paar Stunden die Daten mit dem ManagementServer synchronisieren. Geräte, die hauptsächlich außerhalb des Unternehmensnetzwerks genutzt werden oder sich über einen Mobildatentarif mit dem Internet verbinden, können so konfiguriert werden, dass Updates weniger häufig, manuell oder nur bei einer WLAN-Verbindung stattfinden. Das Gleiche gilt für die Synchronisation: Es lassen sich verschiedene Einstellungen für WLAN- und Mobildatentarife konfigurieren.

11.1.2. Echtzeit- und On-Demand-Schutz

Ebenso wie Desktop- und Laptop-Clients sind auch Android-Clients anfällig für Malware-Infektionen. Insbesondere gerootete Geräte haben keine ausreichenden Mechanismen zum Schutz vor schädlichen Apps aus unbekannten Quellen. Vielmehr kann es schwerwiegende Folgen haben, wenn es bösartige Apps schaffen, sich in die offiziellen App-Stores einzuschleichen. Außerdem können Websites versuchen, Malware bereitzustellen, Sicherheitslücken im Betriebssystem auszunutzen oder den Endbenutzer auf andere Weise zu täuschen. Aus diesem Grund bietet „Internet Security für Android“ einen Echtzeit- und On-Demand-Schutz. Die Registerkarte ALLGEMEIN des Moduls ANDROID-EINSTELLUNGEN enthält Optionen für alle Sicherheitsmodule.

Der WEB-SCHUTZ bietet Echtzeitschutz bei der Nutzung des Android-Browsers. Diese Einstellung sollte aktiviert bleiben. Da der Web-Schutz einen geringen Datenverkehr produziert, lässt er sich so konfigurieren, dass er nur bei einer WLAN-Verbindung des Geräts arbeitet. Die zweite Komponente des

Echtzeitschutzes ist die automatische Virenprüfung, die durch die Auswahl von BEI APP-INSTALLATION unter VIRENPRÜFUNG aktiviert wird. Beim Herunterladen und Starten einer App wird diese von der Virenprüfung transparent auf Malware geprüft und die Installation blockiert, wenn sich die App als schädlich herausstellt.

Der On-Demand-Schutz ist in Form einer vollständigen Virenprüfung des gesamten Geräts verfügbar. Damit Internet Security das Gerät regelmäßig scannt, muss unter VIRENPRÜFUNG die Option BEI APP-INSTALLATION aktiviert werden. Es können zwei Arten von Scans konfiguriert werden: SYSTEM (KOMPLETTER SCAN) oder INSTALLIERTE ANWENDUNGEN. Solange das Gerät vom Scan nicht zu sehr ausgebremst wird, ist eine regelmäßige Systemüberprüfung empfehlenswert, um sicherzugehen, dass sich keine Malware auf Speichermedien (etwa einer SD-Karte) befindet. Je nachdem, wie oft das Gerät benutzt und wie oft neue Software darauf installiert oder gespeichert wird, kann das Intervall auf 1 Tag, 3 Tage, 7 Tage, 14 Tage oder 30 Tage eingestellt werden. In den meisten Fällen ist eine tägliche Überprüfung empfehlenswert: Der Scan verursacht keine spürbaren Verzögerungen und sorgt für maximale Sicherheit. Um sicherzugehen, dass durch die Virenprüfung die Batterie nicht entladen wird, kann sie so konfiguriert werden, dass sie nur während des Aufladens des Geräts stattfindet. Alternativ kann der AKKUSPARMODUS gewählt werden, damit der Scan verschoben wird, wenn sich das Gerät im Energiesparmodus befindet. Dies schont die Batterie, öffnet aber ein Sicherheitslückenfenster, in dem vorhandene Malware unbemerkt bleiben kann.

11.1.3. Geräterichtlinien

Bei Android-Geräten kommt die größte Bedrohung von gerooteten Geräten. Wenn der Endbenutzer einen Root-Zugriff auf das Gerät erhalten hat, kann jede Form von Sicherheit auf der Betriebssystem- oder App-Ebene mühelos untergraben werden, und wenn es die Malware schafft, das Gerät zu infizieren, gewinnt sie einen praktisch unbegrenzten Zugriff auf die Funktionen des Betriebssystems. Um die Kontrolle über verwaltete Android-Geräte zu behalten, sollte daher gerooteten Geräten der Netzwerkzugriff verweigert werden. Dazu kann der Administrator im Bereich POLICIES des Moduls ANDROID-EINSTELLUNGEN die SSID, das KENNWORT und die VERSCHLÜSSELUNG des Unternehmens-WLAN definieren. Wenn GEROOTETE GERÄTE ERLAUBEN nicht aktiviert ist, werden gerootete Geräte, auf denen Internet Security installiert ist, mit dem Fernwartungskennwort (siehe Abschnitt 11.1.6) blockiert und der Zugang zum WLAN wird verweigert.

Zusätzlich zum Blockieren gerooteter Geräte bietet die Registerkarte POLICIES noch weitere Einstellungen. Der Administrator kann für jedes Gerät den Kamerazugriff aktivieren oder deaktivieren (für Geräte mit Android 4.0 und höher). Zum Schutz der auf dem Telefon gespeicherten Daten kann eine Verschlüsselung verlangt werden. Wenn VERSCHLÜSSELUNG ERFORDERLICH (Android 3.0 und höher) ausgewählt ist, öffnet das Gerät automatisch das Android-Fenster mit Verschlüsselungseinstellungen, damit der Benutzer die Verschlüsselung aktivieren kann. Das Fenster lässt sich erst schließen, wenn eine Verschlüsselung aktiviert worden ist.

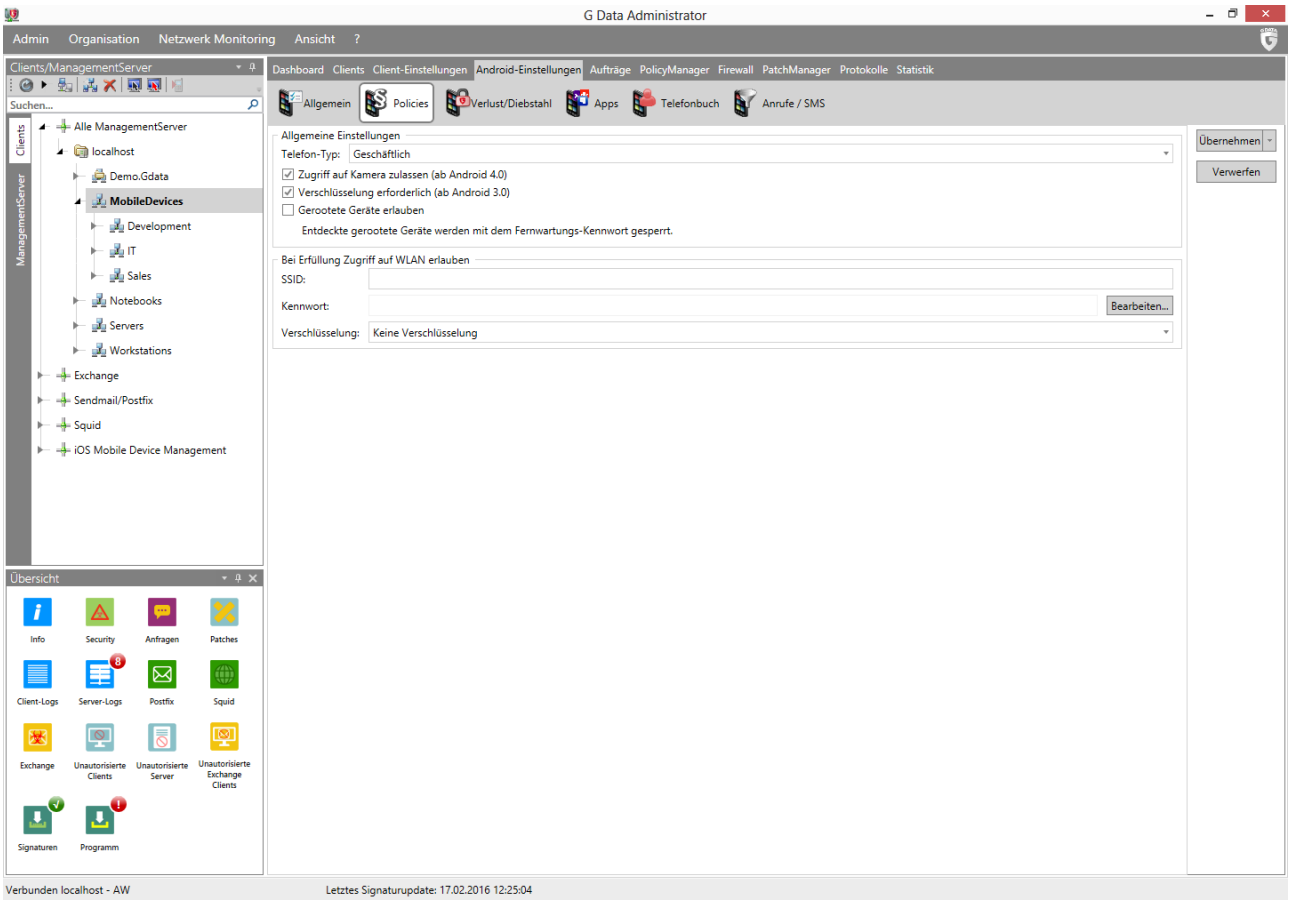

Abbildung 41: G DATA Administrator – Android-Einstellungen, Policies

11.1.4. Apps

Die Attraktivität von Mobilgeräten besteht zum Teil auch darin, dass sich ihre Standardfunktionen durch das Installieren von Apps erweitern lassen. Auch in einem Unternehmensumfeld kann das extrem praktisch sein: Produktivitätstools oder Konfigurationsapps können die Anzahl der Anwendungsfälle für Mobilgeräte deutlich erhöhen. Gleichzeitig sollten Unternehmensgeräte eine kontrollierte Umgebung bieten und dafür sorgen, dass Apps keine Kompatibilitätsprobleme verursachen, sensible Daten abrufen oder Malware verbreiten können. Die App-Verwaltung ist eine leistungsstarke Möglichkeit, die Funktionalität eines Android-Geräts zu kontrollieren und dabei Sicherheit mit Benutzerfreundlichkeit in Einklang zu bringen. Die Administratoren sollten jederzeit wissen, welche Apps auf verwalteten Android-Geräten ausgeführt werden, und diese nach Bedarf blockieren oder zulassen.

Das Modul ANDROID-EINSTELLUNGEN bietet auf der Registerkarte APPS durchdachte Möglichkeiten der App-Verwaltung. Als erster Schritt kann sie für eine Inventur der Apps verwendet werden, die auf Android-Geräten im Netzwerk in Gebrauch sind. Jede installierte App wird mit Name, Version und Größe aufgeführt. Für jede App sollten die Administratoren Informationen über ihren Anbieter, ihre Funktionen und ihre Versionsgeschichte einholen, insofern Informationsquellen verfügbar sind. Bei vielen Apps liefert der offizielle App-Store genügend Einzelheiten, bei anderen kann es erforderlich sein, sich die Homepage des Anbieters anzusehen. Auf der Grundlage dieser Informationen und der beabsichtigten Nutzung des Geräts (je nach Gerätegruppe, -typ und -netzwerkzone) können Apps der Whitelist oder der

Blacklist hinzugefügt werden. Dadurch werden die aufgeführten Apps zugelassen bzw. blockiert. Bei Verwendung des definierten Kennworts wird die Ausführung der Apps blockiert.

Die Nutzung der Black- oder Whitelist hängt davon ab, ob das Gerät komplett gesperrt werden soll. Wenn es das Ziel ist, nur ein paar bekannte schlechte Apps zu blockieren, dem Benutzer aber eine relative Freiheit zu lassen, reicht die Arbeit mit der Blacklist aus. Es sollten aber zumindest die App „Android-Einstellungen“ und Internet Security selbst kennwortgeschützt sein. Dies wird den Endbenutzer daran hindern, unerlaubte Änderungen an den Einstellungen vorzunehmen. Indem der offizielle App-Store auf die Blacklist gesetzt wird, ist gewährleistet, dass keine weiteren Apps installiert werden können. Um die Apps eines Geräts vollständig zu kontrollieren, ist die Arbeit mit der Whitelist die zuverlässigste Möglichkeit. Apps auf der Whitelist können ohne Einschränkungen genutzt werden, aber alle anderen Apps sind gesperrt. Das ist besonders praktisch für Geräte, die für maximale Sicherheit oder einen einzigen Workflow konfiguriert sind. Beispielsweise kann ein Gerät, das nur von Vertriebsmitarbeitern genutzt werden soll, im Whitelist-Modus betrieben werden, sodass nur die Telefonkomponente und die Vertriebsdatenbank-App genutzt werden können.

11.1.5. Kontaktverwaltung und -filterung

Bei Geräten, die in einer Unternehmensumgebung genutzt werden, kann es von entscheidender Bedeutung sein, Kommunikationsströme zu kontrollieren. Das Blockieren von Apps kann helfen, wenn eine Kommunikation vollständig verhindert werden soll, in manchen Szenarien sollte aber besser ein feinerer Filter eingesetzt werden. Anstatt die Telefon-App komplett zu sperren, wenn ein Gerät nur für berufliche Kommunikation genutzt werden soll, könnten aus- und eingehende Anrufe auch gefiltert werden, wenn sie die Unternehmenskriterien nicht erfüllen. Beispielsweise könnte ein Unternehmen, das seine Mitarbeiter mit Telefonen ausstattet, damit diese von unterwegs aus mit dem Hauptsitz kommunizieren können, alle Anrufe blockieren, die nicht an einen im Voraus genehmigten Unternehmenskontakt gehen bzw. von diesem kommen. Für die Verwaltung der Kontakte auf dem Telefon kann das Unternehmenstelefonbuch genutzt werden. Auch ohne die Nutzung von Filtermöglichkeiten kann das Blockieren des eingebauten Gerätetelefonbuchs und das Befüllen des Unternehmenstelefonbuchs von Internet Security ein effektiver Weg sein, um die Kontrolle über die Kontaktdaten zu gewährleisten.

Die Registerkarten TELEFONBUCH und ANRUFE / SMS des Moduls ANDROID-EINSTELLUNGEN bieten zusammen umfassende Möglichkeiten zur Kontaktverwaltung und -filterung. Die Basis aller Funktionen ist die Kontaktdatenbank. Sie fungiert als zentraler Knotenpunkt für alle Unternehmenskontakte, auf deren Grundlage sich Telefonbücher für verschiedene Geräte ebenso wie gezielte Anruf- und SMS-Filter anlegen lassen. Die Datenbank kann im Modul TELEFONBUCH oder ANRUFE / SMS mithilfe der Option KONTAKTDATENBANK ANZEIGEN geöffnet werden. Kontakte können durch Klicken auf die entsprechende Schaltfläche in der Symbolleiste manuell hinzugefügt werden. Das Fenster KONTAKT bietet Eingabefelder für Name, Adresse, E-Mail/Fax/Telefon und Unternehmen. Für Unternehmen mit einer begrenzten Anzahl von Kontakten oder für kleine verwaltete Telefonbücher ist die manuelle Eingabe von Kontakten eine praktische Möglichkeit, die Kontaktdatenbank schnell zu befüllen. Wenn das Netzwerk Active Directory nutzt, können über die Schaltfläche KONTAKTE IMPORTIEREN die Kontaktdaten auch importiert werden. Für einen Import aller Kontakte der Domäne muss die entsprechende Domäne ausgewählt und auf OK geklickt werden. In der Übersichtsliste der KONTAKTDATENBANK können die importierten Kontakte bearbeitet oder

entfernt werden. Wenn die Datenbank mit allen notwendigen Kontaktdaten befüllt worden ist, wird der Vorgang mit SCHLIEßEN beendet. Nachdem alle Kontakte in der KONTAKTDATENBANK definiert worden sind, können diese auf die entsprechenden Geräte verteilt werden. Beispielsweise können alle Geräte mit einer vollständigen Liste der Durchwahlnummern von Kollegen versorgt werden. Alternativ kann Gerätegruppen – kombiniert mit einer Sperre der standardmäßigen Telefonbuch-App und der Nutzung des Moduls ANRUFE / SMS – der Zugriff nur auf bestimmte, ausdrücklich bereitgestellte Telefonnummern im Telefonbuch gewährt werden.

Das Modul ANRUFE / SMS kann zur umfassenden Filterung der ein- und ausgehenden Kommunikation genutzt werden. Es funktioniert wie ein Filter des eingebauten Gerätetelefonbuchs. Anstatt die Android-Telefonbuch-App komplett zu sperren, ermöglicht der Filter eine differenzierte Kontrolle der Kommunikationsströme. Durch die Aktivierung des Whitelist-Modus werden beispielsweise nur solche ein- oder ausgehenden Anrufe zugelassen, bei denen die entsprechenden Telefonnummern auf der Whitelist stehen. Im Blacklist-Modus ist die Kommunikation generell zulässig, aber es können bestimmte Nummern blockiert werden.

11.1.6. Verlust/Diebstahl

Um zu gewährleisten, dass auf E-Mails oder Dokumente des Unternehmens und andere Unternehmenskommunikation nicht zugegriffen werden kann, wenn ein Gerät verloren geht oder gestohlen wird, können verschiedene Diebstahlschutzmaßnahmen definiert werden. Zunächst könnte ein Versuch reichen, das Gerät wiederzufinden. Dabei kann es helfen, das Gerät mit GPS-Technologie zu orten oder einen Alarmton auszulösen. Wenn die Ortung des Geräts nicht möglich ist oder keine verwertbaren Ergebnisse liefert, kann das Gerät gesperrt und so für einen Dieb wertlos gemacht werden. Als letzter Ausweg kann man Geräte auf die Werkseinstellungen zurücksetzen, wodurch alle Daten auf dem Gerät gelöscht werden.

Das Modul ANDROID-EINSTELLUNGEN bietet Zugang zu Maßnahmen bei VERLUST/DIEBSTAHL. Sie können automatisch oder manuell ausgelöst werden. Um alle Maßnahmen zu aktivieren, müssen verschiedene Einstellungen konfiguriert werden. Ein FERNWARTUNGS-KENNWORT (ein numerischer PIN-Code) sollte eingegeben werden. Es wird als Kennwort beim Senden von SMS-Befehlen und als Bildschirmsperrenkennwort genutzt, wenn kein Bildschirmsperrenkennwort ausdrücklich definiert worden ist. Es sollte eine VERTRAUENSWÜRDIGE TELEFONNUMMER eingegeben werden, um zu gewährleisten, dass nicht jeder einen Befehl zum Zurücksetzen des Kennworts senden kann. Ein solcher Befehl wird nur ausgeführt, wenn er von der vertrauenswürdigen Telefonnummer gesendet wird. Schließlich wird die E-MAIL-ADRESSE FÜR BENACHRICHTIGUNGEN eingegeben, um gegebenenfalls Rückmeldungen von den Aktionen zu erhalten.

Wenn ein Gerät verloren geht oder gestohlen wird, lässt sich eine Aktion darauf am einfachsten ausführen, indem man dem Gerät eine SMS-Nachricht schickt. Unter ERLAUBTE SMS-KOMMANDOS lassen sich die Befehle aktivieren oder deaktivieren, die an das Gerät gesendet werden können. Zum Auslösen der entsprechenden Maßnahme wird eine SMS-Nachricht mit folgendem Befehl an das Gerät geschickt:

Befehl	Maßnahme
Kennwort locate	Gerät orten. Das Gerät meldet seinen Standort per SMS. Wenn unter E-MAIL-ADRESSE FÜR BENACHRICHTIGUNGEN eine E-Mail-Adresse eingegeben wurde, werden die Standortdaten auch an diese gesendet.

Kennwort wipe	Persönliche Daten löschen. Alle persönlichen Daten werden gelöscht.
Kennwort ring	Signalton abspielen. Das Gerät gibt einen Klingelton wieder, bis Internet Security gestartet wird.
Kennwort mute	Gerät lautlos schalten. Es werden alle Klingeltöne mit Ausnahme desjenigen lautlos geschaltet, der von der Alarmtonoption ausgelöst wird.
Kennwort lock	Bildschirmsperre mithilfe des Bildschirmsperrenkennworts aktivieren. Wenn kein Bildschirmsperrenkennwort definiert wurde, wird das Fernwartungskennwort verwendet.
Kennwort set device password: *neuesKennwort*	Bildschirmsperrenkennwort festlegen. Legt das Kennwort fest, das zum Sperren des Geräts genutzt wird. Das Gerät wird dadurch nicht automatisch gesperrt: Anschließend muss noch der Sperrbefehl gesendet werden.

Der erste Teil des Befehls (*Kennwort*) ist das FERNWARTUNGSKENNWORT. Bei Bedarf kann es per SMS zurückgesetzt werden. Dazu wird über die VERTRAUENSWÜRDIGE TELEFONNUMMER folgender Befehl gesendet: remote password reset: **neuesKennwort**.

Bei einem Gerätediebstahl wird häufig die SIM-Karte entfernt, damit der ursprüngliche Besitzer das Gerät nicht über seine Telefonnummer kontaktieren kann. Als Gegenmaßnahme können Aktionen definiert werden, die bei einem Wechsel der SIM-Karte automatisch stattfinden. Der Sperrbildschirm des Telefons kann aktiviert werden, sodass ein Zugriff auf das Gerät nicht mehr möglich ist und das Gerät geortet werden kann. Dadurch wird eine E-Mail mit den GPS-Koordinaten an die Adresse geschickt, die unter E-MAIL-ADRESSE FÜR BENACHRICHTIGUNGEN definiert wurde. Diese Maßnahmen müssen deaktiviert werden, wenn ein Wechsel der SIM-Karte erforderlich ist – beispielsweise dann, wenn ein Gerät nicht mehr genutzt oder einem anderen Mitarbeiter zugewiesen wird.

Zusätzlich zu SIM- und SMS-basierten Maßnahmen lassen sich auch über den G DATA Administrator verschiedene Aktionen einleiten. Wenn eine Maßnahme sofort ausgelöst werden muss, kann die NOTFALLFUNKTION verwendet werden. Das Gerät muss dafür keine SMS-Nachrichten erhalten können oder mit dem ManagementServer-Netzwerk verbunden sein: Es stützt sich auf Firebase Cloud Messaging (FCM), einen Online-Dienst von Google, mit dem man Befehle an Android-Geräte schicken kann. Dieser Dienst erfordert die Registrierung eines Google-Kontos, um einen Server-Key und eine Sender-ID für FCM zu erhalten. Weitere Informationen finden Sie auf der FCM-Website[15]. Im G DATA Administrator müssen der API-KEY (FCM: Server-Key) und die SENDER-ID unter ALLGEMEINE EINSTELLUNGEN > ANDROID eingegeben werden.

Wenn SENDER-ID und API-KEY konfiguriert sind, lässt sich über die Schnittstelle vom G DATA Administrator mühelos eine Notfallaktion auslösen. Dazu müssen in der Ansicht CLIENTS das Gerät, auf dem die Maßnahme ausgelöst werden soll, und die entsprechende Aktion ausgewählt werden. Durch Klicken auf FUNKTION AUSFÜHREN wird der Befehl an das Gerät geschickt und unverzüglich ausgeführt. Die Befehle funktionieren genauso wie die, die per SMS ausgelöst werden können.

11.2. iOS

Im Unterschied zu Android-Geräten benötigen iOS-Geräte keine App, um geschützt zu sein. Die Installation eines iOS-MDM-Profils (für iOS 7.0 und höher verfügbar) ermöglicht es den Administratoren, Einschränkungen für Apps, Funktionen und Inhalte sowie für Passcodes und drahtlose Netzwerke zu erzwingen.

[15] Siehe https://firebase.google.com.

11.2.1. Verwalten von iOS-Geräten

iOS-Geräte werden mit der entsprechenden Funktion in der Symbolleiste der Ansicht CLIENTS bereitgestellt und erscheinen automatisch, sobald der Endbenutzer die MDM-Anfrage über die Installations-E-Mail geöffnet hat (weitere Informationen zur Bereitstellung von iOS-Geräten können dem Abschnitt 4.8.5 entnommen werden). Wenn im G DATA Administrator ein iOS-Gerät ausgewählt wird, stehen mehrere iOS-MDM-Module zur Verfügung.

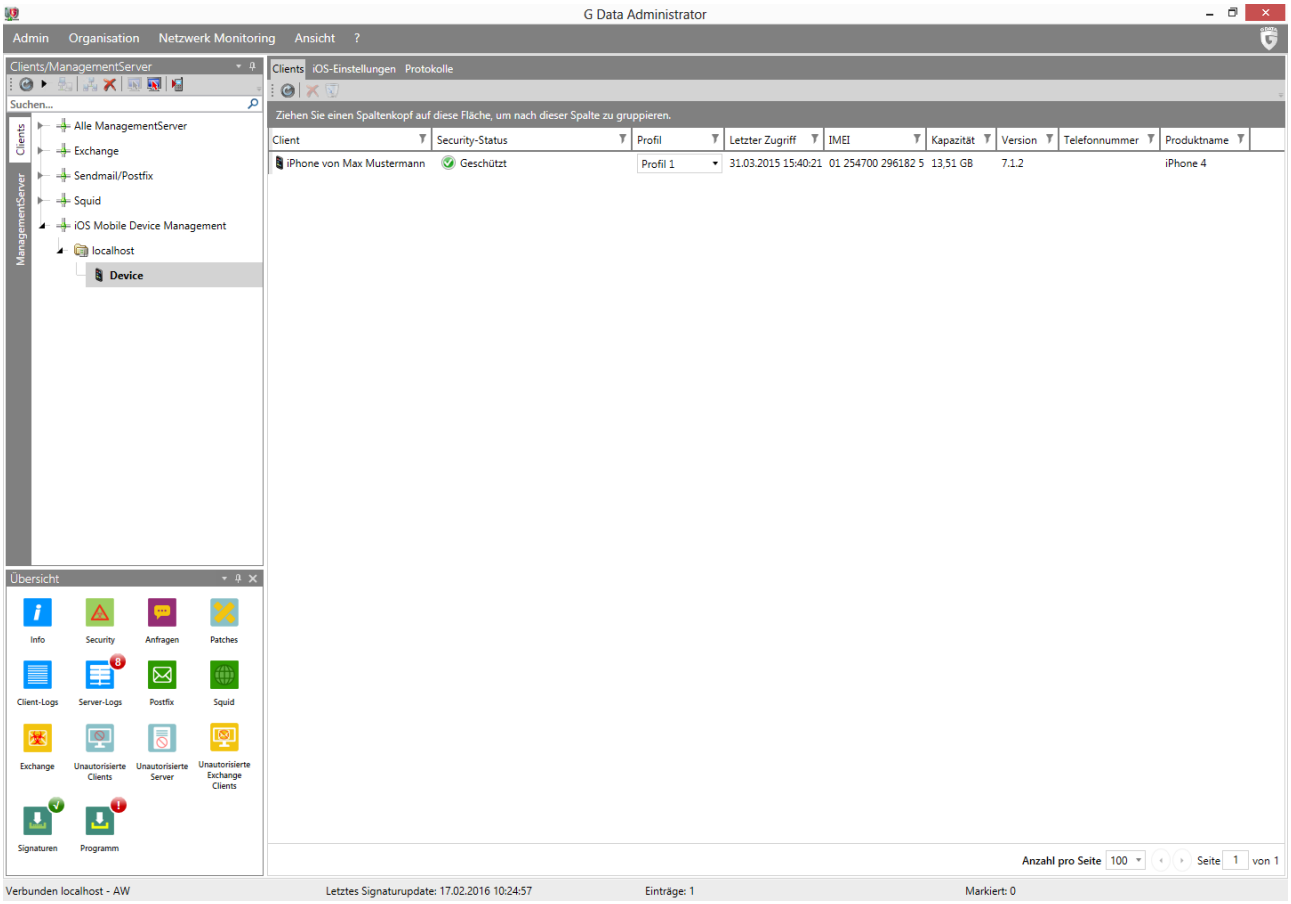

Abbildung 42: G DATA Administrator – Clients (iOS)

Auf der Registerkarte CLIENTS (iOS) erscheint eine Übersicht aller verwalteten iOS-Geräte. Für jeden Client werden mehrere gerätespezifische Merkmale angezeigt, etwa seine IMEI-Nummer, die iOS-Version und der Produktname. In der Spalte SECURITY-STATUS erscheinen Warnungen für Geräte ohne Richtlinienprofil (siehe Abschnitt 11.2.2) sowie Meldungen zum MDM-Installationsstatus, denn das MDM-Konzept von Apple ermöglicht es Endbenutzern, die MDM-Lösung ohne die Genehmigung eines Administrators von einem Gerät zu entfernen. Für Geräte ohne aktive MDM-Lösung (weil sie vom Administrator oder Endbenutzer entfernt wurde oder weil die Installation nicht genehmigt wurde), kann der Installationslink über das Kontextmenü erneut verschickt werden.

Beim Entfernen von Geräten aus der iOS-Geräteverwaltung muss unbedingt zuerst die MDM-Lösung deaktiviert werden. Das Gerät sollte nur entfernt werden, wenn die Spalte SECURITY-STATUS bestätigt, dass die MDM-Lösung deaktiviert worden ist. So wird verhindert, dass sich Geräte nicht mehr verwalten lassen – beispielsweise dann, wenn sie von der Liste entfernt werden, bevor das Gerät den Befehl zur Deaktivierung der MDM-Lösung erhalten hat. Die Kommunikation zwischen dem G DATA ActionCenter

und den iOS-Geräten erfolgt über Push-Nachrichten. iOS-Geräte müssen einen WLAN-Zugang oder eine SIM-Karte mit Datentarif haben, um Push-Nachrichten empfangen zu können. Ohne Datentarif oder WLAN-Zugang kann das Gerät nicht vollständig aktiviert oder verwaltet werden. Einige iOS-Gerätezustände können den Empfang von Push-Nachrichten stören, wodurch sich die Ausführung von MDM-Befehlen verzögert. Um eine korrekte Kommunikation zu gewährleisten, sollte das Gerät aufgeladen sein und sich nicht im Ruhemodus, Nicht-stören-Modus oder Flugmodus befinden. Der Status der verschiedenen Push-Nachrichten lässt sich mit dem (iOS-)Modul PROTOKOLLE nachverfolgen. Die Berichte enthalten Bestätigungen des Profilbereitstellungsstatus und der Diebstahlschutzfunktion. Die Anzahl der Berichte ist auf 1.000 begrenzt. Wenn diese Grenze erreicht ist, werden zuerst die ältesten Berichte entfernt.

11.2.2. Geräterichtlinien

Bei der Nutzung von iOS-Geräten in einer Unternehmensumgebung müssen bestimmte Funktionen gesperrt werden, um zu gewährleisten, dass sensible Daten geschützt sind und die Geräte nur für produktive Zwecke genutzt werden. Geräte- und App-Einstellungen, Inhalte und WLAN-Zugang lassen sich mithilfe von Richtlinienprofilen steuern.

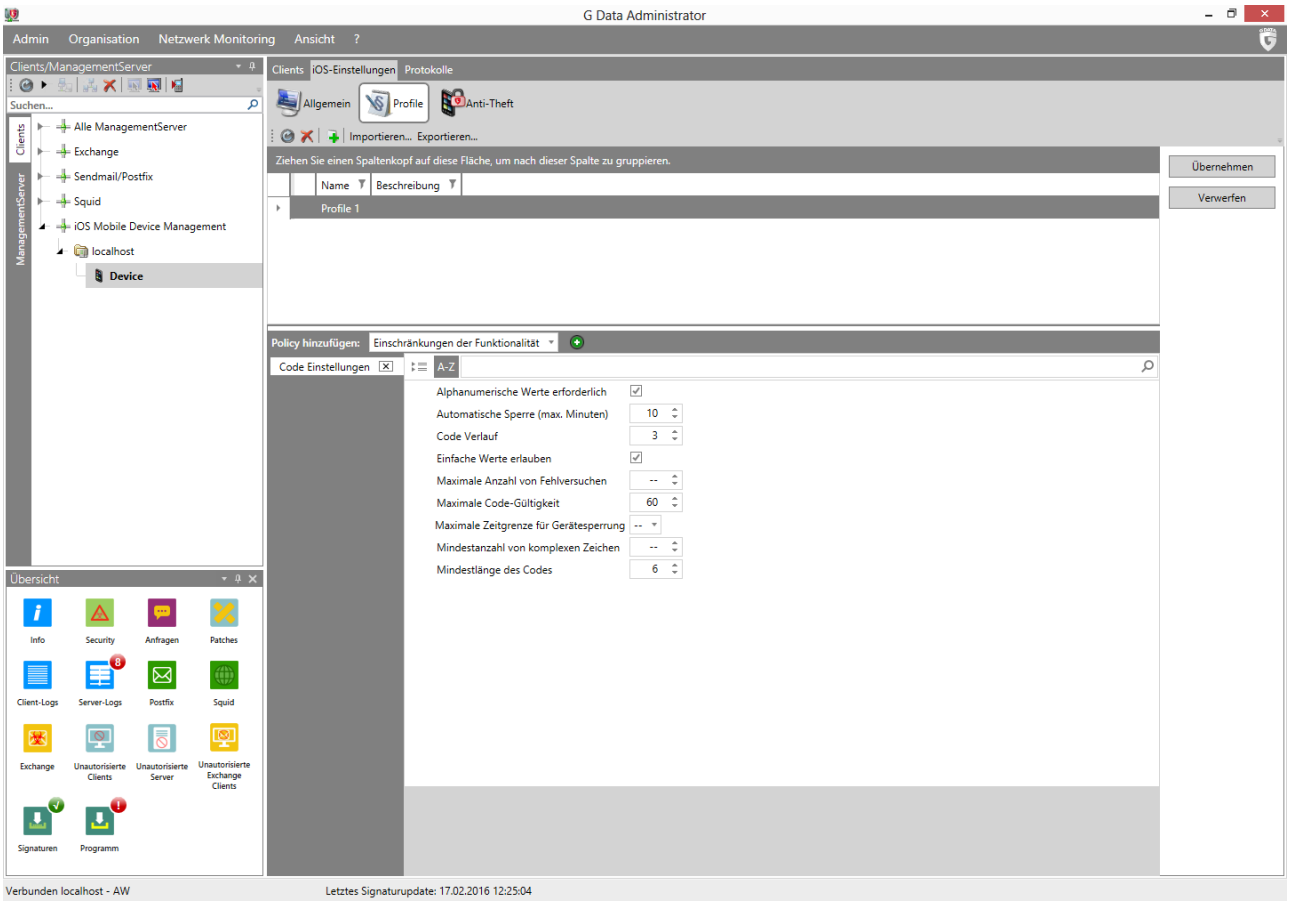

Abbildung 43: G DATA Administrator – iOS-Einstellungen, Profile

Wie bei Android-Geräten hängt die empfohlene Richtliniennutzung vom Zugriff auf sensible Daten und dem Grad der Freiheit ab, die der einzelne Endnutzer haben soll. Wenn Geräte beispielsweise auf das Unternehmensnetzwerk bzw. auf Unternehmensdaten zugreifen dürfen, sollte sichergestellt sein, dass sich auf dem Gerät keine Apps befinden, die sensible Daten gefährden könnten. Die Anzahl der

Einschränkungen hängt auch davon ab, ob das Gerät vom Unternehmen ausgegeben wurde oder einem Mitarbeiter gehört. Die Endbenutzer werden wahrscheinlich keine strenge Verwaltung ihrer privaten Geräte zulassen, bei Unternehmensgeräten kann jedoch eine Reihe strikter Richtlinien eingesetzt werden.

Der G DATA Administrator ermöglicht die Verwaltung der Richtlinienprofile über die Registerkarte PROFILE. Ein Profil besteht aus bis zu fünf Richtlinien, die thematisch gruppierte Einstellungen enthalten. Mit der Richtlinie APP-EINSCHRÄNKUNGEN können Administratoren zum Beispiel den iTunes Store deaktivieren und die Richtlinie CODE EINSTELLUNGEN schreibt Mindeststandards für den Passcode des Geräts vor. Nach dem Hinzufügen von Richtlinien kann ein Profil mithilfe des Moduls CLIENTS (iOS) oder der Registerkarte ALLGEMEIN des Moduls IOS-EINSTELLUNGEN einem oder mehreren iOS-Geräten zugewiesen werden. Dies ermöglicht einheitliche Einstellungen auf allen Geräten.

Die Wahl der Geräterichtlinien liegt beim Administrator und hängt von den Sicherheitsanforderungen des Unternehmens ab. Dennoch können einige Empfehlungen ausgesprochen werden. Wenn das Gerät keinen Passcode besitzt, ist die Sperrbildschirmfunktion unzureichend, die sich durch das Modul DIEBSTAHLSCHUTZ auslösen lässt. Um zu gewährleisten, dass das Gerät im Falle eines Diebstahls gesperrt werden kann, sollte die Richtlinie CODE EINSTELLUNGEN angewendet werden, welche die Nutzung des Passcodes erzwingt. Da die MDM-Implementierung von Apple den Endbenutzern erlaubt, die MDM-Lösung lokal auf iOS-Geräten zu deaktivieren, empfiehlt sich die Nutzung von einer oder mehreren WLAN-Richtlinien, um zu verhindern, dass die Benutzer die Richtlinien beliebig umgehen. Durch die Kombination einer WLAN-Richtlinie mit anderen Richtlinien sind die Endbenutzer gezwungen, die anderen Richtlinien zu akzeptieren, wenn sie weiterhin auf das drahtlose Netzwerk zugreifen möchten. Beispielsweise kann dem drahtlosen Unternehmensnetzwerk ein WPA/WPA2-Kennwortschutz hinzugefügt werden, damit Geräte nicht darauf zugreifen können. Anschließend kann dem MDM-Profil eine WLAN-Richtlinie hinzugefügt werden, die den Netzwerknamen und die Anmeldedaten enthält. Dadurch ist gewährleistet, dass nur iOS-Geräte mit diesem Profil auf das Netzwerk zugreifen können. Wenn ein Endbenutzer versucht, eine Inhaltsrichtlinie durch Deaktivierung der MDM-Lösung zu umgehen, werden nicht nur die Einschränkungen entfernt, sondern auch der Zugang auf das Unternehmens-WLAN, wodurch die weitere Nutzung des Geräts sehr unpraktisch wird.

11.2.3. Diebstahlschutz

Wenn ein Gerät verloren geht oder gestohlen wird, muss als erstes dafür gesorgt werden, dass niemand auf die Daten auf dem Gerät zugreifen kann. Danach kann es per GPS geortet werden (um das Gerät zu finden und zurückzuholen) oder es kann die drastischere Maßnahme ergriffen werden, die Daten auf dem Gerät zu löschen (falls es keine Möglichkeit gibt, das Gerät zu finden und zurückzuholen).

Mit dem Modul IOS-EINSTELLUNGEN kann der Administrator die Diebstahlschutzfunktionen direkt auf der Registerkarte DIEBSTAHLSCHUTZ auslösen. Die Funktionen zum Sperren und Zurücksetzen des Geräts können ausgelöst werden, indem die entsprechende Option ausgewählt und auf FUNKTION AUSFÜHREN geklickt wird. Dabei ist zu beachten, dass die Gerätesperre nur den Sperrbildschirm aktiviert. Wenn kein Passcode festgelegt worden ist, lässt sich der Sperrbildschirm mühelos deaktivieren (siehe Abschnitt 11.2.2). Für Geräte, die mit einem unbekannten Passcode gesperrt worden sind, wird die Option KENNWORTSPERRE ENTFERNEN verwendet.

12. Backups

Das Backup-Modul ist optional verfügbar.

In vielen Unternehmen hat die Digitalisierung von Arbeitsabläufen Computer zu unternehmensweiten Informationsträgern ernannt. Der Zugriff auf digitalisierte Daten ist viel einfacher, als regelmäßig auf Papierarchive zugreifen zu müssen, bringt aber auch seine eigenen Herausforderungen mit sich. Datensicherheit und Datenintegrität müssen sorgfältig überwacht werden. Physische Probleme wie ein Stromausfall oder eine kaputte Festplatte können für Workflows schwerwiegende Folgen haben, besonders dann, wenn sich die Dateien nicht wiederherstellen lassen. Malware kann Dateien verschlüsseln, infizieren oder entfernen, und Dokumente können durch menschliches Versagen entfernt werden. Es ist wichtig, Datei-Backups und die Wiederherstellung sorgfältig zu planen, um die Wiederherstellungszeit nach einem Datenvorfall zu minimieren. Wenn regelmäßig Backups erstellt werden, indem Dateien an einen sicheren Ort kopiert werden, ist gewährleistet, dass Dateien niemals unwiderruflich verloren gehen. Genau wie bei der Entschärfung von Infektionen liegt der Schlüssel auch hier in der Vorausplanung. Wenn Dateien aufgrund eines physischen Problems oder menschlichen Versagens verloren gehen, sollten sie ohne Verzögerung wiederhergestellt werden. Die Erstellung eines Backup- und Wiederherstellungsplans, der sicherstellt, dass die Dateien regelmäßig per Backup gesichert werden, ist unerlässlich, um die Geschäftskontinuität zu gewährleisten.

Ein Backup- und Wiederherstellungsplan ist teils Vorsorge, teils Wiederherstellung. Als Ausgangspunkt kann es hilfreich sein, alle Datenquellen im Netzwerk nach Eigenschaften wie Wert, Risiko oder Backup-Aufwand zu klassifizieren. Wenn das Unternehmen Informationsarbeiter beschäftigt, die den Großteil ihrer Zeit mit der Arbeit an digitalen Dokumenten verbringen, sollten diese Dokumente immer gesichert werden. Ebenso sollten Backups von zentralen Datenspeichern wie Datenbanken, Mail-Servern oder Kooperationsumgebungen erstellt werden, um sicherzustellen, dass im Notfall keine Daten verloren gehen. Im Gegensatz dazu sind manche Daten austauschbar. Das Betriebssystem eines Clients benötigt normalerweise kein Backup, denn es kann bei einer Datenbeschädigung neu installiert werden. Gleiches gilt für Software-Pakete, deren Installationsmedien noch verfügbar sind. Die Konfiguration des Betriebssystems und Software-Einstellungen können hingegen zu den Daten gehören, von denen ein Backup erstellt werden sollte, wenn nach der Installation eine umfangreiche individuelle Anpassung erfolgt ist. Für jede Entscheidung über die Daten, die in Backups enthalten sein sollen, muss Speicherplatz zur Verfügung stehen. Besonders dann, wenn Datensätze regelmäßig per Backup gesichert werden oder große Dateien enthalten, kann der Speicherbedarf exponentiell ansteigen.

Wenn die Daten für das Backup ausgewählt worden sind, stellt sich die Frage, wie oft das Backup durchgeführt werden soll. Backup-Aufträge lassen sich so planen, dass sie nur einmal oder gemäß einem Zeitplan ausgeführt werden. Ein einmaliges Backup ist nur unter ganz bestimmten Umständen hilfreich, etwa dann, wenn ein Datensatz unverzüglich und außerhalb des definierten Zeitplans gesichert werden muss. In den meisten Fällen sollte ein Backup geplant werden. Es sollte jederzeit eine aktuelle Kopie der zu sichernden Daten verfügbar sein, um im Notfall eine schnelle Wiederherstellung zu ermöglichen. Ein geplantes Backup kümmert sich darum. Wenn es einmal konfiguriert ist, gibt es immer eine aktuelle Datenkopie. Man muss anschließend nur noch regelmäßig die Protokolle überprüfen, ob das Backup erfolgreich ausgeführt wurde. Es gibt eine Abwägung von Sicherheit und Leistung. Je öfter Backups erstellt werden, desto weniger Daten gehen verloren, wenn die Festplatte eines Clients beschädigt ist oder Dateien durch Malware infiziert werden. Die Durchführung eines Backups erfordert aber Zeit und

Leistung (Festplattenaktivität) auf dem Client sowie Speicherplatz auf der Festplatte des Backup-Ziels (Server). Dieses Problem wird meistens dadurch behoben, dass man differenzielle Backups verwendet (siehe Abschnitt 12.2).

Es muss aber überprüft werden, ob das Backup-Ziel jederzeit über genügend Festplattenspeicher verfügt. Da Backups ein wesentlicher Teil einer Sicherheitsrichtlinie sind, sollte sichergestellt sein, dass sie erfolgreich verlaufen. Wie bei den meisten IT-bezogenen Aufgaben empfiehlt es sich, eine Person oder ein Team mit der Aufgabe der Planung, Verwaltung und Durchführung von Backups zu beauftragen. Mit einem verantwortlichen Mitarbeiter bzw. Team lassen sich im Notfall schneller Entscheidungen treffen. Wenn ein Administrator oder Endbenutzer einen Datenverlust meldet, sollte der Workflow für rasche Entscheidungen und effektive Datenwiederherstellung optimiert werden.

12.1. Verwalten von Backups

Die nahtlose Integration ermöglicht eine Administration über die Module AUFTRÄGE und SICHERHEITSEREIGNISSE im G DATA Administrator und sorgt dafür, dass sich Konfiguration und Verwaltung der Backups mühelos durchführen lassen. Backup-Aufträge können auf der Registerkarte AUFTRÄGE geplant und verwaltet werden. Wie bei jedem Modul gelten alle Aufträge für den Client oder die Gruppe, der bzw. die in der Ansicht CLIENTS ausgewählt wurde(n). Die Spalten der Liste enthalten die wichtigsten Merkmale der Aufträge und lassen sich nach Client, Gruppe, Status, letzte Ausführung, Intervall, Umfang oder Name sortieren. Bei Client-Aufträgen wird der Client angezeigt, für den sie definiert wurden (bei Gruppen der Gruppenname). Die Spalte STATUS zeigt den aktuellen Status des Auftrags an. Bei Gruppenaufträgen kann der Status pro Client überprüft werden, indem links der entsprechende Client ausgewählt wird. In der Spalte INTERVALL wird das definierte Backup-Intervall angezeigt, etwa EINMAL für einen einzigen Backup-Auftrag oder TÄGLICH für einen regelmäßigen Backup-Auftrag, der jeden Tag ausgeführt wird. Unter UMFANG wird schließlich der Backup-Umfang angezeigt, der für den Auftrag definiert wurde. Wenn ein Backup-Auftrag schon zuvor ausgeführt worden ist, kann er erweitert werden, sodass für jede Ausführung eine Liste von Statusmeldungen angezeigt wird. Durch einen Doppelklick auf den Status lässt sich ein detailliertes Protokoll öffnen.

Die Backup- und Wiederherstellungsaufträge haben individuelle Einstellungen, es gibt aber auch einige allgemeine Optionen. Am wichtigsten ist die Festlegung des Speicherorts. Wenn eine große Anzahl von Backups geplant wird oder, was noch wichtiger ist, wenn diese oft ausgeführt werden, wird viel Speicherplatz auf der Festplatte benötigt. Die Festlegung eines Speicherorts erfordert daher sorgfältige Planung: Der Speicher sollte umfangreich sein und muss sich leicht erweitern lassen. Es gibt noch weitere Anforderungen an den Speicherplatz. Aus Gründen der Leistungsfähigkeit sollte das Ziel nicht komprimiert oder verschlüsselt sein. Die Backup-Software verschlüsselt und komprimiert die Daten bereits automatisch. Wenn sie auf Betriebssystem- oder Hardware-Ebene erneut komprimiert oder verschlüsselt werden, sorgt dies nicht für zusätzliche Sicherheit, sondern verringert die Backup-Leistung erheblich. Das Backup-Ziel muss eine Festplatte sein, die für die Speicherung von Backups vorgesehen ist und keine anderen Dateien enthält. Dadurch können Administratoren die Festplatten leicht physisch archivieren, wenn die Richtlinie zum Datenerhalt des Unternehmens dies verlangt, und eine Verwechslung von normalen Dateien und Backups wird vermieden. Das Backup-Standardziel ist der Server-Ordner „%ProgramData%\G Data\AntiVirus ManagementServer\Backup“ (ab Windows Vista/Windows Server 2008) oder C:\Dokumente und Einstellungen\Alle

Benutzer\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Backup (Windows XP/Windows Server 2003). Da sich diese Ordner auf der Systemfestplatte des Servers befinden, sollten sie nicht als Backup-Ziel verwendet werden. Es sollte mindestens ein Backup-Pfad konfiguriert werden, beispielsweise eine andere Festplatte auf demselben Computer. Werden mehrere Pfade definiert, speichert der G DATA Administrator die Backup-Datei automatisch im ersten Pfad, der genügend freien Festplattenspeicher für die Backup-Datei bietet. Außerdem ist dann gewährleistet, dass sich das Backup-Ziel durch Deaktivieren eines Pfads ganz leicht wechseln lässt (beispielsweise dann, wenn kein Festplattenspeicher mehr übrig ist).

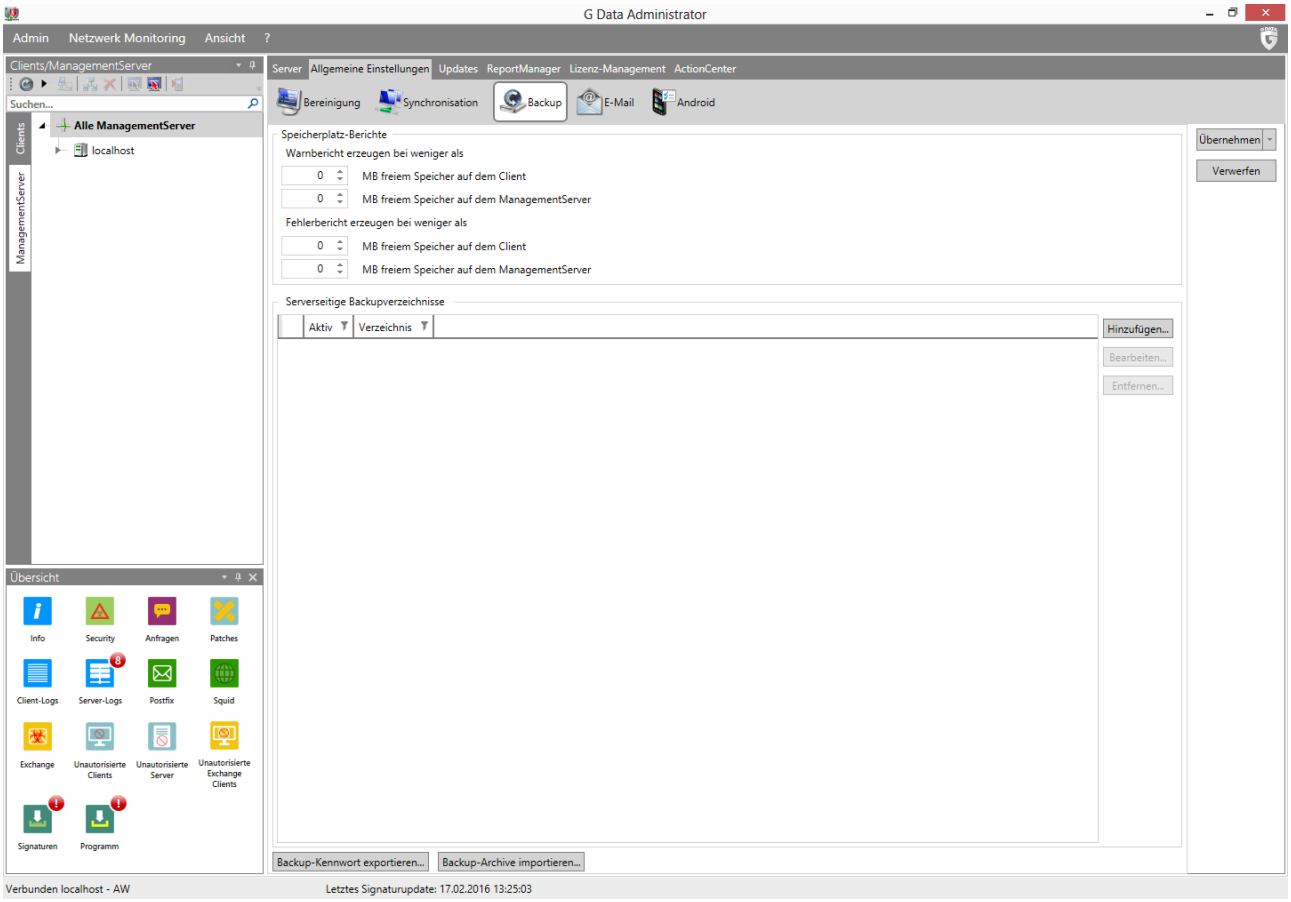

Abbildung 44: G DATA Administrator – Allgemeine Einstellungen, Backup

Zusätzlich zu den Backup-Zielen bietet das Fenster ALLGEMEINE EINSTELLUNGEN > BACKUP auch die Möglichkeit, das Backup-Kennwort zu exportieren. Dies ist empfehlenswert, da Backup-Archive kennwortgeschützt sind. Beim Importieren von Backup-Archiven muss das Kennwort eingegeben oder aus einer Datei importiert werden. Es sollte daher sichergestellt werden, dass das Kennwort exportiert und an einem sicheren Ort gespeichert wird. Durch Klicken auf BACKUP-ARCHIVE IMPORTIEREN wird ein vorhandenes Backup-Archiv importiert. Wenn ein Ordner mit Backups ausgewählt wurde, importiert der G DATA Administrator seinen Inhalt und führt die Backup-Datei(en) in den Listen AUFTRÄGE unter der Überschrift IMPORTIERTE ARCHIVE auf. Mit der Funktion WIEDERHERSTELLUNGS-AUFTRAG lassen sich Backups wie alle anderen Elemente wiederherstellen (siehe Abschnitt 12.3).

Bei der Ausführung eines Backup-Auftrags speichert der Client das Backup in einem lokalen Zwischenspeicher, während es an den ManagementServer übertragen wird. Wenn die Option CLIENTABHÄNGIGEN STANDARDPFAD VERWENDEN ausgewählt ist, wird das Backup in der Partition

zwischengespeichert, die den meisten freien Festplattenspeicher enthält. Wenn es sich dabei um die Systemfestplatte handelt, ist es der Ordner %ProgramData%\G Data\Backup. Bei einer anderen Festplatte ist es das Verzeichnis \G Data\Backup. Durch Deaktivierung dieser Option kann ein anderes als das Standardverzeichnis konfiguriert werden. Das ist besonders hilfreich, um eine Speicherung des Zwischenspeichers auf einer Nicht-Systemfestplatte zu erzwingen.

Für die Durchführung eines Backups müssen sowohl Client als auch Server genügend freien Festplattenspeicher für den Backup-Cache bzw. die Backup-Speicherung haben. Im Bereich ALLGEMEINE EINSTELLUNGEN > BACKUP können Schwellenwerte für den Festplattenspeicher konfiguriert werden. Wenn die Menge des freien Festplattenspeichers auf dem Client oder Server unter den Warnungsschwellenwert fällt, wird dem Modul SICHERHEITSEREIGNISSE eine Warnung hinzugefügt und der Client-Zwischenspeicher wird geleert, wobei außer des letzten Backups jedes zwischengespeicherte Backup entfernt wird, das bereits an den Server übertragen wurde. Fällt der freie Festplattenspeicher auf dem Client oder Server unter den Fehlerschwellenwert, wird dem Modul SICHERHEITSEREIGNISSE eine Fehlermeldung hinzugefügt. Der Backup-Speicher des Servers und der Zwischenspeicher des Clients werden automatisch geleert. Wenn immer noch nicht genügend freier Festplattenspeicher auf dem Server zur Verfügung steht, werden keine Backups durchgeführt. Der Fehlerschwellenwert für Client und Server sollte (mit einem gewissen Spielraum) die Größe eines oder mehrerer der größten Backup-Aufträge abdecken, die ausgeführt werden. Der Warnungsschwellenwert sollte höher angesetzt werden, damit der Administrator rechtzeitig über drohende Speicherprobleme informiert wird.

12.2. Erstellen eines Backups

Wie bei Scans empfiehlt es sich auch hier, den Backup-Plan als Ganzes zu betrachten, anstatt verschiedene zusammenhangslose Backups zu planen. Alle Backup-Aufträge zusammen sollten sicherstellen, dass Dokumente, Einstellungen und andere wichtige Dateien regelmäßig an einen sicheren Ort kopiert werden. Aber für einen effektiven Backup-Plan braucht es mehr als das. Die Verwaltbarkeit von Backup-Aufträgen wird durch Datenkonsolidierung, Client-Einstellungen und Server-Leistung stark beeinflusst. Vor der Planung von Backups sollten diese Fragen berücksichtigt und dann ein vereinheitlichter Backup-Plan erstellt werden.

Je nach Anzahl der Dateien, von denen ein Backup erstellt werden soll, können bis zum Abschluss eines Backup-Auftrags mehrere Stunden vergehen. Bei der Planung eines vollständigen Backups sollte unbedingt ein Zeitpunkt gewählt werden, zu dem der Client nicht in Gebrauch ist, um einen Leistungsverlust zu vermeiden. Bei den nachfolgenden partiellen Backups werden nicht mehr so viele Daten pro Backup gesichert wie beim ersten Mal, da diese Backups nur neue und aktualisierte Dateien umfassen. In diesem Fall ist die Planung eines Backups während der üblichen Arbeitszeit nicht mehr problematisch. Besonders bei wiederkehrenden Aufträgen muss dafür gesorgt werden, dass der Backup-Moment nichts Wichtiges beeinträchtigt. Andere Backup-Aufträge, PatchManager-Aufträge oder Scans sollten nicht gleichzeitig mit einem geplanten Backup erfolgen, damit das System nicht zum Stillstand kommt. Bei der Planung eines Backups für Laptop-Clients kann das Backup verschoben werden, wenn der Laptop im Batteriemodus läuft, um die Festplatte nicht zu belasten und die Batterie nicht aufzubrauchen. Es wird fortgesetzt, sobald der Laptop an eine Steckdose angeschlossen wird. Bei der Planung eines Backups von einer kleineren Anzahl von Dateien, das relativ schnell durchgeführt werden

kann, können Benutzerfreundlichkeit und Laptop-Leistung von der Datensicherheit übertrumpft werden. In den meisten Fällen lässt sich jedoch das Backup sicher bis zur nächsten Aufladung verschieben.

Die Auswahl der Dateien, die pro Backup gesichert werden sollen, ist der schwierigste Teil der Definition eines Backup-Auftrags. Windows nutzt automatisch die standardisierten lokalen Ordner für Dokumente und Einstellungen. Das Modul BACKUP bietet die Möglichkeit, alle diese Benutzerordner automatisch in einen Backup-Auftrag einzubeziehen. Dies ist zwar eine Form der Datenkonsolidierung, es empfiehlt sich aber nicht, nur ein Backup der Benutzerordner zu erstellen: Es kann unnötige Dateien enthalten und Backup-Festplattenspeicher verschwenden, oder es kann Dokumente auslassen, die manuell anderswo oder in einem unzugänglichen Benutzerordner gespeichert wurden. Die Dateispeicherung des Endbenutzers lässt sich am einfachsten verwalten, wenn sie sich auf einem zentralen (Datei-)Server befindet. Das Backup wird vereinfacht, wenn die Datenquellen sowohl auf Client-Ebene als auch netzwerkweit konsolidiert sind. Anstatt jeden Client daraufhin überprüfen zu müssen, ob und wo Dokumente und Einstellungen gespeichert sind, werden sie in einem standardisierten lokalen Ordner oder auf einem Teil des Servers gespeichert. Das spart Zeit und sorgt dafür, dass beim Backup nichts versehentlich ausgelassen wird. Wenn ein benutzerbasierter Profilordner in einem Teil des Netzwerks als standardmäßiges Speicherziel für Dokumente angeboten wird, können Administratoren für alle Endbenutzer gleichzeitig Dateien sichern, wenn sie nur ein Backup des Netzwerkordners planen. Bei kleineren Netzwerken, die möglicherweise keinen Dateiserver besitzen, kann die lokale Konsolidierung von Windows hilfreich sein. Die Administratoren sollten sich aber ihrer Grenzen bewusst sein und dafür sorgen, dass alle unverzichtbaren Dateien auch tatsächlich erfolgreich im Backup gesichert sind.

Neben der serverseitigen Möglichkeit, temporäre Dateien von Backups auszuschließen, können auch lokale Maßnahmen ergriffen werden, um Unordnung zu minimieren und Festplattenspeicher zu sparen. Administratoren sollten sich beim Hinzufügen eines Ordners zu einem Backup-Auftrag vergewissern, dass er nur die Art von Dateien enthält, für die ein Backup erstellt werden soll. Temporäre Dateien, allgemeine Systemdateien und andere Dateien von geringer Priorität sollten vom Backup ausgeschlossen, in einen anderen Ordner verschoben oder entfernt werden.

Man sollte der Versuchung widerstehen, nur einen Backup-Auftrag zu planen, der alles enthält. Pauschale Backup-Aufträge verschwenden Festplattenspeicher, brauchen viel Zeit und erschweren eine schnelle, gezielte Wiederherstellung. Backups lassen sich nach Dateityp, Risiko oder Bedeutung bzw. einer Kombination davon organisieren. Von wichtigen Datenbankdateien sollte beispielsweise regelmäßig ein Backup erstellt werden, während Protokolldateien auf demselben Computer in einem größeren Intervall gesichert werden können. Es kann hilfreich sein, ein Inventar der Dateitypen anzulegen, die auf Netzwerk-Clients produziert und verwendet werden, und dazu anzugeben, wie wichtig sie sind und wie hoch das Risiko eines Datenverlusts ist. Für jede Dateigruppe sollte ein separates Backup geplant werden, dessen Ausführungsintervall sich bei wichtigen oder Hochrisikodateien verkürzt. Vorschläge zu Backup-Kategorien sind in Abschnitt 12.2.1 und danach enthalten.

Es müssen jedoch alle Dateien aufgenommen werden, die für das Unternehmen wichtig sind und nicht verloren gehen sollten. Während des Backup-Vorgangs werden alle kopierten Dateien auf Malware überprüft. Beim Aufbau des Archivs wird sichergestellt, dass kein Backup von infizierten Dateien erstellt wird. Dadurch entfällt die Notwendigkeit, einen zusätzlichen Scan direkt vor der Durchführung des Backups zu planen. Um einen unbefugten Zugriff auf die Dateien zu verhindern, werden alle Backup-Archive verschlüsselt, sodass sie nicht einfach von der Festplatte aus geöffnet werden können. Dies

verhindert auch, dass Malware die Backup-Archive infiziert. Wenn der Backup-Vorgang alle Dateien archiviert hat, wird die Integrität des Archivs überprüft und somit gewährleistet, dass während des Aufbaus keine Probleme aufgetreten sind. Die Datei wird dann vom lokalen Zwischenspeicher zum Server verschoben, der sie in ihren endgültigen Backup-Zielordner verschiebt.

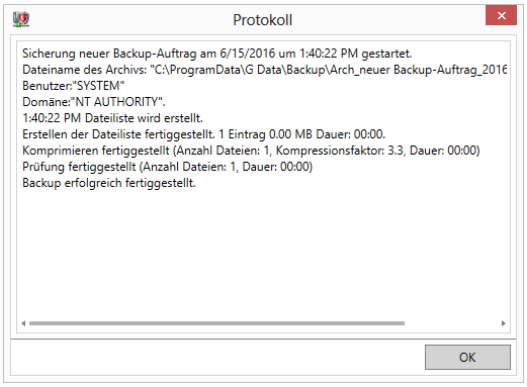

Abbildung 45: G DATA Administrator – Aufträge, Backup-Protokoll

Nach Abschluss eines Backups ist das entsprechende Protokoll über den Auftragseintrag im Modul AUFTRÄGE verfügbar. Für jede Iteration, ob volles oder partielles Backup, wird ein separates Protokoll angelegt. Dateien, die während des Backups in Gebrauch sind, werden möglicherweise nicht korrekt kopiert, oder Lesefehler der Festplatte können zu Komplikationen führen. Deshalb empfiehlt es sich, die Protokolle für jedes Backup regelmäßig zu überprüfen, um zu sehen, ob es erfolgreich durchgeführt wurde und ob zusätzliche Backups oder Maßnahmen geplant werden müssen.

Zusätzlich sollte eine regelmäßige Testwiederherstellung geplant werden. Eine Testwiederherstellung sollte durchgeführt werden, um das Backup in einem beliebigen Client oder Ordner wiederherzustellen und so sicherzustellen, dass es sich korrekt wiederherstellen lässt und die richtigen Dateien enthält. Das Vorhandensein eines Backups ist unbedingt notwendig, wenn Probleme auf einem Client auftreten. Deshalb sind regelmäßige Testläufe oder andere Maßnahmen sehr wichtig, mit denen die Integrität der Backup-Dateien bestätigt wird.

12.2.1. Dokumente

Dokumente sind wohl die Art von Dateien, bei denen ein Backup am wichtigsten ist. In den meisten Unternehmen verbringen Informationsarbeiter sehr viel Zeit mit der Produktion von digitalen Dateien wie Dokumenten, Programmen, Grafiken und anderen Assets. Diese Dateien bilden oft das Herzstück des Produktionsprozesses und ein Datenverlust könnte die Produktion zurückwerfen oder sogar direkt einen Umsatzrückgang verursachen. Das Hauptziel eines Backup-Plans sollte deshalb die Sicherung dieser Dateien sein.

Dokumente können sich auf Festplatten des Clients oder in anderen lokalen und externen Speichern befinden. Das kann Backups deutlich erschweren: Wenn es keinen zentralisierten Dokumentenspeicher gibt, muss für jeden Client ein separater Backup-Auftrag definiert werden, der ausdrücklich seine lokalen Dokumentenspeicherordner abdeckt. Bei Clients, die Benutzerprofilordner wie etwa „Desktop“ oder „Eigene Dokumente“ verwenden, kann ein Backup-Auftrag definiert werden, der alle lokalen Benutzerverzeichnisse abdeckt. Dadurch werden alle in diesen Ordnern gespeicherten Dokumente sowie ausgewählte Einstellungen erfasst. Alternativ kann ein Backup-Auftrag angelegt werden, der die gesamte

Festplatte umfasst, aber die Dateitypen ausschließt, die keine Dokumente sind (dies wird mithilfe der Endung definiert, etwa .exe, .dll oder .com). Die zuverlässigste Backup-Strategie ist aber die Steuerung der Dateispeicherung in einer viel früheren Phase. Eine zentrale Dateispeicherung, beispielsweise auf einem Netzwerkdateiserver, ermöglicht einen sehr einfachen Backup-Auftrag, der einfach nur diese Ordnerstruktur abdeckt. Wenn eine Fragmentierung in dieser Phase verhindert wird, verringert das deutlich die Wahrscheinlichkeit, dass in der Backup-Phase Dateien ausgelassen werden.

Die Auftragsplanung für Dokumenten-Backups hängt von der Häufigkeit ab, mit der die Clients verwendet werden. In den meisten Fällen wird der Client täglich genutzt, weshalb auch ein tägliches Backup durchgeführt werden sollte. Die Backup-Häufigkeit sollte nur sporadisch auf eine Häufigkeit von alle zwei oder drei Tage verringert werden. Das erste Backup sollte ein vollständiges Backup sein, das zu einem Zeitpunkt durchgeführt wird, an dem der Client nicht in Gebrauch ist. Das vollständige Backup umfasst alle Dateien und ist daher relativ groß. Die nachfolgenden Backups können als partielle Backups konfiguriert werden. Diese Art von Backup (auch als differenzielles Backup bekannt) speichert nur die Dateien, die seit dem letzten vollständigen Backup geändert worden sind. Das führt zu einer erheblichen Zeiteinsparung beim Backup und nutzt weniger Festplattenspeicher auf den Backup-Zielen. Die Wiederherstellung des Backups dauert etwas länger, weil es aus mehreren Dateien wieder aufgebaut werden muss (aus dem ursprünglichen vollständigen Backup und dem letzten partiellen Backup). Wenn das ein Problem ist, können auch die nachfolgenden täglichen Backups vollständig Backups sein. Die Menge des erforderlichen Speicherplatzes wird dann aber sprunghaft ansteigen. In diesem Fall besteht die empfohlene Lösung darin, ein wöchentliches vollständiges Backup und ein tägliches partielles Backup zu konfigurieren.

12.2.2. Datenbanken

In vielen IT-gestützten Unternehmen werden bestimmte Arten von Informationen zentral gespeichert. Das kann von einer zentral verwalteten Workflow-Umgebung bis hin zu Kontaktdatenbanken, Vertriebsinformationen und anderen Assets reichen, die die Produktion des Unternehmens betreffen. Eine weitere wichtige Datenbank ist der Nachrichtenspeicher des Mail-Servers. Bei einem Ausfall der Festplatte könnte die einzige Datenbank gelöscht werden, die alle wichtigen E-Mails, Kontakte oder Produktinformationen des Unternehmens enthält. Zum Erhalt der Datensicherheit sollten Backups konfiguriert werden, um sicherzustellen, dass regelmäßig an einem sicheren Ort ein Backup der gesamten Datenbank erstellt wird.

Die Backup-Erstellung von Datenbanken kann kompliziert sein. Je nach Art der Datenbank sind ihre Dateien möglicherweise dauerhaft in Gebrauch. Beispielsweise kann der Backup-Prozess so lange nicht auf eine E-Mail-Datenbank zugreifen, wie der Mail-Server in Betrieb ist. Es muss gewährleistet sein, dass die Datenbankdateien zum Zeitpunkt des Backups nicht in Gebrauch sind. Dazu müssen alle laufenden Prozesse, die die Datenbank nutzen, und Hintergrunddienste beendet werden. Bei vielen Arten von Datenbanken kann dies zu einer erheblichen Störung des Betriebs führen. In diesen Fällen sollte ein Backup während eines bestehenden Wartungsfensters durchgeführt werden, beispielsweise am Wochenende oder nachts, wenn es nur wenige oder gar keine Aktivität gibt.

Wie oft ein Datenbank-Backup durchgeführt werden sollte, hängt davon ab, wie die Datenbanken genutzt werden. Für unverzichtbare Informationen, die regelmäßig oder ständig aktualisiert werden (etwa E-Mail-Datenbanken), empfiehlt sich ein tägliches Backup. Das erste Backup ist ein vollständiges

Backup. Danach sollten nur noch partielle Backups erfolgen, damit sich der Backup-Speicherplatz nicht zu schnell füllt. Bei Datenbanken, die weniger regelmäßig genutzt werden, kann das Backup wöchentlich erfolgen. In diesem Fall lässt sich das Backup leichter planen: Die Betriebsstörungen sind geringer, wenn ein wöchentliches Wartungsfenster genutzt werden kann.

Bei manchen Datenbanken lässt sich ein Backup ganz einfach mit einer dateibasierten Backup-Lösung wie dem Backup-Modul von G DATA erstellen, andere verfügen über eingebaute Backup-Tools. Unabhängig davon, ob man das Backup-Modul von G DATA oder ein eingebautes Tool für Datenbank-Backups nutzt, müssen Backups unbedingt regelmäßig durchgeführt und auf ihre Integrität überprüft werden, um sicherzugehen, dass sie sich bei Bedarf erfolgreich wiederherstellen lassen.

12.2.3. Konfiguration

Im Laufe der Zeit kann die Konfiguration eines Clients erheblich von der abweichen, mit der dieser ursprünglich bereitgestellt wurde. Endbenutzer ändern die Einstellungen im Betriebssystem und möglicher Drittanbieter-Software oft nach ihrem Geschmack, und Administratoren stellen geänderte Konfigurationen bereit, um lokale Probleme zu beheben. Der Verlust von Konfigurationseinstellungen kann ärgerlich sein, wenn nach dem Ausfall einer Festplatte viel Zeit für die Neukonfiguration eines Systems aufgewendet werden muss. Die Erstellung von Backups der Konfigurationsdateien hilft dabei, die zur Neukonfiguration eines Systems nach einer Neuinstallation benötigte Zeit zu verkürzen.

Die Suche nach allen Konfigurationsdateien auf einem Client kann schwierig sein. Manche Einstellungen sind in Dateien gespeichert (normalerweise mit der Endung .ini), andere sind in der Windows-Registry gespeichert, von der sich nur schwer ein Backup erstellen lässt. Bei einer Software, die dies unterstützt, kann die zentrale Speicherung der Einstellungen (in einer zentralen Konfigurationsdatei oder mithilfe einer Methode wie den Microsoft-Gruppenrichtlinien) einen langwierigen Prozess zur Bestimmung der richtigen Dateien verhindern und das Backup vereinfachen. Außerdem lassen sich anschließend Konfigurationsänderungen und Standardeinstellungen leichter auf mehrere Clients gleichzeitig verteilen. Bei kleineren Netzwerken können die Administratoren auch manuell bestimmen, welche Software derzeit auf den Clients installiert und wo ihre Konfiguration gespeichert ist. Das Software-Inventar (CLIENTS-Modul) kann dabei helfen, Informationen über die Software auf den Clients zu finden, benötigt jedoch relativ viel Zeit, um die Konfigurationsdateien zu lokalisieren. Für diejenigen, die sich auffinden lassen, kann ein Backup geplant werden. In den meisten Situationen reicht es aus, einmal im Monat ein Backup auszuführen. Bei Clients, die regelmäßiger neu konfiguriert werden, ist aber auch ein wöchentliches oder tägliches Backup eine Möglichkeit.

12.2.4. Systemdateien

Backups müssen sich nicht nur auf Dateien konzentrieren, die von einem Endbenutzer generiert wurden. Auch von ausführbaren Dateien und anderen Komponenten, die zu einem Betriebssystem oder externen Programm gehören, lässt sich ein Backup erstellen. Wie bei Datenbank-Backups kann dieser Vorgang schwierig sein, da viele Systemdateien dauerhaft in Gebrauch sind. Ein zusätzliches Problem besteht in der Tatsache, dass ein Software-Backup oft nicht für sich allein funktionieren kann. Wenn ein Backup des Ordners „Programme“ eines Clients erstellt wird, werden die vielen Abhängigkeiten wie etwa andere Software, Frameworks oder bestimmte Funktionen und Updates des Betriebssystems nicht

berücksichtigt. Die Wiederherstellung eines solchen Backups auf einem leeren System garantiert nicht, dass die Software funktionieren wird.

Eine bessere Lösung für die Erstellung von Software-Backups ist es, die ursprünglichen Installationsprogramme zu sichern und auf einem Server zu speichern. Was das Betriebssystem selbst betrifft, lässt sich der Wiederherstellungsvorgang vereinfachen, wenn gewährleistet ist, dass immer ein komplettes System-Image des Betriebssystems mit seinen letzten Updates und der gesamten, typischerweise genutzten Drittanbieter-Software zur Verfügung steht. Dieses Image ähnelt einem Backup, enthält aber keine Benutzerdokumente. Stattdessen wird es ausgehend von einem „sauberen“ Betriebssystem mit den neuesten Updates und der gesamten erforderlichen Software erstellt. Es erfordert einen gewissen Aufwand, dieses Image immer auf dem neuesten Stand zu halten, verkürzt aber deutlich die Zeit, die zur Wiederherstellung eines vollständigen Systems benötigt wird. Dies funktioniert am besten in einem Szenario, in dem die Clients persönliche Daten nicht lokal, sondern auf einem Dateiserver speichern: Ein Ausfall der Client-Festplatte verursacht dann keinen Datenverlust und ein Betriebssystem-Image lässt sich schnell wiederherstellen, sobald eine neue Festplatte bereitsteht.

12.2.5. On-Demand-Backup

Backup-Aufträge lassen sich auch manuell, anstatt gemäß einem Zeitplan durchführen. Dies kann in Szenarien hilfreich sein, in denen wegen einer geringen Bedeutung oder aufgrund des geringen Datenverlustrisikos typischerweise überhaupt kein Backup des Clients erstellt wird. Alternativ kann ein Backup auf Anfrage (also „on demand“) schnell die Daten speichern, wenn ein offenbar bevorstehender Hardware-Ausfall die Stabilität des Clients zu bedrohen scheint. Diese Art von Backup-Aufträgen lässt sich im Voraus planen, damit im Notfall eine kurze Reaktionszeit möglich ist. Da ein Auftrag aber nur dem Client zugewiesen werden kann, für den er ursprünglich geplant wurde, gibt es keine Möglichkeit, einen einzelnen Backup-Auftrag für den Notfall vorzubereiten. Das Fenster BACKUP-AUFTRAG ist recht einfach und ermöglicht den Administratoren die schnelle Definition der notwendigen Maßnahmen, wenn ein On-Demand-Backup geplant sein muss.

12.3. Wiederherstellen eines Backups

Im Ernstfall ist es wichtig, dass ein aktuelles Backup zur Verfügung steht. Wenn die Backup-Aufträge richtig geplant wurden, ist der Datenverlust minimal. Im Gegensatz zur Planung der Backups ist die Wiederherstellung der Daten relativ einfach. Die Mindestanforderung ist eine funktionierende Installation des Betriebssystems und des G DATA Security Clients (bei einem kompletten Festplattenausfall müssen beide möglicherweise neu installiert werden).

Um sich alle bestehenden Backup-Aufträge für den Client anzusehen, kann in der Ansicht CLIENTS das Modul AUFTRÄGE geöffnet werden. Nach einem Rechtsklick auf einen Auftrag wird durch Klicken auf BACKUP WIEDERHERSTELLEN das Fenster WIEDERHERSTELLEN geöffnet. Alternativ kann der ManagementServer ausgewählt, das Menü AUFTRÄGE geöffnet und die Optionen HINZUFÜGEN > WIEDERHERSTELLUNGS-AUFTRAG gewählt werden, um einen Überblick über die verfügbaren Backups auf allen Clients zu erhalten. Durch Auswahl eines Backups und Klicken auf OK wird das Fenster WIEDERHERSTELLUNGS-AUFTRAG geöffnet. Nach Bestätigung der Wiederherstellungseinstellungen wird dem Modul AUFTRÄGE ein Wiederherstellungsauftrag hinzugefügt. Dieser wird sofort ausgeführt.

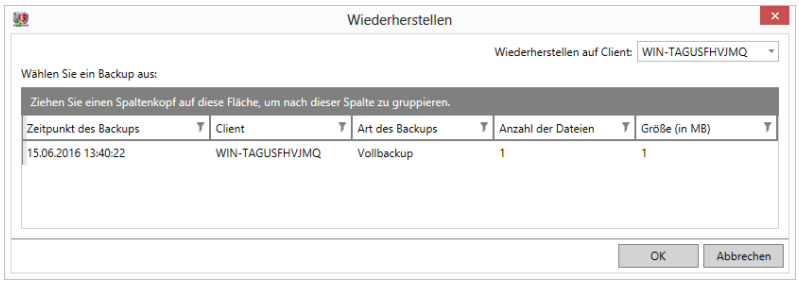

Abbildung 46: G DATA Administrator – Aufträge, Backup wiederherstellen

Bei begrenztem Speicherplatz können die Administratoren die Backup-Archive manuell an andere Speicherorte verschieben. Um sie wiederherstellen zu können, müssen sie jedoch erneut im G DATA Administrator importiert werden. Unter ALLGEMEINE EINSTELLUNGEN > BACKUP kann der Administrator mithilfe der Schaltfläche BACKUP-ARCHIVE IMPORTIEREN die Backup-Archivdateien aus einem beliebigen Ordner importieren. Dazu muss das Backup-Kennwort eingegeben werden, das auf dem ManagementServer, der das Backup erstellt hat, über die Schaltfläche BACKUP-KENNWORT EXPORTIEREN verfügbar ist. Die importierten Backups erscheinen in der Backup-Liste im Modul AUFTRÄGE.

Wiederherstellungsaufträge können so geplant werden, dass sie ein System in dem Zustand wiederherstellen, in dem es sich zum Zeitpunkt des Backups befand. Das gilt hauptsächlich für Backups von Konfigurations- oder Systemdateien. In diesem Fall werden alle Dateien in ihren ursprünglichen Ordnern wiederhergestellt, wobei vorhandene Dateien bei Bedarf überschrieben werden. Datenbanken und Dokumente hingegen können selektiv wiederhergestellt werden, um den Client nur mit den notwendigen Dateien zu versorgen. Die Registerkarte DATEIAUSWAHL kann dazu genutzt werden, das Backup-Archiv zu durchsuchen und Dateien oder Ordner ein- oder auszuschließen. Falls eine Datei versehentlich gelöscht wurde, kann mithilfe eines Backup-Archivs das aktuellste Backup der jeweiligen Datei gesucht und wiederhergestellt werden.

Ein Backup muss nicht unbedingt auf dem Client wiederhergestellt werden, von dem es erstellt wurde. Jedes Backup kann auf jedem Client wiederhergestellt werden, vorausgesetzt, dieser besitzt genügend freien Festplattenspeicher. Wenn das passende Backup ausgewählt ist, bietet das Fenster WIEDERHERSTELLEN das Dropdown-Menü WIEDERHERSTELLEN AUF CLIENT, mit dem ein beliebiger Client ausgewählt werden kann. Im folgenden Fenster können die Dateien ausgewählt werden, die auf diesem konkreten Client wiederhergestellt werden sollen. Dadurch kann der Administrator ein Client-Backup einer Netzwerkrolle erstellen und es auf Clients mit derselben Rolle wiederherstellen.

Es empfiehlt sich, Backup-Archive nach dem ersten Backup-Durchlauf zu testen, um zu überprüfen, ob die Backup-Einstellungen dazu geführt haben, dass alle Dateien korrekt enthalten sind, und ob das Backup-Archiv funktioniert. Durch einen Rechtsklick auf den Backup-Auftrag und die Auswahl der Option BACKUP WIEDERHERSTELLEN wird das Fenster WIEDERHERSTELLEN geöffnet. Nach einer Überprüfung, ob das Backup-Archiv aufgeführt ist, wird durch Klicken auf OK das Fenster WIEDERHERSTELLUNGS-AUFTRAG geöffnet. Um zu überprüfen, ob alle Dateien vorhanden sind, kann die Datei- und Ordnerliste verwendet werden. Um zu kontrollieren, ob sich das Backup ohne Probleme wiederherstellen lässt, wird es so konfiguriert, dass alle Dateien wiederhergestellt werden, und ein neues Zielverzeichnis auf der Registerkarte OPTIONEN definiert.

13. Firewall

Das Firewall-Modul ist Teil der Lösungen Client Security Business, Endpoint Protection Business und Managed Endpoint Security.

Die Firewall ist ein wesentlicher Bestandteil der Netzwerksicherheit. Als erste Verteidigungslinie filtern Firewalls den ein- und ausgehenden Datenverkehr. Dadurch ist gewährleistet, dass Angreifer keinen Fernzugriff auf ausgeführte Dienste haben, und dass die Computer-Software keine externen Server kontaktieren kann. Mithilfe einer Whitelist (Firewall-Regeln) kann bestimmten externen Besuchern ein Zugang gewährt werden und bestimmte lokale Software darf mit externen Servern Kontakt aufnehmen. Je nach Netzwerk-Layout (siehe Kapitel 1) kann eine Firewall ein Hardwaregerät oder eine Softwarelösung sein. Eine physische Firewall filtert den gesamten ein- und ausgehenden Datenverkehr des Netzwerks. Viele Router mit Unternehmensqualität, aber auch Modelle von geringerer Qualität, besitzen eine eingebaute Firewall. Auf der anderen Seite können Softwarelösungen auf einem Server oder Client installiert werden, die Schutz auf Computerebene bieten. Jedes Netzwerk sollte mindestens eine aktive Firewall beinhalten, die dafür sorgt, dass unerwünschter Datenverkehr draußen bleibt. Für alle Unternehmensnetzwerke empfiehlt sich die Aktivierung einer Firewall als erste Ebene der Netzwerksicherheit. Zusätzlich sollten Clients mit einer Software-Firewall ausgestattet sein. Dies ermöglicht eine differenziertere Kontrolle über die Anwendungsberechtigungen. Anstatt bestimmten Datenverkehr für das gesamte Netzwerk zu blockieren, kann der ein- und ausgehende Netzwerkverkehr durch die Definition von Regeln für einzelne Clients oder Netzwerkzonen verwaltet werden.

Firewall-Regeln sollten zentral koordiniert und entsprechend den Sicherheitsrichtlinien des Unternehmens konfiguriert werden. Die Regeln sollten über alle bereitgestellten Firewalls – auf Hardware- oder Software-Basis – hinweg vereinheitlicht werden, um Konflikte zu verhindern. Die Firewall-Regeln haben zwei Ziele: die Netzwerksicherheit verwalten und die Unternehmensrichtlinien einhalten (die nicht unbedingt etwas mit Sicherheit zu tun haben). Für den eingehenden Datenverkehr lassen sich die Firewall-Regeln relativ einfach definieren: Der gesamte Verkehr sollte verworfen werden, wenn er nicht von einem Endbenutzer oder Programm angefordert wurde (beispielsweise beim Surfen im Internet oder beim Einleiten eines Peer-to-Peer-Downloads). Das ist ein reines Sicherheitsthema, bei dem nicht angeforderter Datenverkehr als bösartiger Verbindungsversuch angesehen wird. Für ausgehenden Datenverkehr sind die Regeln komplizierter. Bestimmter Software und bestimmten Diensten kann ausgehender Datenverkehr verweigert werden, weil sie ein Sicherheitsrisiko darstellen können. Andere sind zwar nicht bösartig, erfüllen aber nicht die Unternehmensrichtlinie. Der ausgehende Datenverkehr für ein Chat-Programm ist zwar beispielsweise nicht bösartig, sollte aber trotzdem blockiert werden, wenn Chats laut der Unternehmensrichtlinie nicht erlaubt sind.

Das Firewall-Modul des G DATA Security Clients erzwingt die zentral verwalteten Firewall-Regeln für Clients. Es filtert den gesamten ein- und ausgehenden Netzwerkverkehr und sorgt dafür, dass nicht genehmigte Kommunikation blockiert wird. Die G DATA Firewall nutzt zum Filtern des Netzwerkverkehrs eine zustandsbehaftete Untersuchung. Diese Methode vergleicht nicht nur einzelne Pakete mit einem vordefinierten Regelsatz, sondern berücksichtigt auch die vorherigen Pakete, die mit demselben Server oder Computer ausgetauscht wurden. Auf diese Weise müssen Pakete, die in einem bestehenden TCP-Stream oder einer bestehenden UDP-Verbindung übertragen werden, nicht erneut vollständig untersucht werden, sondern können basierend auf dem Zustand der Verbindung (etwa IP-Adressen oder Ports, die bereits verwendet wurden) gefiltert werden. Dadurch verringert sich die Verarbeitungsleistung, die pro

Paket benötigt wird, und es wird gewährleistet, dass Administratoren und Endbenutzer schnell Regeln definieren können, um einen Verbindungstyp zuzulassen, ohne sich um die genaue IP-Adresse, Portnummer oder Paketrichtung kümmern zu müssen.

Das im G DATA Security Client enthaltene Firewall-Modul ist für den Einsatz auf Client-Computern vorgesehen. Der Client und all seine Schutzmodule (etwa Dateisystemwächter und Firewall) lassen sich zwar problemlos auf Servern installieren, die vordefinierten Regelsätze zielen aber auf Client-Computer ab. Für den Einsatz auf einem Server müssen Administratoren dafür sorgen, dass ein passender Regelsatz definiert ist.

13.1. Verwalten von Firewall-Clients

Die G DATA Firewall lässt sich über ihr eigenes Modul im G DATA Administrator verwalten. Auf der Registerkarte FIREWALL sind alle relevanten Optionen aufgeführt, die auf die Clients anwendbar sind, die in der Ansicht CLIENTS ausgewählt wurden. Wie bei anderen Modulen können auch die Firewall-Einstellungen auf einen oder mehrere Clients gleichzeitig angewendet werden.

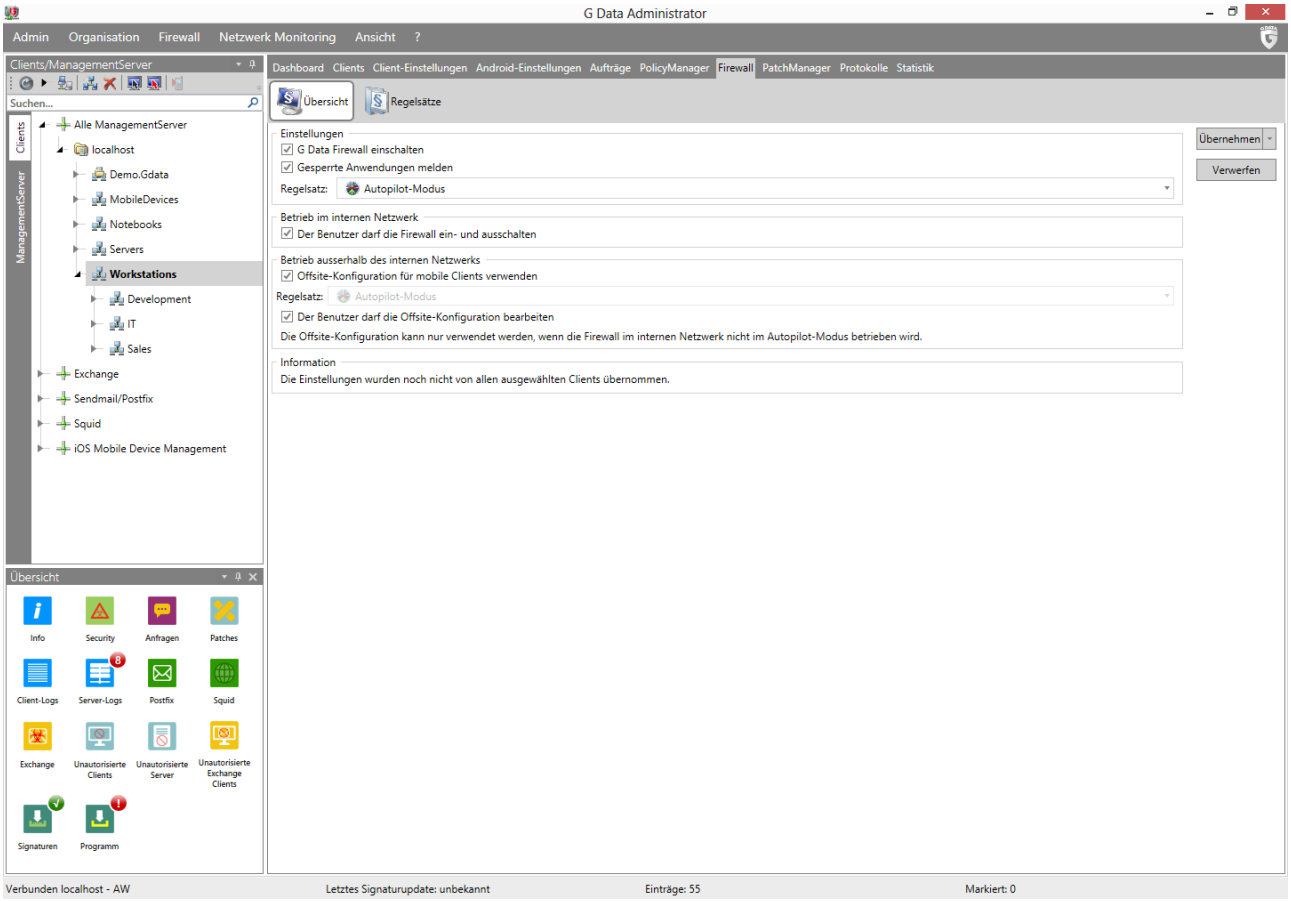

Abbildung 47: G DATA Administrator – Firewall, Übersicht

Es wird allgemein empfohlen, die G DATA Firewall wenigstens auf allen Clients zu aktivieren, die eine Verbindung mit dem Internet herstellen, und idealerweise auf allen Netzwerk-Clients. Die G DATA Firewall sollte nur dann nicht aktiviert werden, wenn eine alternative Client-Firewall verwendet wird, um Konflikte zu verhindern. Ab Version 14 müssen Clients ohne Firewall-Komponente auf die neue Version aktualisiert werden, bevor die Firewall aktiviert werden kann.

Zur Überwachung der Client-Aktivität sollte die Option GESPERRTE ANWENDUNGEN MELDEN aktiviert werden. Dadurch wird sichergestellt, dass die G DATA Firewall bei jeder Sperrung einer Anwendung einen Bericht an den ManagementServer sendet, der im Modul SICHERHEITSEREIGNISSE angezeigt wird. Wenn eine Client-Anwendung von einer der Firewall-Regeln gesperrt wird, zeigt der Bericht die problematische Anwendung an und ermöglicht es den Administratoren bei Bedarf, sie direkt einem der Regelsätze hinzuzufügen. Wie bei den Virusmeldungen können auch wiederholte Firewall-Berichte darauf hinweisen, dass ein Endbenutzer einen Computer missbräuchlich verwendet oder dass ein Teil seiner Arbeit aufgrund von Nutzungsbeschränkungen nicht ausgeführt werden kann.

Pro Client oder Gruppe kann ein Offsite-Regelsatz aktiviert werden. Die Aktivierung einer speziellen Offsite-Konfiguration ist besonders für solche Clients sinnvoll, die regelmäßig außerhalb des Unternehmensnetzwerks benutzt werden. Die G DATA Firewall verwendet die normale Konfiguration so lange, wie der Client mit dem Unternehmensnetzwerk verbunden ist, schaltet aber in die Offsite-Konfiguration, sobald der Computer eine Verbindung mit einem anderen Netzwerk herstellt. Dadurch wird die Sicherheitsrichtlinie für das Unternehmensnetzwerk eingehalten und gleichzeitig dem Endbenutzer mehr Flexibilität ermöglicht, wenn der Computer anderswo verwendet wird. Ein Offsite-Regelsatz kann nur aktiviert werden, wenn der Client einen Regelsatz für das Unternehmensnetzwerk verwendet. Die Nutzung des Autopilot-Modus verbietet die Verwendung der Offsite-Konfiguration.

13.2. Autopilot

Der Autopilot ist die Standardeinstellung für alle Clients der G DATA Firewall. Diese Option konfiguriert die Firewall so, dass sie ihre Aufgaben komplett im Hintergrund ausführt. Die Endbenutzer werden mit keinerlei Aufforderungen konfrontiert, und die Administratoren müssen nur eine minimale Anzahl von Verwaltungsaufgaben ausführen. Der Autopilot belastet die Verwaltung nur sehr wenig und kann in Netzwerken eingesetzt werden, in denen nur eine minimale Anzahl von Drittanbieteranwendungen genutzt wird oder in denen der Software-Bestand relativ stabil ist. Ein- und ausgehende Verbindungen werden automatisch bewertet und zugelassen oder blockiert. Wenn die Software versucht, eine ausgehende Verbindung herzustellen, erlaubt die Firewall die Verbindung dann, wenn der Prozess nicht als Malware erkannt wird. Für die ersten beiden Versuche einer ausgehenden Verbindung wird eine temporäre Regel festgelegt, die den Datenverkehr durch die Firewall erlaubt. Wenn derselbe Prozess zum dritten Mal versucht, eine ausgehende Verbindung zu öffnen, wird dem Autopilot-Regelsatz eine Regel hinzugefügt, nach der die Software dauerhaft zugelassen wird. Eingehende Verbindungen werden immer verworfen, wenn sie nicht Teil einer Kommunikation sind, die von einem der Prozesse auf dem System eingeleitet wurde.

Wenn der Administrator das Modul SICHERHEITSEREIGNISSE im Auge behält, kann er überprüfen, wie oft die Firewall Anwendungen blockiert. Wenn sich herausstellt, dass der Autopilot-Modus unverzichtbare aus- oder eingehende Verbindungsversuche verbietet, empfiehlt es sich, die betroffenen Clients auf den manuellen Regelsatzmodus umzuschalten. Das Gleiche gilt für Laptop-Clients: Computer, die oft außerhalb des Unternehmensnetzwerks benutzt werden, sollten auf manuelle Regelsätze umgeschaltet werden, um Offsite-Konfigurationsfunktionen zu ermöglichen.

13.3. Regelsätze

Wenn nicht der Autopilot-Modus verwendet wird, haben die Administratoren eine Vielzahl von Möglichkeiten, die Firewall zu konfigurieren. Die G DATA Firewall nutzt Regelsätze: Sammlungen von anwendungs-, protokoll- und portbasieren Regeln, die den Datenfluss des Netzwerks von und zu den Clients steuern. Regelsätze ermöglichen eine hochdifferenzierte Kontrolle über den Netzwerkverkehr, ihre Konfiguration dauert jedoch länger als die des Autopilot-Modus. Die Administratoren sollten mit Layout, Protokollen und Anwendungen des Netzwerks vertraut sein, bevor sie versuchen, die Firewall mit einem individuellen Regelsatz zu konfigurieren. Nachdem ein Regelsatz angelegt wurde, lässt er sich einem oder mehreren Clients zuweisen. Dazu wird der Bereich Übersicht geöffnet und der Regelsatz als normaler oder Offsite-Regelsatz konfiguriert.

Im Bereich Regelsätze werden Regelsätze für das gesamte Netzwerk angelegt und bearbeitet. Im oberen Teil des Bereichs zeigt die Dropdown-Liste Regelsatz alle definierten Regelsätze an. Die Firewall arbeitet standardmäßig im Autopilot-Modus ohne definierte Regelsätze. Durch Klicken auf Neu kann ein neuer Regelsatz hinzugefügt werden. Das Anlegen eines neuen Regelsatzes erfordert die Eingabe eines Namens. Es kann optional eine Anmerkung hinzugefügt werden, um den Satz näher zu beschreiben (zum Beispiel, für welchen Client er vorgesehen ist oder ob bestimmte Anwendungen, Protokolle oder Teile enthalten sind). Durch die Aktivierung der Option Stealth-Modus aktiviert dürfen Clients nicht auf Porttests antworten, wodurch die Sicherheit weiter erhöht wird. Firewall-Regeln können schließlich auch aus dem standardmäßigen Regelsatz ausgewählt werden. Dieser Satz enthält Regeln für viele gebräuchliche Anwendungen, darunter Windows- und Microsoft-spezifische Funktionen, aber auch Drittanbieter-Software wie Adobe Reader und Mozilla Firefox. Die Auswahl von Regeln für Anwendungen, die im Netzwerk in Gebrauch sind, spart Zeit, es sollte aber sichergestellt werden, dass nur die notwendigste Kommunikation erlaubt ist. Durch Klicken auf OK wird der neue Regelsatz angelegt, der die ausgewählten Regeln enthält. Neben der Regelsatzliste befindet sich die Schaltfläche Bearbeiten, mit der sich Name und Anmerkung bearbeiten lassen. Die Schaltflächen Importieren und Exportieren können genutzt werden, um Regelsätze zu speichern und zu importieren.

Sie sind praktisch für Regelsatz-Backups oder für das mühelose Hinzufügen vordefinierter Regeln. Regelsätze enthalten eine beliebige Anzahl von Regeln, die entweder vordefiniert, benutzerdefiniert oder als Antwort auf einen Bericht erstellt wurden. Verbindungen werden anhand jeder Regel im Regelsatz bewertet. Die Regeln werden in der Reihenfolge der Priorität (Rang) aufgeführt: Bei jedem Verbindungsversuch übertrumpft die Regel auf Rang 1 die Regel auf Rang 2, diese übertrumpft die Regel auf Rang 3 usw. Dies ermöglicht die differenzierte Kontrolle von Ports und Protokollen, um beispielsweise mit Regel 1 UDP-Datenverkehr an Port 2000 zuzulassen und mit Regel 2 den gesamten übrigen UDP-Datenverkehr zu verwerfen. Mithilfe des Steuerelements Rang rechts neben der Liste können Regeln an andere Positionen der Liste verschoben werden. Zum Deaktivieren einer Regel innerhalb eines Regelsatzes muss das Kontrollkästchen neben dem jeweiligen Namen deaktiviert oder die Regel bearbeitet und die Option Regel aktiviert deaktiviert werden.

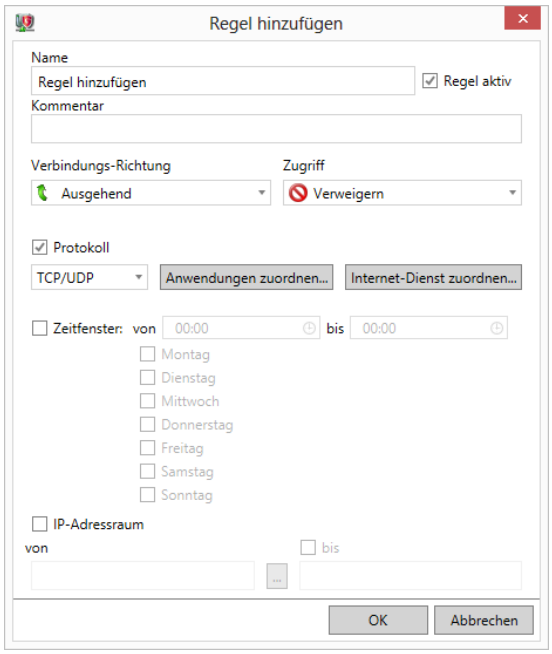

Abbildung 48: G DATA Administrator – Firewall, Regelsätze, Neue Regel

Neue Regeln können manuell mit der Schaltfläche NEU oder durch Klicken auf die Schaltfläche ASSISTENT mit dem Regelassistenten hinzugefügt werden. Mithilfe des Assistenten lässt sich eine Regel aus dem standardmäßigen Regelsatz zum ausgewählten Regelsatz hinzufügen, eine bestehende Regel kopieren, der Zugriff für eine bestimmte Anwendung gewähren oder verweigern oder ein bestimmter Port öffnen bzw. schließen. Das manuelle Hinzufügen einer neuen Regel ist dann am hilfreichsten, wenn der Assistent nicht genügend Flexibilität bietet – beispielsweise dann, wenn Regeln nur für einen bestimmten Zeitrahmen gelten sollen. Jede Regel besteht aus mehreren Komponenten. Die erforderlichen Basisinformationen sind Verbindungsrichtung und Zugriffstyp. Firewall-Regeln lassen sich für eingehende, ausgehende oder ein-/ausgehende Verbindungen festlegen. Manchen Anwendungen könnte nur der Versand von Paketen erlaubt werden, während für andere der Netzwerkzugriff vollständig gesperrt werden kann. Zusätzlich zu den Basisinformationen sollten eines oder mehrere der folgenden Merkmale ausgewählt werden: PROTOKOLL, ZEITFENSTER oder IP-ADRESSRAUM. Das Dropdown-Menü „Protokoll“ enthält verschiedene Protokolle, für die der Datenverkehr durch die Firewall gefiltert werden kann. Zusätzlich kann eine spezifische Anwendung bzw. ein spezifischer Port definiert werden. Das Popup-Fenster ANWENDUNGEN ermöglicht eine spezifische Kontrolle über die Anwendung, die blockiert oder zugelassen werden soll. Es kann dazu genutzt werden, einfach nur den Datenverkehr von einer oder mehreren Anwendungen zu filtern oder den Datenverkehr einer Anwendung nur dann zu blockieren bzw. zuzulassen, wenn dieser von einem bestimmten übergeordneten Prozess gestartet wurde. Im Fenster PORTS können Administratoren der Regel einzelne Ports oder Portbereiche hinzufügen. Mithilfe der Option ZEITFENSTER lässt sich die Regel auf eine bestimmte Tageszeit oder auf bestimmte Wochentage beschränken. Das kann sowohl für Sicherheitszwecke als auch für Unternehmensrichtlinien hilfreich sein. Schließlich kann mit der Option IP-ADRESSRAUM eine (externe) IP bzw. ein IP-Bereich hinzugefügt werden, auf die bzw. den der Datenverkehr beschränkt werden soll. Das kann eine IPv4- oder IPv6-Adresse, ein DNS-Server, ein Standard-Gateway-Server oder ein WINS-Server sein.

Das Fenster NEUE REGEL ist täuschend einfach, es lassen sich damit aber anspruchsvolle Firewall-Regeln erstellen. Welche Regeln genau erstellt werden sollen, hängt jeweils von Netzwerkkonfiguration,

Software-Bestand, Sicherheitsanforderungen und Unternehmensrichtlinien ab. Regeln aus dem standardmäßigen Regelsatz können ein großartiger Ausgangspunkt sein, aber fast jeder Regelsatz erfordert noch eine gewisse Feinabstimmung, bevor er im ganzen Netzwerk bereitgestellt werden kann. Eine versehentliche Blockierung von wichtigem Datenverkehr kann für die Endbenutzer extrem unpraktisch sein. Bei der Entwicklung eines Regelsatzes empfiehlt es sich daher, den Satz erst auf einem Client zu testen, bevor er in größerem Umfang bereitgestellt wird. Dabei muss gewährleistet sein, dass die Kommunikation zwischen dem Client und seinem ManagementServer nicht unterbrochen wird, denn dies würde die Problembehandlung deutlich erschweren.

Im Allgemeinen empfiehlt es sich, die Firewall für den Betrieb im Whitelist-Modus zu konfigurieren: Es werden nur Regeln für bekannte Anwendungen definiert und der gesamte übrige Datenverkehr blockiert. Dies lässt sich durch das Einfügen von Regeln am Ende des Regelsatzes erreichen, mit denen der gesamte Datenverkehr für alle Protokolle und Ports blockiert wird. Jeder Verbindungsversuch, der nicht von einer der anderen Regeln abgedeckt ist, wird blockiert. Dieser Regelsatzmodus ist zwar sehr sicher, seine Konfiguration kann aber kompliziert sein, da sich nur sehr schwer alle Arten von Datenverkehr vorhersagen lassen, die ein Client generieren wird. Es braucht eine gewisse Zeit, das normale Nutzungsmuster eines Client-PC sowie die Regeln herauszufinden, die konfiguriert werden müssen, um das beabsichtigte Verhalten abzudecken. Eine Methode besteht darin, einen Client als Regelsatztestgebiet zu bestimmen. Auf diesem Client sollte der Großteil der (oder die gesamte) Software installiert sein, die im Netzwerk in Gebrauch ist. Ausgehend von Regeln aus dem Standardregelsatz kann dieser Client dazu verwendet werden, den Datenverkehrsbedarf des Netzwerks zu messen und die entsprechenden Berechtigungen hinzuzufügen. Das Firewall-Protokoll kann sehr hilfreich sein, um sich ein detailliertes Bild von den Verbindungsversuchen zu machen (siehe Abschnitt 13.5).

Vor der Einführung von Regelsätzen sollte sichergestellt werden, dass jede Netzwerkzone ihren eigenen Regelsatz mit den passenden Regeln besitzt. Regelsätze sollten nur Regeln für den Kommunikationsbedarf der jeweiligen Netzwerkzone und ihrer Clients enthalten. Es kann ein Sicherheitsrisiko darstellen, zu vielen Anwendungen einen Zugriff auf das Netzwerk zu gewähren. Gleichzeitig sollte sich die Anzahl der Regelsätze handhaben lassen: Je mehr Regelsätze definiert sind, desto mehr Zeit erfordert die Behebung von Problemen mit Datenverkehrsberechtigungen im Netzwerk. Aus demselben Grund sollten nicht mehr genutzte Regeln aus den Regelsätzen gelöscht werden. Wenn beispielsweise ein Software-Produkt zurückgezogen und im Netzwerk nicht mehr genutzt wird, sollte(n) seine zugehörige(n) Regel(n) aus dem Firewall-Regelsatz entfernt werden. Ein „sauber“ gehaltener Regelsatz ermöglicht eine bessere Übersicht über die bestehenden Regeln und erleichtert die Problembehandlung.

13.4. Berechtigungen für Endbenutzer

Eine Firewall ist eine unverzichtbare Ebene in der Netzwerksicherheit, kann aber gleichzeitig die Aktivität des Endbenutzers auf einem Client-Computer behindern, wenn sie eine unbedingt erforderliche Anwendung blockiert. Die Administratoren können einen Teil der Verantwortung für die Firewall-Verwaltung auf den Endbenutzer übertragen, indem sie ihm erlauben, die Firewall zu aktivieren oder zu deaktivieren bzw. den Regelsatz der Offsite-Konfiguration zu ändern. Das kann praktisch sein, weil der Endbenutzer Probleme mit Berechtigungen dann unverzüglich beheben kann, aber auch gefährlich: Die Sicherheitsrichtlinien des Unternehmens können umgangen werden, wenn der Endbenutzer Regelsätze

ändern oder die Firewall komplett deaktivieren darf. Es empfiehlt sich hier vorsichtig vorzugehen und diese Optionen nur für problematische Client-Installationen oder Endbenutzer festzulegen, die über die entsprechende Erfahrung verfügen.

Endbenutzer können über den G DATA Security Client auf die Firewall-Einstellungen zugreifen. Durch einen Rechtsklick auf das Infobereichssymbol wird die Option FIREWALL angezeigt, die zur Benutzeroberfläche der G DATA Firewall führt. Dort können die Regelsätze bearbeitet werden (wenn die Option dazu aktiviert ist und der Client außerhalb des Unternehmensnetzwerks verwendet wird). Die Firewall kann durch Klicken auf FIREWALL DEAKTIVIEREN deaktiviert werden. Dadurch wird die Firewall ohne weitere Warnung deaktiviert. Sie wird nicht automatisch erneut aktiviert, der Status „Deaktiviert“ bleibt also auch nach Neustarts bestehen. Diese Option sollte daher nur mit großer Vorsicht genutzt werden: Es gibt praktisch keinen Anwendungsfall, in dem der Endbenutzer eine solche Berechtigung erhalten sollte.

13.5. Protokolle

Die Firewall-Komponente meldet dem G DATA Administrator blockierte Anwendungen. Es kann jedoch hilfreich sein, einen erweiterten Einblick in die ein- und ausgehenden Verbindungen zu erhalten. Wenn eine Anwendung unerklärlicherweise blockiert wird oder eine Statistik über verworfene eingehende Verbindungen erstellt werden soll, kann das lokale Firewall-Protokoll helfen. Wenn Endbenutzer die Möglichkeit haben sollen, sich detaillierte Protokolle anzusehen, kann der Administrator das Kontrollkästchen DER BENUTZER DARF DIE OFFSITE-KONFIGURATION ÄNDERN aktivieren. Dadurch wird dem Kontextmenü des Infobereichsymbols vom G DATA Security Client die Option FIREWALL hinzugefügt. Durch Klicken auf FIREWALL wird die Hauptbenutzeroberfläche der Firewall-Komponente geöffnet. Im Bereich PROTOKOLL wird eine detaillierte Übersicht über alle ein- und ausgehenden Verbindungen angezeigt. Der Endbenutzer kann das Verbindungsprotokoll, die initiierende Anwendung, die Richtung, den lokalen Port, den Remote-Host, den Remote-Port und den Grund für die Entscheidung über Zulassung oder Blockierung der Verbindung überprüfen.

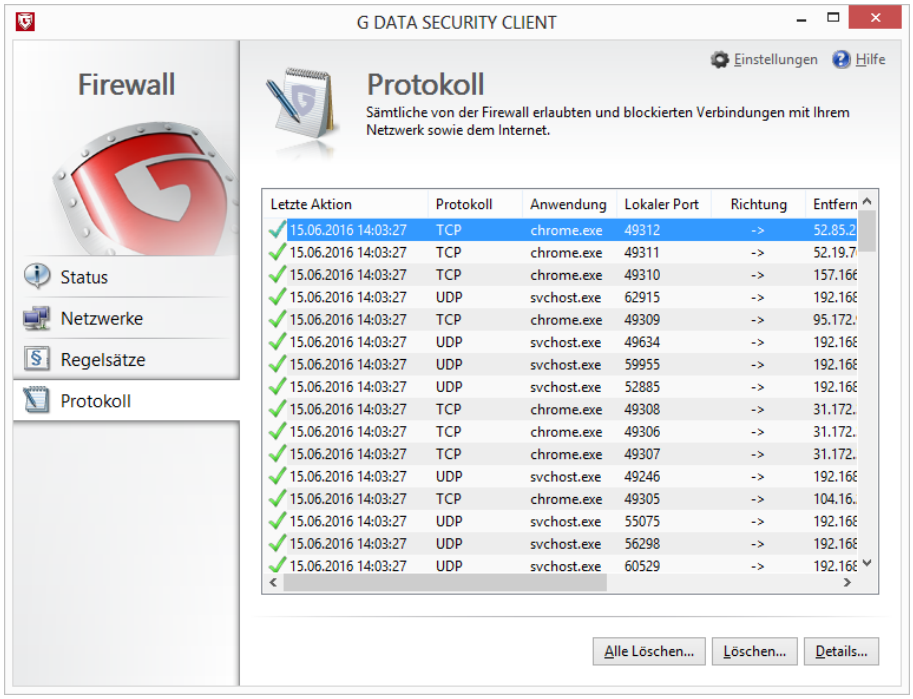

Abbildung 49: G DATA Security Client – Firewall, Protokoll

Wenn die Protokolle nicht von den Endbenutzern verwendet werden sollen, kann der Administrator die Firewall-Benutzeroberfläche weiterhin blockieren und stattdessen selbst direkt auf die Protokolldateien zugreifen. Dies ist allerdings eine erweiterte Ansicht, die recht überwältigend sein kann. Das Firewall-Protokoll wird als SQLite-Datenbankdatei gespeichert. Dieses Dateiformat kann von einer Reihe von Datenbank-Browsern wie etwa SQLite Datenbank Browser (www.sf.net/projects/sqlitebrowser/) gelesen werden. Das Verbindungsprotokoll wird in der Datenbankdatei „LiveStrm.dat“ gespeichert, die sich normalerweise unter C:\Programme (x86)\G Data\AVKClient\Firewall befindet. Die Datenbank enthält mehrere Tabellen, und das Verbindungsprotokoll befindet sich in der Tabelle „Verbindungen“. Jeder Eintrag steht für eine Verbindung und ihre Eigenschaften sind in mehreren Spalten aufgeführt. Die nachfolgende Tabelle enthält die wichtigsten Spalten und ihre Beschreibungen.

Spalte	Beschreibung
AdapterID	Kennung des Netzwerkadapters
AdapterName	Name des Netzwerkadapters
Allowed	Die Verbindung wurde erlaubt (-1) oder blockiert (0).
HasProcess	Die Prozesskennung, die die Verbindung initiiert hat. Kann mit einer Liste der laufenden Dienste verglichen werden.
IPv6	Die Verbindung nutzt das IPv6- (-1) oder IPv4-Protokoll (0).
LocalPort	Der lokale Verbindungsport
Outgoing	Die Verbindung war eingehend (-1) oder ausgehend (0).
ProcName	Der Prozess, der die Verbindung initiiert hat. Kann mit einer Liste der laufenden Dienste verglichen werden.
Protocol	Das Verbindungsprotokoll[16]
Reason	Ein numerischer Wert, der den Grund für die Entscheidung darstellt, warum die Verbindung zugelassen oder blockiert wurde.
RemoteHost	Der Remote-Host
RemoteIP	Die Remote-IP-Adresse
RemotePort	Der Remote-Verbindungsport
RuleID	Die Kennung der Regel, welche die Entscheidung darüber gesteuert hat, ob die Verbindung zugelassen oder blockiert wird. Entspricht der Kennung in einer der Regeltabellen der SQLite-Datenbank „GDFwSvc.dat“.

In der Spalte REASON wird für jede Verbindung ein numerischer Wert angezeigt. Dieser Wert liefert zusätzliche Informationen darüber, warum die Verbindung zugelassen oder blockiert wurde. Der am häufigsten auftretende Wert ist 7 (REASON_RULE_MATCH), was bedeutet, dass die Verbindung mit einer Regel in einem der definierten Regelsätze übereinstimmte. Die vollständige Liste der Werte lautet wie folgt:

Wert	Grund
0	REASON_FILTER_OFF
1	REASON_FLUSHED
2	REASON_ASK_USER_CACHE
3	REASON_ASK_USER_WRONG_CHECKSUM

[16] Die Protokollnummer kann in der IANA-Datenbank für Protokollnummern (www.iana.org/assignments/protocol-numbers) nachgeschlagen werden.

4	REASON_ASK_USER
5	REASON_ASK_USER_NO_FRONTEND
6	REASON_ASK_USER_NO_PROCESS
7	REASON_RULE_MATCH
8	REASON_RULE_MATCH_WRONG_CHECKSUM
9	REASON_SKIP_ID
10	REASON_SUBSEQUENTLY
11	REASON_BY_CONNECTION
12	REASON_ENDPOINT_DOES_NOT_EXIST
13	REASON_ADAPTIVE_MODE
14	REASON_ANSWER_FROM_OUTGOING
15	REASON_RULESET_DEFAULT
16	REASON_ANSWER_FROM_INCOMING
17	REASON_RULE_MATCH_WRONG_PARENT_CHECKSUM
18	REASON_RULE_MATCH_UNMATCHING_PARENT
19	REASON_ASK_USER_WRONG_PARENT_CHECKSUM
20	REASON_ASK_USER_UNMATCHING_PARENT
21	REASON_PROCESS_DIED
22	REASON_TCP_ENDPOINT_IS_NOT_LISTENING
23	REASON_RULE_MATCH_WRONG_MODULE_CHECKSUM
24	REASON_JUST_OUTGOING
25	REASON_DHCP_POLICY
27	REASON_FIREWALL_OFF
28	REASON_ICS
29	REASON_WRONG_CHECKSUM_COMMITTED_BY_AV
30	REASON_AUTOPILOT

14. PolicyManager

Der PolicyManager ist Teil der Lösungen Endpoint Protection Business und Managed Endpoint Security.

Sicherheitsebenen wie Firewall, Dateisystemwächter oder On-Demand-Schutz blockieren Infizierungsversuche und liefern Endbenutzern eine sichere Computerumgebung ohne Malware. Viele Unternehmensrichtlinien definieren aber andere Inhaltsarten, die nicht zugänglich sein sollten. Unangemessener Inhalt wird oft blockiert, Anwendungen werden auf die Blacklist gesetzt oder der Internetzugang wird eingeschränkt. Ebenso wird oft die Verwendung externer Geräte mit Clients beschränkt, indem die Nutzung von USB-Sticks verboten wird. Alle diese Maßnahmen haben gemeinsam, dass sie nicht nur für die Netzwerksicherheit konfiguriert werden, sondern auch die Client-Nutzungsrichtlinien erzwingen. Der PolicyManager von G DATA vereinheitlicht diese Ansätze in einem benutzerfreundlichen Modul, mit dem sich Clients für genau die Art von Nutzung konfigurieren lassen, für die sie gedacht sind.

Vor der Definition von Richtlinien sollten Administratoren eine vollständige Übersicht über die Client-Rollen im Netzwerk und die gewünschte Anzahl an Rechten für Endbenutzer erarbeiten. Clients, die in der IT-Abteilung genutzt werden, haben beispielsweise andere Berechtigungen als die im Vertrieb oder in der F&E. Gleichzeitig kann es unternehmensweite Regeln geben, die auf alle Clients angewandt werden sollten: Wenn das Unternehmen allgemeine Sicherheitsrichtlinien definiert hat, können diese dabei helfen, die entsprechenden PolicyManager-Regeln aufzustellen. Ein unternehmensweites Verbot von USB-Sticks lässt sich beispielsweise mit dem Bereich GERÄTEKONTROLLE von PolicyManager leicht umsetzen. Mit einer Kombination aus ANWENDUNGSKONTROLLE, GERÄTEKONTROLLE und WEB-INHALTSKONTROLLE lassen sich Regeln erstellen, die gewährleisten, dass keinerlei sensible Daten das Unternehmensnetzwerk verlassen können, weder über Filesharing-Anwendungen noch über USB-Sticks oder eine Cloud-Speicherung.

Der PolicyManager lässt sich dazu verwenden, bestimmte Aspekte der Client-Nutzung einzuschränken. Die Fähigkeit der Endbenutzer zur effektiven Nutzung des PC sollte jedoch nicht beschränkt werden. Wie bei allen anderen Sicherheitsaspekten auch sollten die Richtlinien nicht sofort auf allen Clients bereitgestellt werden. Jede Richtlinienänderung sollte auf einem oder mehreren Testclients getestet werden, um ihre Auswirkungen richtig einschätzen zu können. Sie sollte nur zur Standardrichtlinie für alle Clients hinzugefügt werden, wenn sie wie beabsichtigt funktioniert.

Das PolicyManager-Modul ist in vier Bereiche unterteilt: ANWENDUNGSKONTROLLE, GERÄTEKONTROLLE, WEB-INHALTSKONTROLLE und INTERNETNUTZUNGSZEIT. Jeder der Bereiche kontrolliert einen bestimmten Aspekt der Client-Nutzung und kann für sich aktiviert oder deaktiviert werden. Wie üblich gelten die Einstellungen für die Clients, die in der Ansicht CLIENTS ausgewählt wurden. Die PolicyManager-Module können für normale Client-Endbenutzer oder für normale Client-Endbenutzer und Administratoren aktiviert werden. Die letztere Einstellung empfiehlt sich für eine optimale Sicherheit besonders dann, wenn lokale Administratoren nicht die Richtlinienregeln umgehen dürfen.

14.1. Anwendungen

Wenn man Endbenutzern erlaubt, Anwendungen auf einem Client auszuführen, kann das für die Sicherheit und Richtlinie zur einer Problemquelle werden. Software aus unbekannter Quelle kann Malware enthalten. Außerdem könnte eine große Gruppe von Anwendungen als unerwünschte Software ausgewiesen werden. In den meisten Unternehmensszenarien brauchen Endbenutzer beispielsweise

keine Peer-to-Peer-Downloadsoftware. Instant-Messaging-Anwendungen sind eine weitere Art von Software, die oft blockiert wird. Mit der Anwendungskontrolle können die Administratoren Anwendungsrollen mithilfe einer Black- oder Whitelist, die sich je nach Client konfigurieren lässt, verwalten und erzwingen.

Bevor entschieden werden kann, ob eine Anwendung auf die Whitelist oder die Blacklist gesetzt werden soll, sollten sich die Administratoren bewusst sein, welche Software auf den Netzwerk-Clients läuft. Die Software-Liste enthält nicht nur Pakete, die offiziell bereitgestellt wurden. Wenn es keine Einschränkungen hinsichtlich der Installation von neuer Software gibt, könnten Endbenutzer weitere Anwendungen installiert haben. Eine Übersicht über die Software, die auf einem Client in Gebrauch ist, kann mithilfe des Moduls CLIENTS gewonnen werden. Der darin enthaltene Bereich SOFTWARE zeigt alle Programme an, die auf einem Client installiert wurden. Mithilfe dieser Informationen kann entschieden werden, welche Anwendungen zulässig sind und welche nicht. Die Software kann vorläufig mithilfe der Whitelist- und Blacklist-Funktionen des Software-Inventars sortiert werden. Für jedes Programm muss entschieden werden, ob es auf Client-PCs zulässig sein soll oder nicht. Dazu wird nach einem Rechtsklick die Option ZUR WHITELIST HINZUFÜGEN oder AUF DIE BLACKLIST SETZEN ausgewählt. Über die Schaltflächen NETZWERKWEITE BLACKLIST und NETZWERKWEITE WHITELIST lassen sich die entsprechenden Listen anzeigen, die dann als Grundlage für die Entscheidungsfindung im Modul ANWENDUNGSKONTROLLE genutzt werden können. Dabei muss die Spalte HERSTELLER beachtet werden, da der Herstellername zum Anlegen einer Blacklist- oder Whitelist-Regel in PolicyManager verwendet werden kann.

Damit die Anwendungskontrolle richtig funktioniert, muss die Komponente „Dateisystemwächter“ im G DATA Security Client aktiviert sein (siehe Abschnitt 8.2.1). Für jeden Client kann gewählt werden, ob die Anwendungskontrolle im Blacklist- oder im Whitelist-Modus funktionieren soll. Im Blacklist-Modus werden alle in der Anwendungsliste definierten Anwendungen blockiert, wenn ein Endbenutzer sie auszuführen versucht. Der Whitelist-Modus erlaubt nur die Ausführung der Anwendungen in der Liste und blockiert alle anderen. Es ist zwar möglich, für verschiedene Clients verschiedene Modi zu definieren, aber es empfiehlt sich, den gleichen Modus für alle Clients zu verwenden, um die Verwaltung einfacher zu gestalten. Der Whitelist-Modus ist der sicherste Modus: Es können nur Anwendungen ausgeführt werden, die als sicher gelten. Die Definition einer Whitelist verlangt aber, dass die Administratoren vor der Installation der Richtlinie einige Tests durchführen. Denn sie sollten jedes Programm kennen, das zulässig sein soll, damit Endbenutzer bei der Arbeit nicht auf Blockaden stoßen. Die Alternative ist der Blacklist-Modus: Die Administratoren müssen nur die Programme definieren, die sie nicht zulassen möchten. Die Schattenseite einer Blacklist ist aber, dass sie sich nicht automatisch um die Programme kümmert, die dem Administrator bei der Definition der Blacklist nicht bekannt waren. Wenn ein Endbenutzer selbst ein Programm installiert, wird dies beim Betrieb im Blacklist-Modus nicht automatisch blockiert.

Eine neue Regel hinzuzufügen, ist unkompliziert und wird entweder nach Hersteller, Datei oder Verzeichnis definiert. Eine Herstellerregel blockiert oder erlaubt ausführbare Dateien basierend auf ihrer Herstellerzeichenfolge. Besonders bei der Nutzung des Whitelist-Modus muss sichergestellt sein, dass wenigstens das Betriebssystem und die Sicherheitskomponenten von G DATA richtig geladen werden können. Dazu wird eine Herstellerregel mit der Zeichenfolge **Microsoft*** bzw. **G DATA*** hinzugefügt oder es werden die entsprechenden Standardregeln verwendet. Wenn ein Hersteller generell – mit Ausnahme von einem oder mehreren Programmen – blockiert werden soll, können dessen ausführbare Dateien oder Ordner als Ausnahme von dieser konkreten Regel definiert werden. Dateiregeln lassen sich hinzufügen,

indem Eigenschaften der zu blockierenden Datei eingegeben werden, wie z. B. Dateiname, MD5-Prüfsumme, Produktname, Dateiversion oder Copyright. Diese Felder können manuell eingegeben oder automatisch mithilfe der Option MERKMALE EINER DATEI ERMITTELN befüllt werden. Dadurch kann der Administrator die Datei auswählen, um sich zu vergewissern, ob die Eigenschaften korrekt eingegeben wurden. Am Anfang oder Ende einer der Eigenschaftszeichenfolgen kann ein Sternchen stehen. Dies ist besonders praktisch, wenn nur ein bestimmter Versionsbereich blockiert werden soll. Mit einer Verzeichnisregel können Administratoren einen Ordner wählen, aus dem ausführbare Dateien blockiert oder zugelassen werden sollen. Optional können dabei auch Unterordner mit einbezogen werden.

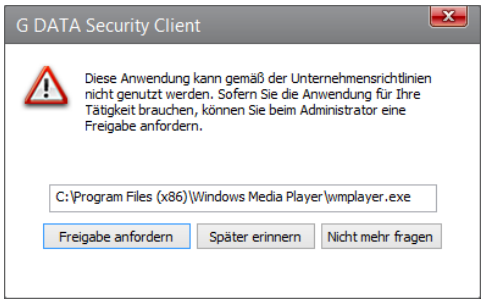

Abbildung 50: G DATA Security Client – Anwendungskontrolle

Wenn alle Regeln definiert wurden und die Anwendungskontrolle für die entsprechenden Clients aktiviert wurde, muss die korrekte Funktion aller Regeln getestet werden. Versucht ein Endbenutzer, eine blockierte Anwendung zu starten, verhindert der G DATA Security Client automatisch den Zugriff. Wenn der Administrator die Option DER BENUTZER DARF BLOCKIERTE ANWENDUNGEN MELDEN aktiviert hat, öffnet der Security Client ein Popup-Fenster mit Einzelheiten der Anwendung. Mit der Schaltfläche FREIGABE ANFORDERN kann dem Modul SICHERHEITSEREIGNISSE im G DATA Administrator ein Bericht hinzufügt werden. Mithilfe dieses Berichts kann der Administrator direkt eine neue Regel zur Anwendungskontrolle hinzufügen und die Anwendung auf die Whitelist setzen, wenn der Endbenutzer sie verwenden darf. Für Clients, bei denen Anwendungen ohne Interaktion oder Rückmeldung des Benutzers blockiert werden sollen, empfiehlt es sich, diese Option deaktiviert zu lassen.

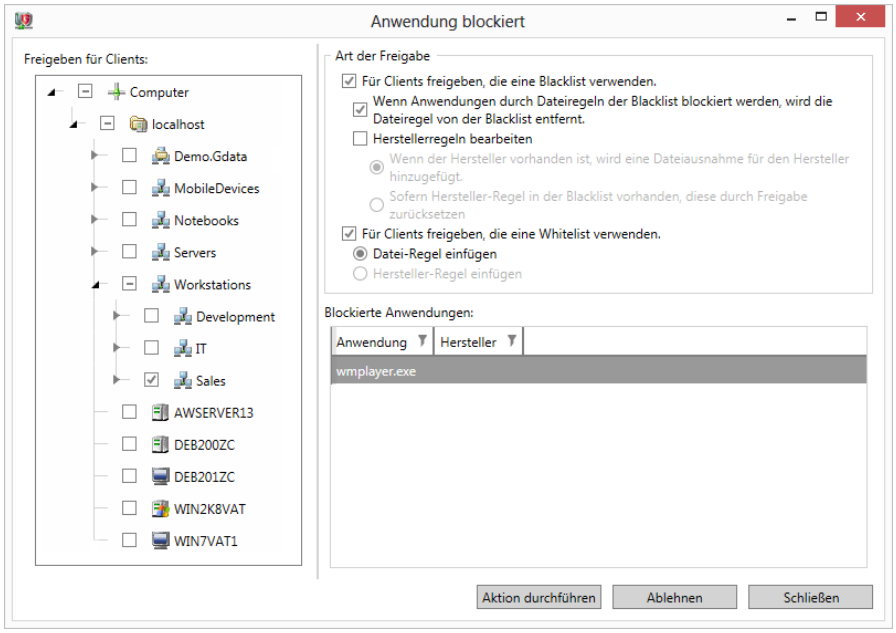

Abbildung 51: G DATA Administrator – Sicherheitsereignisse, Anwendung blockiert

Der Bericht, den die Anwendungskontrolle im Modul SICHERHEITSEREIGNISSE hinzufügt, erlaubt eine gewisse Flexibilität bei der Definition einer Regel. Die blockierte Anwendung erscheint in der unteren rechten Ecke. Links können der oder die Clients ausgewählt werden, für die die neue Regel angelegt werden soll. Standardmäßig ist das der Client, von dem der Bericht gesendet wurde. Die Anwendungen können aber für jeden der Netzwerk-Clients auf die Whitelist oder Blacklist gesetzt werden. Die ART DER FREIGABE lässt sich für den Blacklist- und den Whitelist-Modus noch weiter optimieren. Für Clients, die eine Blacklist verwenden, kann die Regel entfernt werden, die die betroffene Anwendung blockiert. Wenn sie von einer Herstellerregel blockiert wird, kann die Datei als Ausnahme von dieser Regel hinzugefügt oder die Regel als Ganze entfernt werden. Für Clients, die eine Whitelist verwenden, kann das Programm als Dateiregel oder Herstellerregel hinzugefügt werden.

14.2. Geräte

Die meisten bösartigen Bedrohungen stammen aus dem Internet, aber auch Wechseldatenträger sind immer noch ein sehr beliebter Angriffsvektor für Malware. Wechseldatenträger wie USB-Sticks und CD-ROMs können Viren enthalten, aber Administratoren sollten sich nicht nur Sorgen über Angriffe machen: Sensible Dateien könnten das Unternehmensnetzwerk über Wechseldatenträger verlassen, beispielsweise dann, wenn ein Mitarbeiter eine wichtige Datenbank auf einen USB-Stick kopiert. Auch Webcams, die oft in Laptops eingebaut sind, aber aus Gründen des Datenschutzes deaktiviert werden können, stellen eine heikle Gerätekategorie dar. Mit dem Bereich GERÄTEKONTROLLE können Administratoren die Kontrolle über diese Gerätekategorien auf allen Netzwerk-Clients übernehmen.

Der Administrator kann pro Gerätekategorie Zugriffsrechte definieren. Diese sind für Disketten, CDs/DVDs, Wechseldatenträger und Webcams identisch: LESEN/SCHREIBEN, LESEN oder ZUGRIFF VERBIETEN. Wenn LESEN/SCHREIBEN ausgewählt ist, haben die Benutzer vollen Zugriff auf das oder die ausgewählten Geräte. Der LESEZUGRIFF ist in den Situationen eine nützliche Option, in denen die Endbenutzer Daten auf einen Client, aber nicht von einem Client kopieren dürfen. ZUGRIFF VERBIETEN ist die beste Option, wenn ein Gerät komplett blockiert werden soll. Dies ist die sicherste Funktion: Die Geräte können Clients nicht mit Malware infizieren und sie können nicht dazu verwendet werden, um Daten aus dem Unternehmensnetzwerk nach außen zu tragen.

Die vollständige Blockierung von Gerätekategorien ist der einfachste Teil der Nutzung der GERÄTEKONTROLLE. Es kann aber Situationen geben, in denen Endbenutzer oder Administratoren ein Gerät lokal nutzen möchten, trotz eines netzwerkweiten Verbots. Anstatt einen LESE- oder LESE-/SCHREIBZUGRIFF für alle Geräte in einer Kategorie zu aktivieren, können die Administratoren mit der Whitelist-Funktion spezifische Geräte definieren, die benutzt werden dürfen. Wenn eine Gerätekategorie auf LESEN oder ZUGRIFF VERBIETEN eingestellt wurde, können mithilfe der Whitelist LESE- oder LESE-/SCHREIBBERECHTIGUNGEN zu einem bestimmten Gerät oder Datenträger hinzugefügt werden. Vor der Einführung einer Geräterichtlinie sollten die wesentlichen Geräte- oder Medienberechtigungen auf die Whitelist gesetzt werden, um Störungen der Workflows auszuschließen.

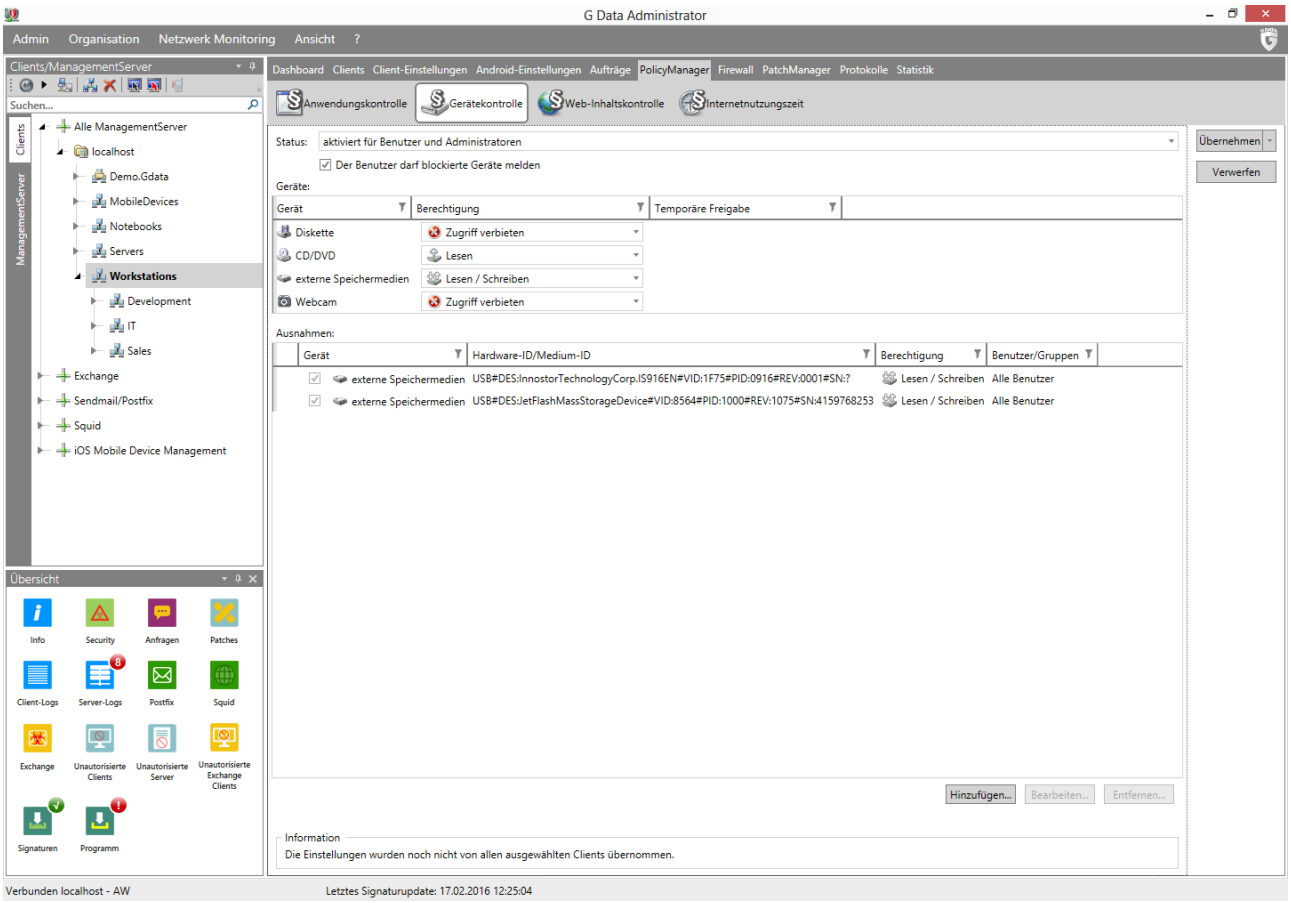

Abbildung 52: G DATA Administrator – PolicyManager, Gerätekontrolle

Durch Klicken auf die Schaltfläche NEU wird das Popup-Fenster für einen Whitelist-Eintrag geöffnet. In dem Fenster sind nur die Gerätekategorien aufgeführt, die in der Gerätekategorieliste eingeschränkt wurden. Gerätekategorien, denen LESE-/SCHREIBBERECHTIGUNGEN zugewiesen wurden, werden nicht blockiert und benötigen daher auch keine Whitelist-Einträge. Mit dem Feld HARDWARE-ID/MEDIUM-ID wird das Gerät bzw. Medium definiert, das der Whitelist hinzugefügt werden soll. Mit der Schaltfläche … kann die korrekte ID bestimmt werden, die auf die Whitelist gesetzt werden soll. Das Popup-Fenster ermöglicht eine Suche auf lokalen Geräten oder auf Geräten eines beliebigen Netzwerk-Clients. Durch die Auswahl einer Hardware-ID kann ein ganzes Gerät auf die Whitelist gesetzt werden. Beispielsweise kann bei einem System, bei dem alle DVD-Laufwerke blockiert sind, ein DVD-Laufwerk als Ausnahme definiert sein. Eine Medium-ID hingegen hilft dabei, ein bestimmtes Medium auf die Whitelist zu setzen. Bei einem System mit blockierten DVD-Laufwerken kann beispielsweise die Berechtigung zur Nutzung einer bestimmten CD oder DVD hinzugefügt werden. Das ist auch für Clients praktisch, die keinerlei Wechseldatenträger nutzen dürfen, aber den Zugriff auf einen bestimmten (unternehmensverwalteten) USB-Stick benötigen. Die Ausnahmen können auf konkrete Windows-Benutzer bzw. Benutzergruppen begrenzt werden. Dies ist besonders dann hilfreich, wenn Benutzer oder Abteilungen auf eine bestimmte Geräteklasse oder ein bestimmtes Medium zugreifen müssen, das zuvor im gesamten Netzwerk blockiert wurde (beispielsweise, wenn Benutzer der PR-Abteilung einen USB-Stick benötigen, um ihre Pressemappen vorzubereiten).

Ähnlich wie die Anwendungskontrolle kann auch das Modul „Gerätekontrolle“ seine Arbeit mit oder ohne Interaktion des Benutzers erledigen. Durch Auswahl der Option DER BENUTZER DARF BLOCKIERTE GERÄTE MELDEN

hat der Benutzer die Möglichkeit, den Zugriff auf ein blockiertes Gerät anzufordern. Das Popup-Fenster bietet eine Möglichkeit, eine Berechtigung zur Nutzung des Geräts oder Mediums anzufordern. Dadurch wird im Modul SICHERHEITSEREIGNISSE ein Bericht generiert. Auf der Grundlage des Berichts kann eine Whitelist-Ausnahme hinzugefügt werden. Die Gerätekategorie selbst kann für ausgewählte Clients oder, basierend auf der Geräte- oder Medium-ID, nur für ein bestimmtes Gerät oder Medium aktiviert werden. Die Möglichkeiten für die Whitelist-Funktion hängen von den Daten ab, die im Bericht verfügbar sind. Beim Hinzufügen von Geräteausnahmen ist Vorsicht geboten. Die Entscheidung sollte nicht nur auf den Anforderungen der Benutzer basieren. Nach Möglichkeit sollte man sich das Medium verschaffen, für das die Berechtigung angefordert wurde, und überprüfen, ob diese tatsächlich erforderlich ist. Beim Hinzufügen einer Ausnahme sollte nach Möglichkeit immer mit Medien- und nicht mit Hardware-Ausnahmen gearbeitet werden. Dadurch wird die Gefahr einer unbefugten Gerätenutzung und Malware-Infektion begrenzt. Auch Ausnahmen können für einen konkreten Zeitraum hinzugefügt werden. Wurde ein Gerät vorübergehend zugelassen, wird der Zeitraum im Modul POLICYMANAGER angezeigt und die Ausnahme kann jederzeit storniert werden.

14.3. Web-Inhalt

Ein beliebter Teil von Unternehmensrichtlinien ist die Beschränkung des Zugriffs auf bestimmte Websites. Für das Blockieren einer Website kann es viele Gründe geben. Einer ist die Produktivität: Endbenutzer können daran gehindert werden, Websites zu besuchen, die mit ihren aktuellen Aufgaben nichts zu tun haben, etwa Online-Spiele oder soziale Netzwerke. Des Weiteren kann der Inhalt von Websites ungesetzlich oder unangemessen sein. Filesharing-Websites, nicht jugendfreie Inhalte oder Websites zur Verbreitung von Hacking sind in fast allen Fällen für die Arbeit irrelevant und sollten blockiert werden. Diese Art von Websites findet sich oft in den dunkleren Teilen des Internets, in denen bösartige Webhosts oder gehackte Werbenetzwerke versuchen könnten, Besucher mit Malware zu infizieren.

Bevor eine der Kategorien in der WEB-INHALTSKONTROLLE vom PolicyManager blockiert wird, sollte ein Inventar der unverzichtbaren Websites angelegt werden. Damit gewährleistet ist, dass wichtige Websites nicht versehentlich blockiert werden, sollten diese vor der Einführung einer Richtlinie zu NETZWERKWEITE AUSNAHMEN hinzugefügt werden. Wenn es spezielle Websites gibt, die blockiert werden müssen, sollten auch sie hinzugefügt werden.

Um Zeit und Mühen zu sparen, können Administratoren vordefinierte Website-Kategorien blockieren. Es sind verschiedene Kategorien verfügbar, die nach Art des Inhalts gruppiert sind. Jede Kategorie besteht aus einer Liste von URLs, die auf die Blacklist gesetzt wurden und blockiert werden können. Die Administratoren sollten für jede Netzwerkzone entscheiden, welche Website-Kategorien blockiert werden sollen. Es empfiehlt sich, zumindest ungesetzliche Inhalte zu blockieren (je nach örtlicher Gesetzgebung umfasst dies Kategorien wie kriminelles Fachwissen, Drogen, Filesharing, Glücksspiel und Hacking). Entsprechend den Netzwerkrichtlinien und Wünschen des Administrators können weitere Kategorien aktiviert werden (zugunsten der Produktivität Kategorien wie Blogs, Chats und soziale Netzwerke – unangemessene Inhalte lassen sich mit Kategorien wie „Nicht jugendfreier Inhalt“, „Hass“ oder „Nacktheit“ blockieren).

Wenn in der Ansicht CLIENTS der richtige Client oder die richtige Gruppe ausgewählt wurde, können die zu blockierenden Kategorien gewählt werden. Wenn das Kontrollkästchen vor dem Kategoriennamen

aktiviert ist, ist ein Zugriff auf Websites dieser Kategorie zulässig. Zur Blockierung des Zugriffs wird die Kategorie deaktiviert. Es ist jede beliebige Kombination von Kategorien möglich. Da Kategorien für eine sehr weitreichende Serie von Szenarien zur Verfügung gestellt werden, empfiehlt es sich nicht, den Zugriff auf alle gleichzeitig zu blockieren, da dies den Website-Zugriff erheblich behindern würde. Die Administratoren sollten eine spezifische Auswahl auf der Grundlage der Arten von Websites treffen, die die Mitarbeiter besuchen dürfen oder nicht. Zusätzlich zur Kategorieliste können Websites mithilfe der NETZWERKWEITE AUSNAHMEN blockiert oder zugelassen werden. Die Ausnahmen gelten für das gesamte Netzwerk, damit der Administrator umgehend alle Clients konfigurieren kann. Beispielsweise können Websites, die für Workflow-Prozesse unerlässlich sind, oder auch die eigene Website des Unternehmens auf die Whitelist gesetzt werden.

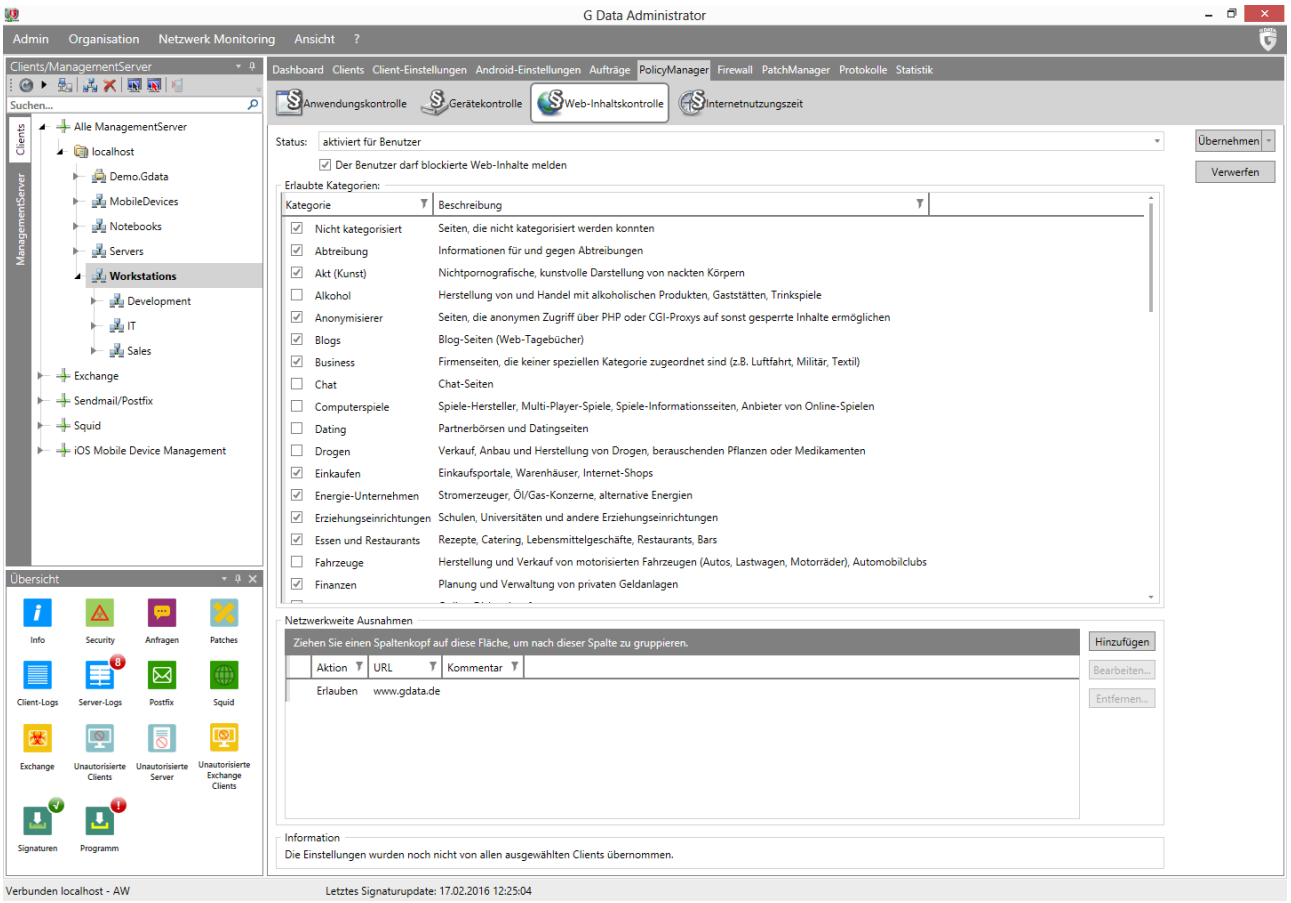

Abbildung 53: G DATA Administrator – PolicyManager, Web-Inhaltskontrolle

Die Web-Inhaltskontrolle ist von der Scan-Ebene des HTTP-Datenverkehrs abhängig (siehe Abschnitt 8.1). Das bedeutet, dass die Option zur Verarbeitung von Internetinhalten für jeden Client aktiviert werden sollte, auf dem die Web-Inhaltskontrolle eingesetzt werden soll. INTERNETINHALTE (HTTP) VERARBEITEN kann auf der Registerkarte WEB des Moduls CLIENT-EINSTELLUNGEN aktiviert werden. Wenn der Client einen Proxy-Server nutzt, kann dieser auf derselben Registerkarte aktiviert werden. Wenn ein Endbenutzer im Browser eine URL anfordert, überprüft der G DATA Security Client die URL anhand der zentralen URL-Liste von G DATA, um ihre Kategorie anzufordern. Wenn die Kategorie blockiert ist oder die Website auf der netzwerkweiten Blacklist steht, wird die Anforderung verweigert und die Seite nicht geladen. Wenn es Latenzprobleme gibt und das Nachschlagen der Kategorie innerhalb von 1.000 Millisekunden kein Ergebnis liefert, wird die Website geladen. Wenn die Option DER BENUTZER DARF BLOCKIERTE WEB-INHALTE MELDEN

aktiviert ist, erscheint jedes Mal ein Popup-Fenster, wenn eine Website blockiert ist. Der Benutzer kann den Zugriff auf die Website anfordern, wodurch im Modul SICHERHEITSEREIGNISSE ein Bericht generiert wird. Der Administrator kann dann entweder den Zugriff auf die komplette Kategorie (für jeden Client und jede Gruppe) erlauben oder die Website auf die netzwerkweite Whitelist setzen.

14.4. Internetnutzungszeit

Das vierte und letzte PolicyManager-Modul legt den Schwerpunkt nicht auf das Filtern, sondern auf das komplette Blockieren von Internetinhalten. Wie bei allen Richtlinien gibt es auch hier eine Richtlinien- und eine Sicherheitskomponente. Was die Richtlinie angeht, können Administratoren den Internetzugang auf bestimmte Tageszeiten beschränken, ihn auf eine maximale kumulative Zeitspanne beschränken oder ihn komplett blockieren. Mitarbeiter, die keinen Internetzugriff benötigen, können so dazu gezwungen werden, sich auf ihre Aufgaben zu konzentrieren, oder dürfen das Internet nur während der Mittagspause nutzen. Darüber hinaus sorgt die Einschränkung des Internetzugriffs für Sicherheit, da sie die Zeitspanne verkürzt, in der der Angriffsvektor verfügbar ist. Es muss aber genau überlegt werden, in welchen Szenarien er genutzt werden kann. Durch die Blockierung des Internetzugriffs werden Workflows stark eingeschränkt, die davon abhängig sind, Informationen online abzurufen oder zu veröffentlichen.

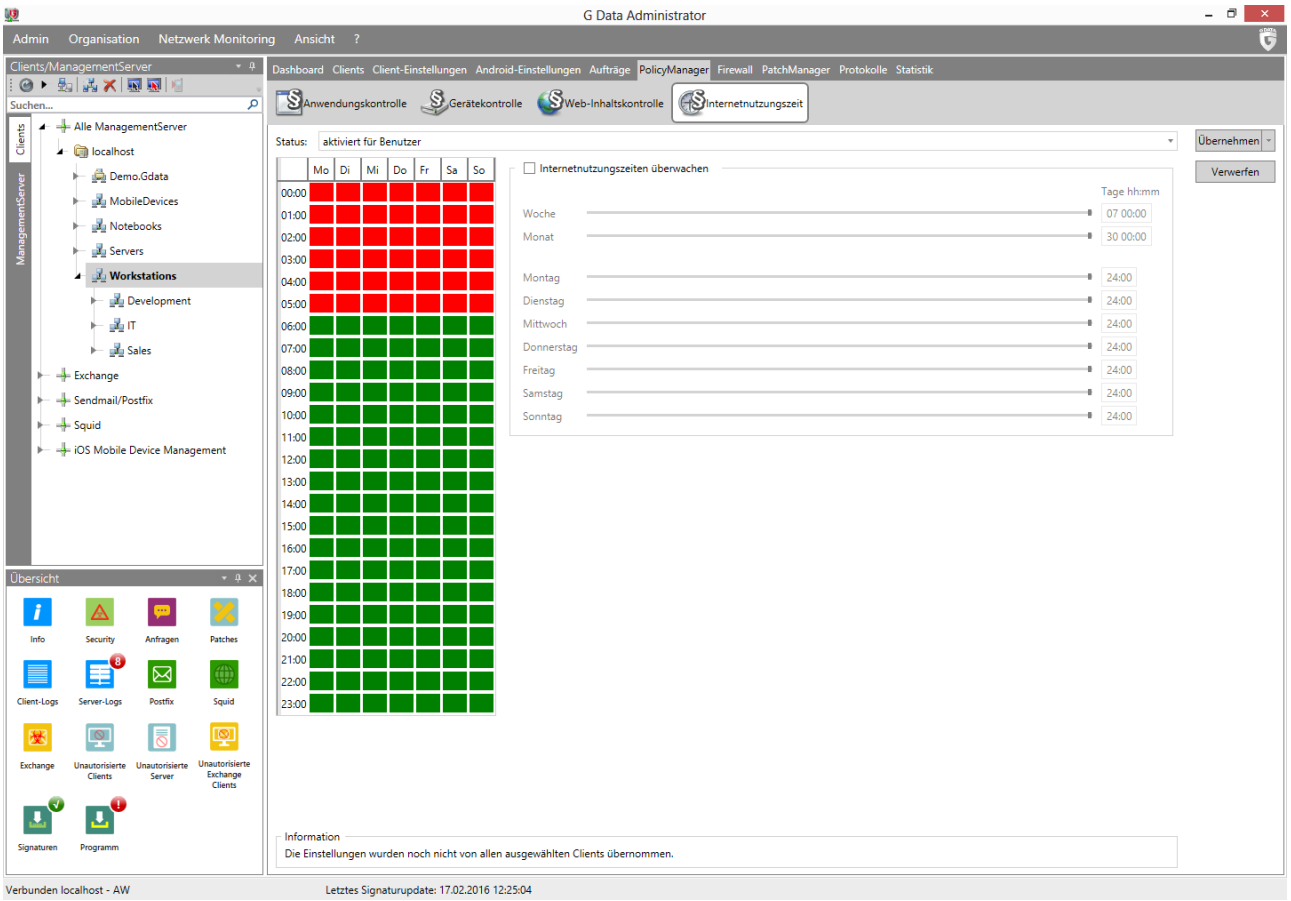

Abbildung 54: G DATA Administrator – PolicyManager, Internetnutzungszeit

Der Bereich INTERNETNUTZUNGSZEIT im PolicyManager enthält zwei wichtige Komponenten. Links zeigt das Raster an, zu welchen Zeiten an welchen Wochentagen der Internetzugriff gewährt oder eingeschränkt werden soll. Mit dem Zeitraster lassen sich verschiedene Konfigurationen in Kraft setzen. Um mehrere

Zeitfenster gleichzeitig auszuwählen, kann darauf geklickt und es gezogen oder alternativ die Tastenkombination Strg + Klicken bzw. Umschalt + Klicken genutzt werden. Mit einem Rechtsklick wird ausgewählt, ob die Internetnutzung für diese Zeitfenster blockiert oder zugelassen werden soll. Um beispielsweise zu gewährleisten, dass der Internetzugriff nur während der Mittagspause möglich ist, werden alle Zeitfenster (Strg + A) ausgewählt, mit der rechten Maustaste darauf geklickt und die Option ZEIT SPERREN ausgewählt. Anschließend wird die Uhrzeit der Mittagspause ausgewählt, mit der rechten Maustaste darauf geklickt und die Option ZEIT FREIGEBEN ausgewählt. Wenn ein Endbenutzer versucht, auf eine Website zuzugreifen, während der Internetzugriff blockiert ist, erscheint im Browser eine Warnseite. Es ist zu beachten, dass Einschränkungen des Internetzugriffs durch eine Veränderung der Ortszeiteinstellung umgangen werden könnten. Falls die Einstellung noch nicht aktiviert wurde, empfiehlt es sich, mithilfe eines Gruppenrichtlinienobjekts die Endbenutzer an einer Änderung der Ortszeiteinstellungen zu hindern.

Auf der rechten Seite können mit einer Reihe von Schiebereglern tägliche, wöchentliche oder monatliche Nutzungsgrenzen definiert werden. Diese Grenzen werden getrennt vom und zusätzlich zum Zeitraster erzwungen. Die Schieberegler lassen sich aktivieren, indem das Kontrollkästchen INTERNETNUTZUNGSZEITEN ÜBERWACHEN aktiviert und anschließend die maximale Zeitspanne eingegeben wird, in der das Internet genutzt werden darf. Standardmäßig ist der Internetzugriff immer verfügbar: 30 Tage im Monat, 7 Tage die Woche und 24 Stunden am Tag. Mit den Schiebereglern kann diese Zeitspanne verkürzt werden. Alternativ kann die Zeit auch manuell eingegeben werden. Wenn man beispielsweise im Wochenfeld **04 20:05** eingibt, bedeutet das, dass die Internetnutzung 4 Tage, 20 Stunden und 5 Minuten erlaubt ist. Sobald die zulässige Internetnutzung für einen bestimmten Zeitraum überschritten ist, sehen die Benutzer eine Warnseite, wenn sie eine Website öffnen. Bei einem Konflikt zwischen den Zeiteingaben wird die kürzeste Zeitspanne verwendet. Wenn beispielsweise eine Zeitgrenze von vier Tagen im Monat definiert ist, aber eine wöchentliche Grenze von fünf Tagen eingestellt ist, begrenzt die Software die Internetnutzung automatisch auf vier Tage.

Wie die WEBINHALTSKONTROLLE (siehe Abschnitt 14.3) ist auch die INTERNETNUTZUNGSZEIT von der Scan-Ebene des HTTP-Datenverkehrs abhängig. Das bedeutet, dass die Option zur Verarbeitung von Internetinhalten für jeden Client aktiviert werden sollte, auf dem die Internetnutzungszeit nachverfolgt werden soll. Der Datenverkehr an anderen Ports als denen, die für die Scan-Ebene des HTTP-Datenverkehrs definiert wurden, wird nicht überwacht.

15. PatchManager

Das PatchManager-Modul ist optional verfügbar.

Mit Patches werden oft Sicherheitslücken repariert, durch die Angreifer Zugriff auf Systeme erhalten könnten, auf denen die betroffene Software ausgeführt wird. Bei der Reaktion auf Sicherheitsnotfälle kommt es auf die schnelle Installation der Patches an. Als erschwerender Faktor kommt hinzu, dass die Veröffentlichung eines Patches aufgrund der öffentlichen Bekanntgabe von Informationen über die Sicherheitslücke, die üblicherweise mit Patch-Freigaben einhergeht, Hacker dazu anspornt, einen Exploit für den Sicherheitsbug zu entwickeln. Durch das Rückentwickeln von Patch-Dateien können Angreifer die Informationen erhalten, die für einen wirksamen Angriff notwendig sind. Dadurch wird zusätzlicher Druck auf die Administratoren ausgeübt, die ihre Systeme rechtzeitig mit Patches versorgen müssen. Die Patch-Verwaltung hilft dabei, die Patch-Installation zu beschleunigen, und verbessert die Effizienz des gesamten Prozesses, indem sie Vorgehensweisen zur Patch-Installation koordiniert und standardisiert, wodurch eine erfolgreiche Ausnutzung von Softwarebugs durch Hacker verhindert wird.

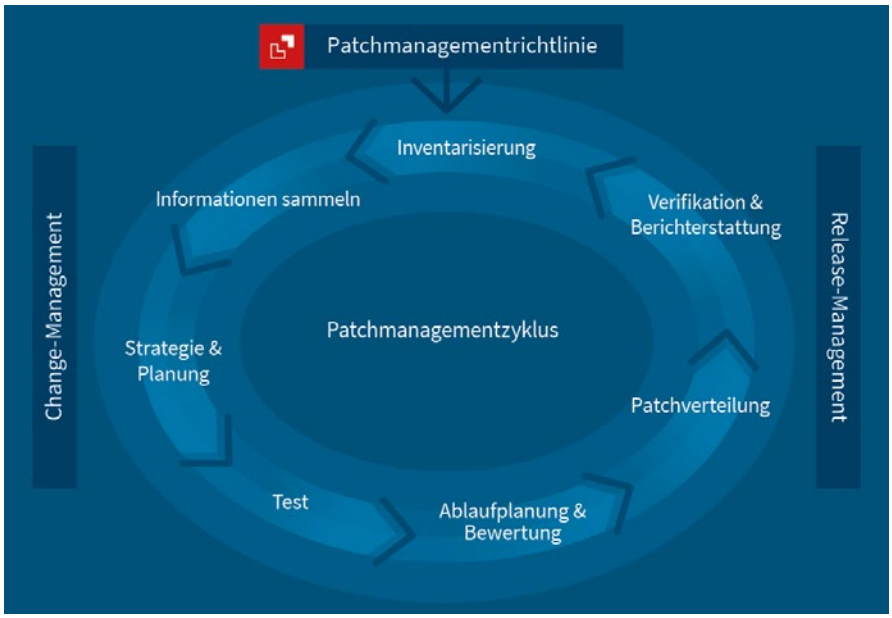

Abbildung 55: Patch-Verwaltungszyklus

Der Patch-Verwaltungszyklus lässt sich in verschiedene Phasen aufteilen (siehe Abschnitte 15.1 bis 15.7)[17]. Je nach ihren Wünschen und Anforderungen können Unternehmen verschiedene Phasen zusammenführen, indem sie sie bündeln und derselben Person zuweisen, oder auch nach Bedarf weitere konkrete Maßnahmen definieren. Vorhandene Standards des Veränderungs- und Release-Managements können (teilweise) integriert werden. Einige Schritte des Verfahrens, vor allem die Installation, lassen sich automatisieren, aber verschiedene Schlüsselaktionen müssen für jeden Zyklus manuell ausgeführt werden. Daher ist die Planung zur Optimierung dieses Prozesses entscheidend. Es kann sehr hilfreich sein, eine Patch-Verwaltungsrichtlinie zu definieren, die sich mit häufigen Fragen befasst. Sollen alle verfügbaren Patches standardmäßig installiert werden oder gibt es eine Klassifizierung, vielleicht basierend auf der Schwere der Sicherheitslücken, die sie beheben? Werden Patches proaktiv installiert (um mögliche Sicherheitslöcher zu stopfen) oder reaktiv (nur beim Auftreten von Problemen) oder in

[17] Eine theoretischere Übersicht über die verschiedenen Schritte enthält das G DATA TechPaper #0171 „Patchmanagement Praxisleitfaden“.

einer Kombination von beiden? Es empfiehlt sich, so viele verallgemeinerte Regeln wie möglich aufzustellen, um unnötigen Zeitaufwand für Entscheidungen zu jedem einzelnen Patch zu vermeiden. Die Lösung besteht aber auch nicht darin, einfach jedes verfügbare Patch zu installieren: Es muss ganz bewusst ausgewählt werden, um Überlastungs- und Kompatibilitätsprobleme in Netzwerk und System zu verhindern.

Da die Patch-Verwaltung eine zeitaufwendige Aufgabe ist, kann die vollständige Automatisierung eine verlockende Möglichkeit sein. Der PatchManager kann nahezu eigenständig arbeiten: Mit der Registerkarte EINSTELLUNGEN im PatchManager lassen sich automatisierte Einführungen kritischer Patches konfigurieren. Diese Methode gewährleistet zwar, dass die Clients pünktlich mit den neuesten kritischen Patches versorgt werden, es ist aber dennoch nicht ratsam, den PatchManager auf diese Weise zu konfigurieren. Ein Patch mag für einen bestimmten Client durchaus anwendbar sein, das bedeutet aber nicht, dass er sich ohne Probleme installieren lässt. Nach seiner Installation könnten Kompatibilitätsprobleme auftreten und die Verfügbarkeit von System oder Software behindern. Die Patch-Verwaltung sollte immer ein angemessenes Testverfahren beinhalten, und kein Teil des Zyklus sollte nachlässig behandelt werden.

Das Modul PATCHMANAGER unterstützt zwar den SQL Server Express, doch für mittlere bis große Netzwerke wird ein eigener SQL-Server empfohlen.

15.1. Schritt 1: Aktualisierung des Inventars

Zunächst ist es wichtig, ein Inventar der Computer im Netzwerk sowie ihrer Soft- und Hardware zu erstellen und zu pflegen. Mit dem Modul CLIENTS können Administratoren auf eine vollständige Liste der installierten Software für jeden Netzwerk-Client zugreifen. Das Inventar lässt sich organisieren, um verschiedene Arten von Informationen zu liefern. Die Standardansicht zeigt eine einfache Liste der gesamten Software, die auf den ausgewählten Clients installiert ist. Die Liste enthält das Installationsdatum, den Software-Hersteller und die aktuell installierte Version. Durch die Gruppierung der Elemente nach Hersteller und Name steht für jedes Produkt eine schnelle Übersicht zur Verfügung, mit der überprüft werden kann, ob die aktuellste Version auf allen Computern installiert wurde.

An dieser Stelle sollte überprüft werden, ob auf den Netzwerk-Clients Software ausgeführt wird, die nicht zur Standardinstallation gehört. Die Administratoren können nicht die potentiellen Sicherheitsrisiken der gesamten Software kennen. Mit dem Software-Inventar lassen sich nicht sanktionierte Software-Installationen leichter aufspüren. Die Administratoren können dann entscheiden, die Software zu ihrer offiziellen Installationsliste (Whitelist) hinzuzufügen oder sie zu entfernen (Blacklist). Die Benutzer von G DATA Endpoint Protection Business können das PolicyManager-Modul (siehe Kapitel 14) nutzen, um netzwerkweite Richtlinien anzuwenden oder um Software auf die Whitelist oder die Blacklist zu setzen und so die Installation zu kontrollieren.

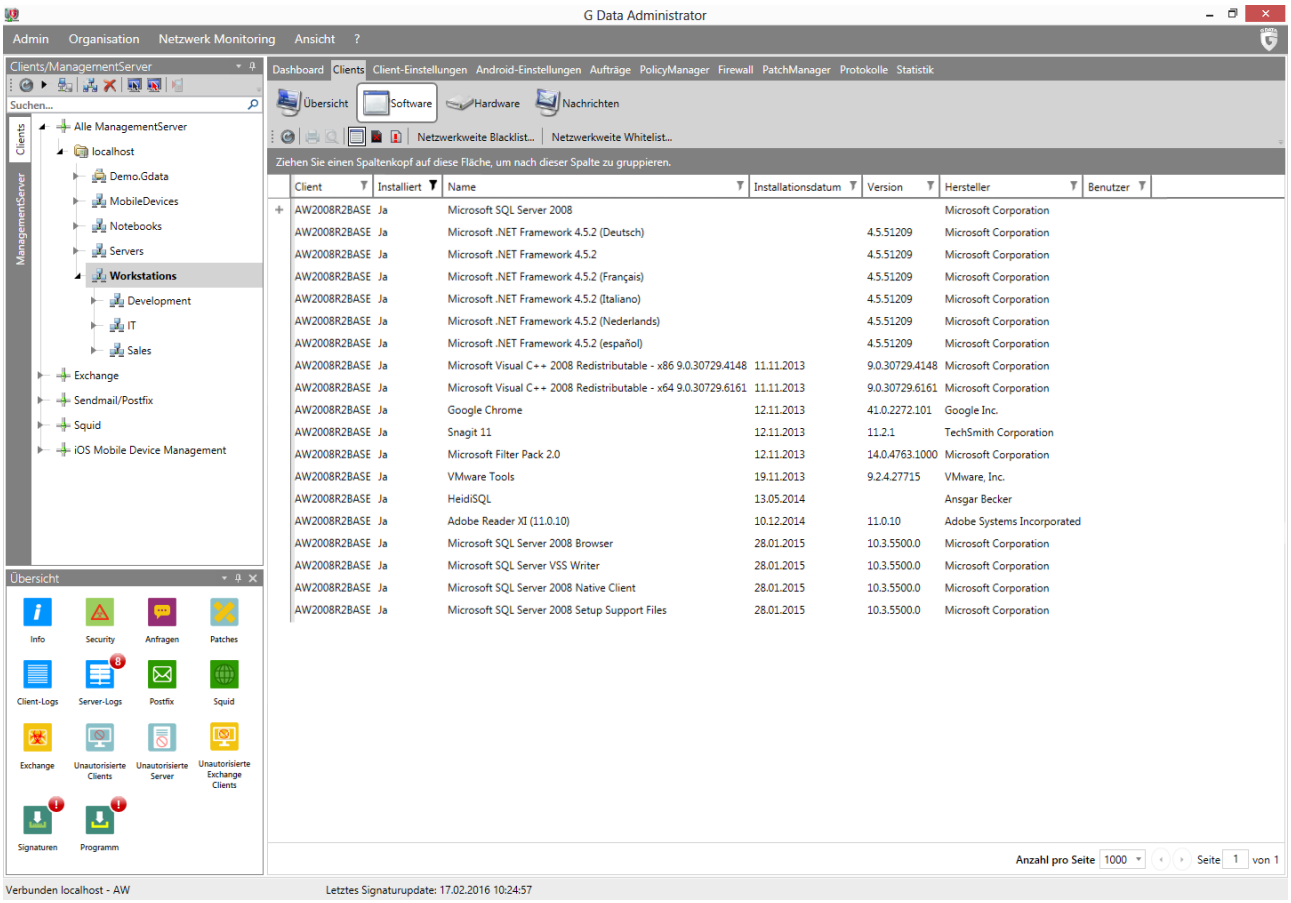

Abbildung 56: G DATA Administrator – Clients, Software

Es ist nicht nur wichtig, die Software nachzuverfolgen; eine erfolgreiche Installation hängt auch von den physischen Voraussetzungen wie etwa den Hardware-Spezifikationen ab. Mit der Funktion des Hardware-Inventars lässt sich eine Vielzahl von Spezifikationen nachverfolgen. Physische Angaben wie CPU-Geschwindigkeit und der Umfang des internen Speichers helfen dabei, Geschwindigkeit und Leistung der Patch-Installation vorherzusagen. Die Menge des freien Festplattenspeichers ist wichtig, um zu verhindern, dass die Patch-Installation Fehler verursacht. Zusätzlich können die Firmware-Versionen von BIOS und Motherboard nachverfolgt werden, um sie mit neu veröffentlichter Firmware zu vergleichen.

15.2. Schritt 2: Sammeln von Informationen

Sobald ein Inventar erstellt wurde, sollten die Administratoren mit den Informationen über die neuesten Patches Schritt halten. Das PatchManager-Modul enthält auf der Registerkarte PATCH-KONFIGURATION eine Liste aller verfügbaren Patches für eine Vielzahl von Produkten. Die Datenbank wird automatisch aktualisiert, sobald die Hersteller einen neuen Patch veröffentlichen. Eine Übersicht über Hersteller, Produkte und Patches lässt sich einer Reihe von Diagrammen oben auf der Registerkarte entnehmen.

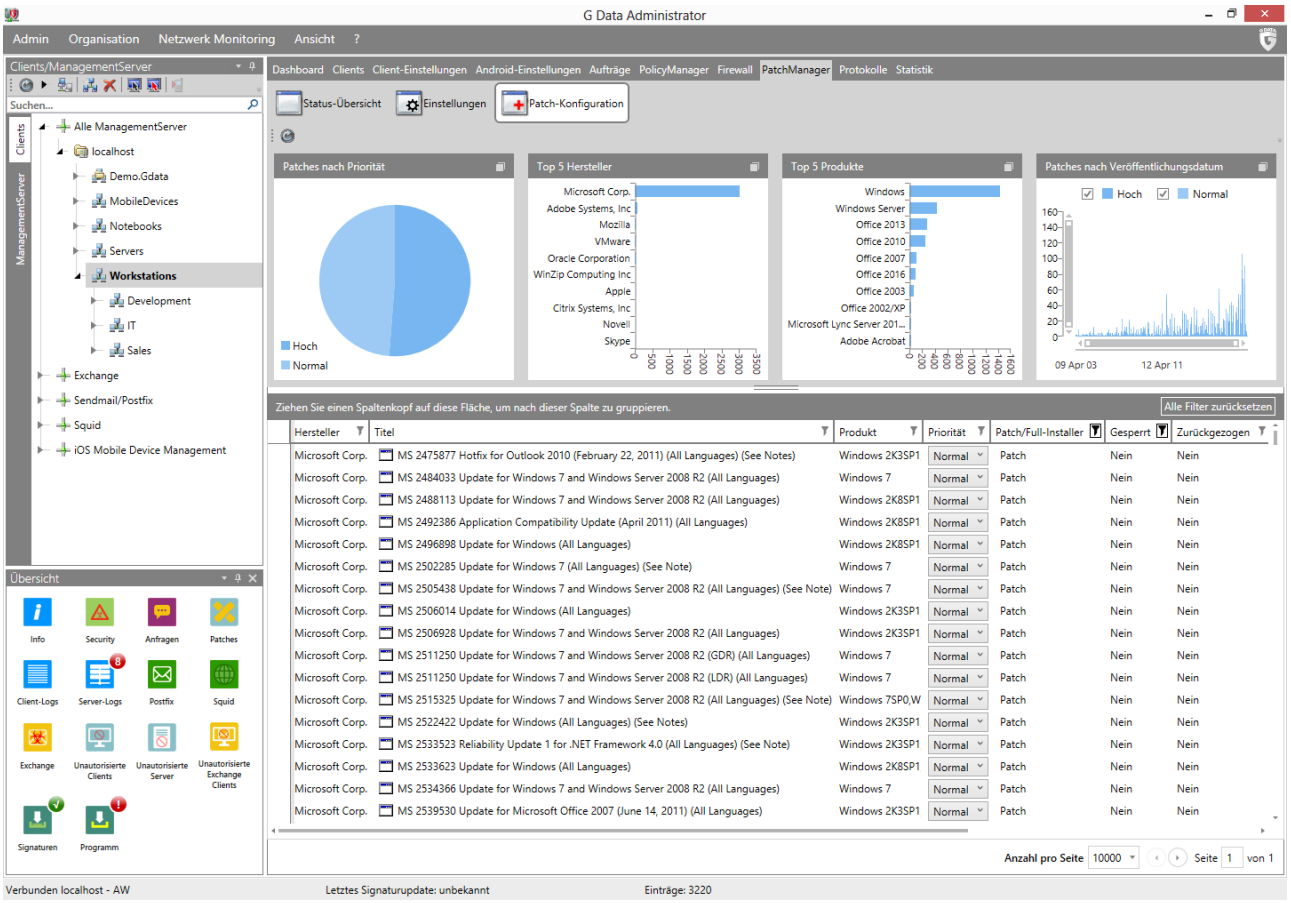

Abbildung 57: G DATA Administrator – PatchManager, Patch-Konfiguration

Die Patch-Liste ist standardmäßig nach HERSTELLER, PRIORITÄT und PRODUKT gruppiert. Dadurch können die Administratoren Patches für ein bestimmtes Produkt schnell nachschlagen. Die standardmäßigen Anzeigefiltereinstellungen schließen vollständige Software-Installationsprogramme ebenso von der Liste aus wie alle blockierten Einträge. Mithilfe der Option ALLE FILTER ZURÜCKSETZEN wird der Anzeigefilter zurückgesetzt. Wenn ein Patch ein anderes Patch ersetzt hat, lässt sich sein Eintrag erweitern, um eine Liste aller Patches einzusehen, die es ersetzt. Es lassen sich weitere Informationen zu einzelnen Patches (oft mit kompletten Versionshinweisen) abrufen, indem mit der rechten Maustaste auf ein Patch geklickt und seine Eigenschaften überprüft werden.

15.3. Schritt 3: Strategie und Planung

Bei jeder Veröffentlichung eines neuen Patches sollte es mit allen Client-Systemen verglichen werden, um festzustellen, ob es sich auf ein Produkt bezieht, das im Netzwerk in Gebrauch ist. Für kritische Patches lässt sich dieser Prozess auf der Registerkarte EINSTELLUNGEN automatisieren. Um ein oder mehrere Patches auf ihre Anwendbarkeit zu überprüfen, kann auf der Registerkarte STATUS-ÜBERSICHT die Option PATCHES AUF ANWENDBARKEIT PRÜFEN ausgewählt werden. Dadurch wird ein SOFTWAREERKENNUNGSAUFTRAG für den bzw. die angegebenen Clients geplant. Alternativ kann ein automatischer Scan für jedes neue Patch ausgeführt werden, das der Datenbank hinzugefügt wird. Dazu gehören kritische ebenso wie weniger kritische Patches. Mit dem Modul AUFTRÄGE kann ein SOFTWAREERKENNUNGSAUFTRAG geplant werden, der sofort ausgeführt wird, wenn ein neues Patch zur Verfügung steht. Der PatchManager überprüft dann die neuen Patches auf allen angegebenen Clients auf ihre Anwendbarkeit. Auch wenn Softwareerkennungsaufträge

anwendbare Patches automatisch installieren können, empfiehlt es sich doch, Patch-Prüfungen im Voraus zu planen (siehe Abschnitt 15.4).

Nach der Prüfung auf Anwendbarkeit werden der bzw. die entsprechenden Server oder Clients in der Ansicht CLIENTS ausgewählt und die Registerkarte STATUS-ÜBERSICHT im PatchManager geöffnet. Die Liste ist standardmäßig nach STATUS, PRIORITÄT, HERSTELLER und PRODUKT gruppiert. Dadurch lassen sich schneller die Patches finden, die anwendbar oder nicht anwendbar sind bzw. bereits installiert wurden. Patches, die für das bzw. die Client-Systeme anwendbar sind, sind diejenigen, die überprüft, getestet und schließlich bereitgestellt werden müssen.

Der PatchManager liefert für jedes Patch eine Reihe von Informationen, um die Entscheidung zu erleichtern, ob ein bestimmtes Patch bereitgestellt werden muss oder nicht. In seiner Listenübersicht zeigt das PatchManager-Modul die Produkte an, für die ein Patch gilt, ebenso sein Veröffentlichungsdatum, seinen offiziellen Titel und seine Priorität. Für jedes Patch werden eine vollständige Beschreibung und normalerweise auch eine URL für die offiziellen Versionshinweise angegeben. Diese Informationen helfen Administratoren bei der Entscheidung darüber, wie schwerwiegend eine bestimmte Sicherheitslücke ist und wie schnell ihr Patch bereitgestellt werden muss. Die bedeutendsten Patches sollten mit einer höheren Priorität als die nicht kritischen Patches installiert werden. Dabei sollte nicht vergessen werden, dass nicht pauschal alle Patches installiert werden sollten. Die Automatisierung der Patch-Verwaltung soll nicht die Entscheidungsfindung aus der Gleichung herausnehmen, sondern genug Einzelheiten liefern, um fundierte Entscheidungen treffen und den Installationsvorgang optimieren zu können. Der PatchManager liefert so viele Informationen wie möglich, aber die Entscheidung darüber, ein Patch zu testen und schließlich bereitzustellen, liegt immer beim Administrator.

15.4. Schritt 4: Testen

Wenn entschieden wurde, dass ein bestimmtes Patch bereitgestellt wird, kann das Testverfahren beginnen. Es wird empfohlen, Patches auf einer Reihe von repräsentativen Computern zu testen. Diese Computer sollten den Clients ähneln, die tatsächlich in Gebrauch sind, damit auf mögliche Probleme getestet werden kann, ohne die tatsächlichen Clients zu stören. Nicht jeder Administrator hat aber Zugang zu genügend vielen Computern, um eine kleine Nachbildung seines Netzwerks aufzubauen. Hier empfiehlt sich die Methode der Virtualisierung; wenn es wirklich keine andere Lösung gibt, kann ein nicht unbedingt notwendiges Teilnetz des Netzwerks genutzt werden. In diesem Fall lässt sich mit dem G DATA Administrator eine Testumgebung in einer oder mehreren Gruppen organisieren. Patches können auf einem oder mehreren Clients in einer oder mehreren Gruppen bereitgestellt werden, um die Installation und ihre Auswirkungen zu beobachten.

Um ein oder mehrere Patches für eine Testgruppe bereitzustellen, wird die Gruppe in der Ansicht CLIENTS ausgewählt. Dazu wird das Modul AUFTRÄGE geöffnet und ein neuer SOFTWAREVERTEILUNGSAUFTRAG angelegt. Anschließend wird das zu verteilende Patch bzw. die Patches ausgewählt und festgelegt, zu welcher Zeit die Verteilung stattfinden soll. Die Auswahl eines Patches lässt sich vereinfachen, wenn man die Patch-Liste nach HERSTELLER oder PRODUKT gruppiert. Dieser Vorgang wird mit allen passenden Patches und für alle passenden Testgruppen wiederholt. Es empfiehlt sich, immer nur einen Patch pro System zu testen, damit sich mögliche Probleme einem konkreten Patch zuordnen lassen.

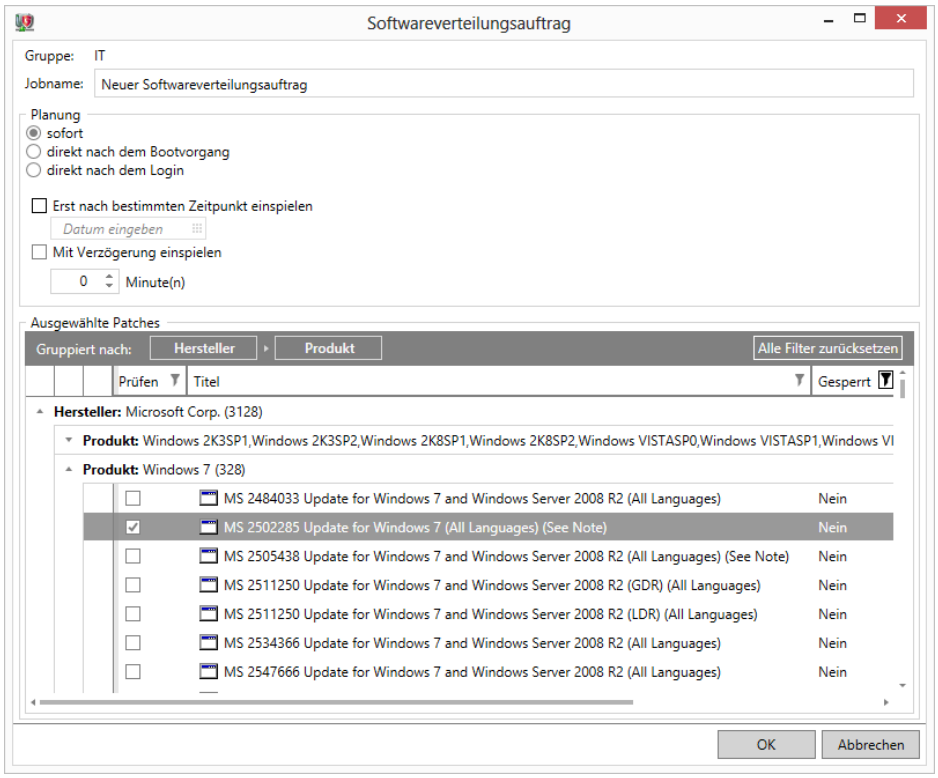

Abbildung 58: G DATA Administrator – Aufträge, Softwareverteilungsauftrag

Während des Testzeitraums und in der Überprüfungsphase nach der Installation lässt sich mithilfe des Moduls REPORTMANAGER herausfinden, welchen Status die bereitgestellten Patches haben und welche Computer potentiell Fehler verursachen (siehe Abschnitt 6.3). Mit dem ReportManager kann der Administrator mehrere Module auswählen, die in einem Bericht zusammengefasst werden. Seine PATCHMANAGER-Kategorie bietet mehrere nützliche Optionen, zum Beispiel die am häufigsten nicht installierten Patches oder Computer mit nicht ausgeführten Softwareverteilungsaufträgen (was auf Installationsprobleme hinweisen kann) oder die Computer mit den häufigsten Patch-Anforderungen oder -Ablehnungen (für eine anschließende Analyse).

Zusätzlich zum ReportManager-Modul kann der Status der Patch-Prüfung auch im Modul AUFTRÄGE eingesehen werden. Dazu wird der entsprechende Auftrag geöffnet und die Einzelheiten überprüft, um sich den Status für jedes Patch anzusehen. Wenn ein Patch nicht erfolgreich bereitgestellt zu sein scheint, sollte das Software-Inventar für diesen Client aktualisiert und erneut überprüft werden. Wenn das Patch nicht bereitgestellt werden kann, wird das System lokal überprüft und eine manuelle Patch-Installation versucht. Wenn ein Patch während der Testphase Probleme verursacht, sollte es nicht in großem Stil bereitgestellt werden, bis die Probleme behoben worden sind.

Die Patch-Prüfung könnte theoretisch übersprungen werden: Der PatchManager kann kritische Patches automatisch installieren, wenn die entsprechende Option auf der Registerkarte EINSTELLUNGEN aktiviert ist. Dies empfiehlt sich nicht: Patches sollten immer auf ihre Kompatibilität getestet und nur dann eingeführt werden, wenn gewährleistet ist, dass sie keine Probleme verursachen werden.

15.5. Schritt 5: Planung und Zuweisung

Nach Abschluss der Testphase kann die tatsächliche Installation geplant werden. Wenn alle anwendbaren Patches lokalisiert und getestet wurden, kann ein Plan aufgestellt werden. Mithilfe der Richtlinie zur Patch-Verwaltung wird entschieden, in welcher Reihenfolge und auf welchen (Gruppen von) Computern zuerst die Patches bereitgestellt werden sollen. Mithilfe der Funktion NACHRICHTEN des Moduls CLIENTS lassen sich die Clients über den Patch-Plan informieren und vor eventuellen Neustarts warnen.

15.6. Schritt 6: Patch-Installation

Für ordnungsgemäß getestete Patches kann ein SOFTWAREVERTEILUNGSAUFTRAG geplant werden. Dazu wird mithilfe des Moduls AUFTRÄGE ein SOFTWAREVERTEILUNGSAUFTRAG mit den richtigen Patches für die richtigen Clients geplant. Um eine Störung der Endbenutzer-Workflows zu verhindern, können Patches so geplant werden, dass sie zu einem bestimmten Zeitpunkt oder direkt nach dem nächsten Start oder der nächsten Anmeldung bereitgestellt werden. Eine optionale Verzögerung verhindert, dass Patches bereitgestellt werden, wenn gerade andere systemintensive Prozesse laufen.

15.7. Schritt 7: Überprüfen und Berichten

Bei der Überprüfung und Auswertung der Patch-Installation können die Inventurtools eine große Hilfe sein. Außerdem bietet das PatchManager-Modul eine Möglichkeit für direkte Rückmeldungen der Benutzer. Patches, die auf das System anwendbar sind, aber noch nicht bereitgestellt wurden oder gar nicht installiert werden sollen, können von Endbenutzern angefordert werden, wenn ein dringender Bedarf für die Reparatur eines Produkts besteht. Wenn der Administrator die entsprechende Option aktiviert, können Endbenutzer eine Zurücksetzung der Patches anfordern, falls Probleme mit der Leistungsfähigkeit oder Kompatibilität auftreten. Die Administratoren können jederzeit manuell eine Zurücksetzung einleiten und so eine schnelle Lösung bieten, wenn ein bestimmtes Patch Probleme verursacht. Das Anforderungssystem für Verteilung und Zurücksetzung ist direkt in das PatchManager-Modul integriert und ermöglicht es dem Administrator, direkt vom Modul SICHERHEITSEREIGNISSE aus einen Verteilungs- oder Zurücksetzungsauftrag zu planen.

16. Network Monitoring

G DATA verfügt über das optionale Modul Network Monitoring, das in Kombination mit den anderen Sicherheitslösungen verwendet werden kann. Durch das Nachverfolgen einer Vielzahl von Netzwerkgeräten, einschließlich Hardware und Software, können die IT-Mitarbeiter die Geschäftskontinuität sicherstellen. Zu den Geräten gehören Endpunkte und Server (Festplatten, CPU, Arbeitsspeicher), Netzwerkinfrastruktur (Netzwerkschnittstellen, Router, Switches, Zugangspunkte, Firewalls), Peripheriegeräte, Prozesse und Dienste.

Mithilfe regelmäßiger Überwachungsberichte und konfigurierbarer Alarmmeldungen können die Mitarbeiter alle Geräte warten und unterstützen, proaktiv die Anzahl der Ereignisse begrenzen sowie Infrastrukturinstallationen und -erweiterungen planen. Das Network Monitoring macht Geräteverwaltung, Leistungsoptimierung und Wartung für Unternehmen jeder Größe – von KMUs bis Konzernen – effizienter und kostengünstiger.

16.1. Verwenden des Network Monitorings

Die zunehmende Zahl von Netzwerkgeräten macht es dem Administrator nicht immer leicht, Verfügbarkeitsrisiken bzw. Leistungsengpässe zu erkennen. Hier schafft das Network Monitoring Abhilfe. Durch die kontinuierliche Überwachung wird der Administrator auf Leistungsprobleme aufmerksam, sobald sie entstehen, und kann sich anbahnende Entwicklungen mitverfolgen. Mithilfe historischer Trenddaten können Schwachstellen im Netzwerk optimiert werden, bevor die Last die Leistung beeinträchtigt oder einen Ausfall verursacht. Melden die Benutzer Probleme mit einer Datenbank, einem CRM-System oder einem Web-Shop, weil sie nicht verfügbar sind, sind (historische) Daten und Fehlerprotokolle sehr hilfreich.

Das Network Monitoring ist auch bei Infrastrukturentwicklungen, also Netzwerkmigration und -erweiterung, nützlich. Beispielsweise kann der Administrator durch das Kartieren der Netzwerktopologie die Infrastrukturkomponenten ermitteln, die verbessert werden müssen, oder dafür sorgen, dass das Netzwerk alle installationsspezifischen Voraussetzungen erfüllt. Wird die Leistung über einen längeren Zeitraum mitverfolgt, hat der Administrator auch die Möglichkeit, Einblicke in die Leistungsgrade zu erhalten. Gemessen werden können Reaktionszeit von Anwendungen und Infrastruktur, Nutzungsgrad, Durchsatz und Kapazität. Diese Messpunkte dienen beim Planen neuer Infrastruktur als Basis für Migrations- und Erweiterungsszenarien, um fundierte Entscheidungen über Skalierbarkeit und Verfügbarkeit zu treffen. Dadurch lässt sich ein Gleichgewicht bei der Kapazitätsplanung finden, damit Leistungsspitzen angemessen verarbeitet werden, es aber keine Infrastruktur gibt, die größtenteils ungenutzt bleibt.

Da das Network Monitoring eine Vielzahl von Daten protokollieren kann, eignet es sich besonders gut für Prüf- und Regeltreuezwecke. Es kann nicht nur die Datennutzung für Geräte in der Netzwerkinfrastruktur mitverfolgen, sondern auch Standardkonfigurationen und Änderungen an der Protokollkonfiguration überwachen. Dadurch können Unternehmen ihre Infrastruktur auf die Zertifizierung vorbereiten und sicherstellen, dass sie trotz sich vergrößernder Infrastruktur regeltreu bleiben.

Die Eigenschaften des Network Monitorings harmonieren hervorragend mit den Sicherheitslösungen. Mit dem Network Monitoring als einer Ebene des Sicherheitskonzepts für das Unternehmensnetzwerk können Anzeichen verdächtiger Aktivität erkannt werden, beispielsweise eine ungewöhnlich hohe

Netzwerklast, die auf DoS-Angriffe (Denial of Service) hindeuten könnte. Auf infizierten Netzwerkgeräten zu beobachten sind unter Umständen auch eine untypische Prozessorlast bzw. Speichernutzung oder Dienste, die sich ungewöhnlich verhalten, sowie Prozesse, die nicht mehr reagieren, oder Datenverkehr von Malware-Infektionen. In Kombination mit dem PatchManager-Modul (siehe Kapitel 15) unterstützt das Network Monitoring den Administrator dabei, Sicherheitslücken umgehend zu erkennen und zu schließen.

Ob Cloud-Infrastrukturmanagement, virtuelle Server oder andere Mehrmandantenszenarien: Hier ist das Network Monitoring entscheidend, um das Geschäftsmodell aufrechtzuhalten. Die Infrastruktur muss aufgebaut und gewartet werden, um eine nennenswerte Kundenbasis zu bedienen. Mithilfe des Network Monitorings können Anforderungen abgeschätzt und die Leistung für alle Anwendungen und Dienste im Netzwerk beibehalten werden. Auf gleiche Weise wird die Virtualisierung physischer Server vorbereitet, indem ihr Lese-/Schreibzugriff, der Netzwerkdatenverkehr, die CPU-Nutzung und andere Leistungsdaten gemessen werden.

16.2. Vorbereitung und Installation

Das Modul Network Monitoring besitzt die gleiche Client-Server-Struktur wie die anderen Schutzebenen und lässt sich problemlos zu neuen oder vorhandenen G DATA Installationen hinzufügen. Die Cloud-basierte Architektur wird vom lokalen G DATA ManagementServer unterstützt. Der G DATA Security Client fungiert als Agent, der Daten von lokalen Datenpunkten und anderen Netzwerkgeräten sammelt. Diese Werte meldet er dem G DATA ManagementServer, der sie dann mit dem Cloud-Dienst G DATA ActionCenter synchronisiert. Der Cloud-Dienst kumuliert und speichert Daten, sendet Benachrichtigungen und ermöglicht über https://ac.gdata.de den Zugriff auf eine umfangreiche Web-Oberfläche.

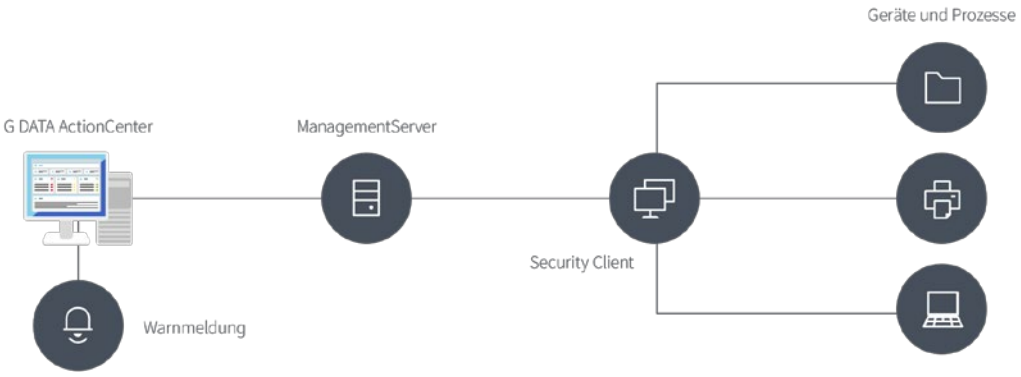

Abbildung 59: G DATA Network Monitoring – Architektur

Zur Installation des Network Monitorings wird ein Konto für das G DATA ActionCenter benötigt, das kostenfrei über die Web-Oberfläche erstellt werden kann. Das ActionCenter und der G DATA ManagementServer werden über die ActionCenter-Anmeldedaten im Modul ACTIONCENTER des G DATA Administrators verknüpft. Daraufhin synchronisiert der G DATA ManagementServer die Daten mit dem ActionCenter. Die mit dem ActionCenter-Konto verknüpften ManagementServer sind auf der Seite SERVER aufgeführt. Neben Angaben zum Server kann der Administrator auf dieser Seite auch Berechtigungen für andere Benutzer festlegen, die über das ActionCenter auf die Network Monitoring-Konfiguration zugreifen wollen. Dies kann dann nützlich sein, wenn mehrere Administratoren Zugang zu diesen

Informationen benötigen, insbesondere, wenn es sich um Warnmeldungen handelt (siehe Abschnitt 16.4).

Die weitere Konfiguration des Network Monitorings erfolgt mittels Metriken und Metrikvorlagen über die Web-Oberfläche. Eine Vorlage enthält eine vordefinierte Überwachungsart samt Konfigurationsparametern. Beispiel:

- Überwachung eines konkreten Vorgangs auf einem Windows-Gerät
- Überwachung der Serververfügbarkeit
- Überwachung des Tonerfüllstands eines Druckers

Nach dem Festlegen der Vorlage wird sie einem oder mehreren Geräten zugewiesen, um die Metrik zu erstellen. Das Gerät führt diese bestimmte Überwachungsaktion dann regelmäßig durch und meldet das Ergebnis an den zugeordneten ManagementServer. Der Server synchronisiert daraufhin die Ergebnisse mit dem ActionCenter, das seinerseits die in der Vorlage festgelegten Aktionen durchführt (also beispielsweise eine Warnmeldung sendet).

Je nach Art der Metrik sind möglicherweise zusätzliche Einstellungen erforderlich. Metriken, die SNMP benötigen, müssen mit dem überwachten Gerät kommunizieren können. Manche Geräte, wie beispielsweise Netzwerkdrucker, unterstützen SNMP automatisch. Ein SNMP-Agent ist erforderlich, um die SNMP-basierte Kommunikation mit Windows- und Linux-Computern zu ermöglichen. Unter Linux wird hierfür das Paket net-snmp aus dem Speicher installiert. Windows-Benutzer können das Installationsprogramm von der Sourceforge-Seite für Net-SNMP herunterladen[18].

Bei manchen Softwarepaketen ist ein Plug-in erforderlich, um mit dem SNMP-Agenten zu kommunizieren. Beim Konfigurieren einer Metrik, die einen Apache Web-Server überwacht, muss zuerst Apachestatistics installiert werden. Apachestatistics, mit dem Apache-Modul mod_statistics und dem Plug-in netsnmp, kann von Sourceforge heruntergeladen werden[19]. Die Download-Datei enthält Hinweise zur Installation von Apachestatistics.

16.3. Konfiguration

Zum Einrichten des Network Monitorings sind eine oder mehrere Metrikvorlagen erforderlich. Die Metrik entsteht durch das Zuweisen der Vorlage zu einem Gerät. Die Metrik meldet ihre Werte regelmäßig an das G DATA ActionCenter (über den G DATA Security Client und den G DATA ManagementServer), die dann in den Ansichten DASHBOARD bzw. METRIK der Web-Oberfläche angezeigt werden.

Nach der Anmeldung am G DATA ActionCenter und der Auswahl des Moduls NETWORK MONITORING wird METRIKEN ÜBERSICHT geöffnet. Per Klick auf VORLAGEN VERWALTEN wird VORLAGE ERSTELLEN angezeigt. Die Parameter einer Metrikvorlage hängen vom jeweiligen Anwendungsfall für das Network Monitoring ab (typische Beispiele finden Sie in Abschnitt 16.1). In jeder Vorlage müssen zumindest folgende ALLGEMEINE EINSTELLUNGEN eingegeben werden:

- KATEGORIE: Auswahl der Metrikkategorie. Jede Kategorie regelt mehrere Metriken. Bei Auswahl von SNMP-GERÄTE wird die Liste METRIK beispielsweise mit Metriken zur SNMP-Statistik vorbelegt, darunter empfangene bzw. gesendete Netzwerkdaten und TCP-Verbindungen.

[18] Siehe http://net-snmp.sourceforge.net.
[19] Siehe https://sourceforge.net/projects/apachestatistics/.

- METRIK: Auswahl einer verfügbaren Metrik für die ausgewählte Kategorie.
- ZIEL/HOSTNAME: Alle Metriken werden auf dem Gerät ausgeführt, dem sie zugewiesen sind. Es sammeln aber nicht alle Metriken ihre Daten nur auf diesem Gerät. Einige Metriken, insbesondere die Netzwerk-basierten, erfordern zusätzlich die Angabe eines Ziels. Die Metrik wird dann nach wie vor auf dem Gerät ausgeführt, dem sie zugewiesen ist, testet aber auch den Host, der unter ZIEL/HOSTNAME angegeben wurde. Die Metrik PING REQUEST wird beispielsweise auf dem Localhost ausgeführt, testet aber den Host HOSTNAME.
- NAME: Mit einem Namen können die Metrikvorlagen in der Liste METRIK-VORLAGEN VERWALTEN voneinander unterschieden werden.

Nach Eingabe der allgemeinen Einstellungen kann die Vorlage gespeichert und zum Erstellen einer Metrik genutzt werden. Für viele Network Monitoring-Szenarien empfiehlt es sich jedoch, auch die OPTIONALEN EINSTELLUNGEN und EINSTELLUNGEN FÜR ALARM zu konfigurieren. Mit den Einstellungen SCHWELLWERT und MESSWERT-BEDINGUNG können die Auswertungsbedingungen der Metriken eingestellt werden. Zum Messen der Serververfügbarkeit kann beispielsweise ein Schwellwert von 1000 ms eingegeben werden. Übersteigt der gemessene Wert diesen Schwellwert, ändert sich der Metrikstatus von OK in WARNUNG oder (falls der Wert wiederholt erreicht wird) in KRITISCH. Unter EINSTELLUNGEN FÜR ALARM können eine oder mehrere E-Mail-Adressen angegeben werden, an die eine Warnmeldung gesendet werden soll. Daraufhin wird der Administrator per E-Mail benachrichtigt, dass der Server länger als 1000 ms braucht, um zu antworten.

Eine Metrikvorlage kann einem oder mehreren Geräten zugewiesen werden, um eine Metrik zu erstellen. Auf der Seite METRIKEN ÜBERSICHT kann unter METRIKEN ERSTELLEN eine oder mehrere Metrikvorlagen einem oder mehreren Geräten zugewiesen werden. Die Erstellung einer Metrik umfasst vier Schritte.

1. Auswahl einer oder mehrerer Metrikvorlagen.
2. Auswahl eines oder mehrerer Geräte. Die gewählten Metrikvorlagen werden auf alle Geräte angewendet. Einige Vorlagen können nur für ManagementServer, andere nur für Clients übernommen werden. Das ActionCenter bildet die Vorlagen automatisch auf die passenden Geräte ab.
3. Die Geräte, für die Metrikvorlagen gelten sollen, müssen in der Übersicht aufgeführt sein.
4. Die Anzahl der neuen Metriken sollte den Erwartungen entsprechen und nicht di zulässige Höchstzahl an Metriken (je nach Lizenz) übersteigen.

Nach einem Klick auf METRIKEN ERSTELLEN werden die entsprechenden Metriken angelegt. Durch das Vorlagenmodell kann der Administrator mehrere Metriken gleichzeitig aktualisieren. Nach dem Bearbeiten einer Vorlage werden die Änderungen für alle Metriken übernommen, die auf dieser Vorlage beruhen. Wird beispielsweise auf einer Reihe von Geräten die Nutzung des Arbeitsspeichers überwacht, zeigt sich unter Umständen, dass der Speicher vergrößert werden muss, da der Schwellwert zu oft unterschritten wird. Nach der Vergrößerung des Arbeitsspeichers auf den betroffenen Geräten kann in der Metrikvorlage ein neuer Schwellwert eingegeben werden, der direkt für alle Geräte gilt.

16.4. Infrastrukturanalyse

Nach der Erstellung einer oder mehrerer Metriken hat der Administrator je nach Anwendungsfall verschiedene Möglichkeiten, um die gemeldeten Daten mitzuverfolgen. Bei Szenarien, in denen Veränderungen umgehend gemeldet werden, sind Alarme die Methode der Wahl. Im Notfall kann hier

schnell reagiert werden. Alarmmeldungen können in Metrikvorlagen aktiviert und für alle Metriken übernommen werden, die auf dieser Vorlage beruhen. Wird eine Alarmmeldung aktiviert, müssen auch entsprechende E-Mail-Gruppen festgelegt werden, um das Problem zügig zu beheben. Alarmmeldungen können auch an einen E-Mail-Verteiler gesendet werden, beispielsweise ein Notfallteam der IT-Abteilung. Die Empfänger einer Alarmmeldung sollten in der Lage sein, entsprechende Maßnahmen zu ergreifen. Müssen sie unabhängig vom Administrator agieren, können sie zur Verwendung des ActionCenters berechtigt werden (siehe Abschnitt 16.2). Zumindest muss ein Ablaufplan festgelegt werden, damit im Notfall die passenden Aktionen durchgeführt werden können.

Der Administrator muss nicht warten, bis eine Alarmmeldung gesendet wird. Das Network Monitoring protokolliert alle Metrikwerte, die von den überwachten Geräten gemeldet werden. In der Ansicht DASHBOARD werden die Daten kumuliert und numerisch pro Metrikstatus angezeigt (OK, WARNUNG und KRITISCH). Die Metriken können auch nach Status sortiert werden, um sich schnell einen Überblick zu verschaffen. Sind eine oder mehrere Metriken nicht im Status OK, findet sie der Administrator sofort und kann den Fehler weiter untersuchen. Der Bereich PROTOKOLLE beinhaltet Berichte für Metriken, die ihren ersten Wert bzw. alle Fehler melden oder ihren Status ändern.

Ist eine ausführlichere Analyse erforderlich, bieten die einzelnen Metrikseiten weitere Hilfe. Jede Seite enthält ein Diagramm, auf dem der Administrator Tendenzen erkennen kann, noch bevor sie ein kritisches Niveau erreichen. Das Diagramm kann so konfiguriert werden, dass es die Werte eines bestimmten Zeitraums anzeigt, um so Tendenzen aufzuzeigen. Steigt die RAM-Nutzung eines Geräts an und fällt dann plötzlich ab, kann dies auf ein Arbeitsspeicherproblem für bestimmt Prozesse hindeuten. Mithilfe dieser Angaben kann der Administrator umgehend handeln, also Metriken für Systemprozesse festlegen oder etwaige Probleme lokal auf dem Gerät selbst untersuchen. Neben dem Diagramm werden auch die absoluten Mindest- und Höchstwerte sowie ein Protokoll jedes Statuswechsels der Metrik angezeigt (beispielsweise von OK in WARNUNG).

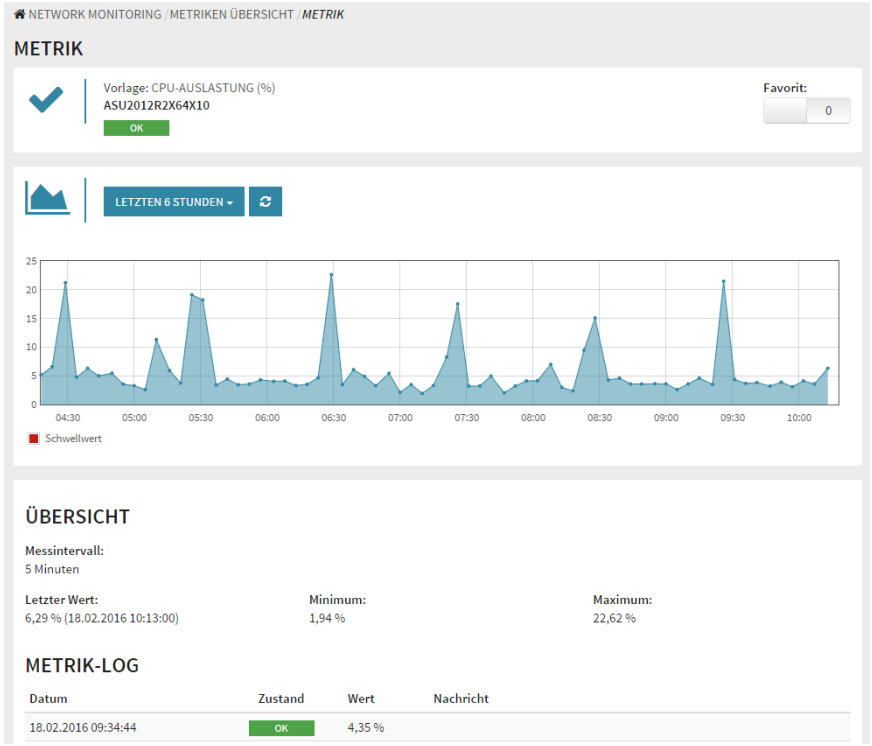

Abbildung 60: G DATA ActionCenter – Metrik-Ansicht

Mithilfe der verfügbaren Daten für einzelne Dienste kann der Administrator auch Trends auswerten. Anhand historischer Überwachungsdaten lassen sich beispielsweise Zeiten mit besonders hoher bzw. geringer Auslastung für eine Netzwerkschnittstelle ermitteln. Aus diesen Datenpunkten kann eine Messbasis erwarteter Werte erstellt werden, um daraus Alarmschwellwerte abzuleiten. Dieser Ablauf sollte nach und nach optimiert werden, da Schwellwerten nicht immer ganz einfach bestimmbar sind. Ist der Schwellwert zu niedrig, kommt es zu unnötigen Alarmmeldungen bei Diensten, die auch unter Last die benötigte Leistung erbringen. Andere Dienste funktionieren überhaupt nicht mehr, wenn die Last ansteigt. In diesem Fall sollte eine Alarmmeldung erfolgen, noch bevor der Wert ein kritisches Maß erreicht. Dieses kritische Maß ergibt sich aus einer langfristig beobachteten Leistungsstatistik, die mit Daten über Dienstverfügbarkeit und Güteverlust in Zusammenhang gesetzt wird. Außerdem kann der Administrator proaktiv Leistungstests einrichten, um die „Bruchstelle“ der Infrastruktur zu finden. Diese Tests können auch nach einem Leistungszwischenfall durchgeführt werden, um sicherzugehen, dass die ergriffenen Verbesserungsmaßnahmen ihre Wirkung zeigen.

17. Mail-Server-Sicherheit

Um eine Infizierung von Endbenutzer-Hardware wie Desktop-Computern oder Smartphones mit Malware zu verhindern, reicht es nicht aus, nur diese Endpunkte zu schützen. Auch weitere Netzwerkkomponenten sollten geschützt werden, um Bedrohungen frühzeitig herauszufiltern. Ein wichtiger Baustein dieser mehrschichtigen Sicherheit ist der Schutz des Mail-Servers. Durch einen Scan aller ein- und ausgehenden E-Mails kann verhindert werden, dass Malware und Spam ihr Ziel erreichen.

Auch bei Unternehmen, die keinen lokalen Mail-Server hosten, empfiehlt sich das Scannen aller E-Mails. Wie die Mail-Server-Sicherheit umgesetzt wird, hängt von der aktuellen Einrichtung des Mail-Servers ab. Wenn Sie den Microsoft Exchange Server verwenden, sollten Sie die Exchange Mail Security installieren. Sendmail- und Postfix-Server können mithilfe des Linux Mail Security Gateway geschützt werden. Andere Mail-Server lassen sich abdecken, indem das MailGateway als Gateway auf dem Mail-Server selbst oder auf einem speziellen Gateway-Server für E-Mail-Sicherheit installiert wird. Abschnitt 4.2.4 enthält ausführliche Informationen über die verschiedenen Installationsarten und den Installationsvorgang.

17.1. Exchange Mail Security

Das Modul „Exchange Mail Security“ ist optional verfügbar.

Die Exchange Mail Security ergänzt die vorhandenen Exchange-Workflows. Durch eine tief greifende Integration in den Server liefert das Plug-in einen transparenten Malware-Schutz: Ohne spürbare Verzögerungen oder eine Interaktion des Benutzers werden alle ein- und ausgehenden Objekte gescannt und nur weitergegeben, wenn sie frei von Malware sind. Die Plug-in-Installation sieht aus wie eine normale Client-Server-Installation. Das Exchange-Plug-in wird auf dem Exchange-Server installiert und berichtet an einen vorhandenen ManagementServer. Nach der Eingabe des Servers während der Installation verbindet sich das Exchange-Plug-in mit dem ManagementServer und erscheint in der Ansicht CLIENTS vom G DATA Administrator. Ist ein Exchange-Client ausgewählt, bieten die Registerkarten CLIENTS, AUFTRÄGE, SICHERHEITSEREIGNISSE und STATISTIK ähnliche Funktionen wie ihre Gegenstücke für die normale Client-Verwaltung. Malware-Scan- und AntiSpam-Einstellungen sowie Virensignatur- und Programmdatei-Updates können über das Modul EXCHANGE-EINSTELLUNGEN konfiguriert werden. Nach der Aktivierung aktualisiert sich das Exchange-Plug-in automatisch jedes Mal selbst, wenn es eine Verbindung mit dem ManagementServer herstellt (in dem Intervall, das unter ALLGEMEINE EINSTELLUNGEN > SYNCHRONISATION definiert ist). Ein manuelles Update kann jederzeit über die Registerkarte CLIENTS initiiert werden.

17.1.1. Virenschutz

Exchange Mail Security kann verschiedene Arten von Scans konfigurieren: Der Zugriffs-Scan garantiert dauerhaften Schutz, während der On-Demand-Scan so eingestellt werden kann, dass bestimmte Postfächer zu bestimmten Zeitpunkten gescannt werden.

17.1.1.1. Zugriffs-Scan

Der Zugriffs-Scan ist mit dem Dateisystemwächter des G DATA Security Clients vergleichbar. Er überwacht alle ein- und ausgehenden E-Mails auf dem Exchange Server. Die E-Mails werden automatisch

gescannt und erst verfügbar gemacht, wenn sie Malware-frei sind. Der Zugriffs-Scan kann auf der Registerkarte ALLGEMEIN aktiviert und seine Scan-Parameter werden unter SCAN-EINSTELLUNGEN konfiguriert. Der Scan kann mit ein oder zwei Scan-Engines durchgeführt werden. Die Verwendung von zwei Engines sorgt für optimale Sicherheit und ist die empfohlene Option. Wenn die Scan-Leistung aber nicht so gut wie erwartet ist, kann eine der beiden Engines deaktiviert werden. Auch dann ist die Erkennung noch sehr gut und die Leistung wird erhöht. Die Scan-Leistung kann weiterhin durch die Wahl der Dateien beeinflusst werden, die gescannt werden sollen. Die sicherste Option ist das Scannen aller Dateien, dies dauert aber länger als ein begrenzter Scan. Ein begrenzter Scan umfasst nur Programmdateien und Dokumente, also die Dateitypen, die am wahrscheinlichsten infiziert sind. Mithilfe der Heuristik können typische Merkmale von Malware analysiert und so die Erkennung weiter gesteigert werden. Die Chance auf false-positive Ergebnisse steigt damit leicht, aber die Malware-Erkennung wird deutlich verbessert. Wenn man das Scannen von Archivdateien aktiviert, ist gewährleistet, dass auch solche Malware gefunden wird, die sich in Archiven versteckt. Dies verlängert allerdings die Scan-Dauer, und wenn im Archiv eine infizierte Datei gefunden wird, wird das gesamte Archiv desinfiziert oder entfernt. Wurden Quarantänemaßnahmen konfiguriert, wird die gesamte E-Mail (einschließlich Archiv) in Quarantäne verschoben. Die Option ARCHIVE PRÜFEN kann deaktiviert werden, wenn alle Clients den Dateisystemwächter nutzen, um zu gewährleisten, dass die Malware sofort nach ihrer Extraktion aus dem Archiv bekämpft wird.

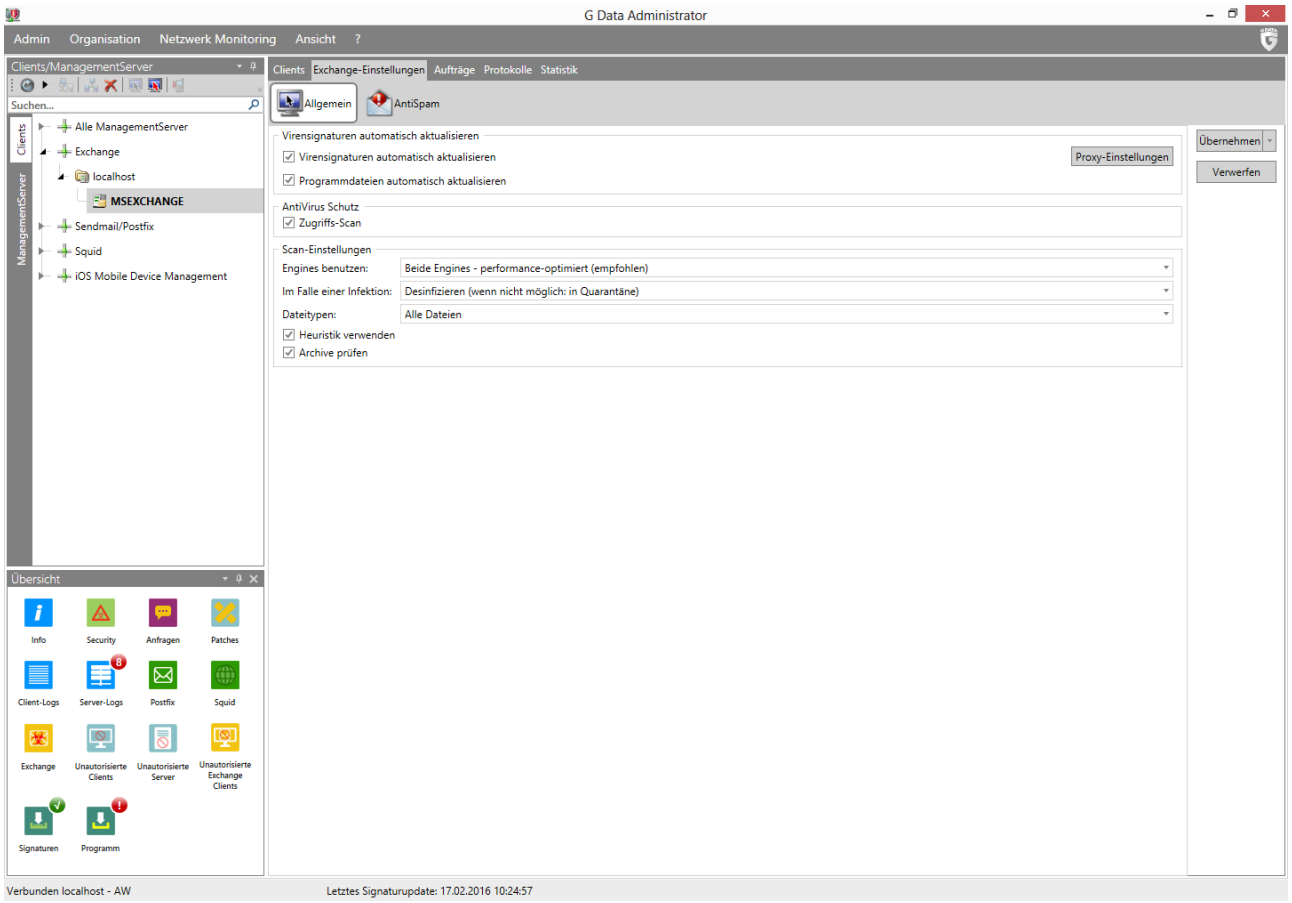

Abbildung 61: G DATA Administrator – Exchange-Einstellungen, Allgemein

Bei der Erkennung von Malware können verschiedene Schritte unternommen werden. Die empfohlene Aktion ist der Versuch, die Malware aus der Datei zu entfernen bzw. ihr Verschieben in Quarantäne, wenn

eine Entfernung nicht funktioniert. Dadurch wird ein Datenverlust so weit wie möglich verhindert und gleichzeitig sichergestellt, dass die Malware nicht ausgeführt werden kann. Im Modul SICHERHEITSEREIGNISSE erscheint ein Bericht, wenn Malware blockiert wird, und die in Quarantäne verschobenen Dateien können untersucht werden. Alternativ kann die Exchange Mail Security infizierte Anhänge löschen, die gesamte Nachricht löschen oder die Bedrohung protokollieren, ohne sie zu blockieren. Die sofortige Löschung eines infizierten Objekts ist die sicherste Option, kann aber bei einer false-positive Erkennung dafür sorgen, dass Daten entfernt werden. Eine reine Protokollierung der Bedrohungen wird nicht empfohlen, da dadurch jede erkannte Malware ignoriert wird. Der Exchange Server und seine Clients können darauf zugreifen und sie möglicherweise ausführen. Auch wenn dem Modul SICHERHEITSEREIGNISSE ein Bericht hinzugefügt wird, mit dem der Administrator manuelle Maßnahmen ergreifen kann, so bietet das Zeitfenster zwischen Bericht und Maßnahme doch die Möglichkeit einer Infizierung und möglicherweise einer weiteren Verbreitung.

17.1.1.2. On-Demand-Scan

Im Modul AUFTRÄGE lassen sich einzelne und regelmäßige Scans planen, die so ähnlich wie die Client-Scans funktionieren (siehe Abschnitt 9.2). Die Einstellungen entsprechen denen für Client-Scans, mit Ausnahme der Optionen, die für Exchange-Objekte nicht relevant sind Anstatt den Scan-Umfang mithilfe des Dateisystems zu definieren, wird ein Exchange-Scan für die Funktion in bestimmten Postfächern definiert. Wie bei den Dateisystemscans empfiehlt es sich, alle Objekte auf dem Server regelmäßig zu scannen. Dazu kann ein wöchentlicher, zweiwöchentlicher oder monatlicher Scan geplant werden. Ein Komplett-Scan kann sehr leistungsintensiv sein. Er sollte zu Nebenzeiten, wie etwa am Wochenende oder nachts, geplant werden.

17.1.2. AntiSpam

Ein großer Prozentsatz des E-Mail-Verkehrs besteht aus Spam. Die E-Mails enthalten zwar keine Malware, aber viele dieser Nachrichten sind unerwünscht, wie etwa Massen-E-Mails mit Medikamentenwerbung oder illegalem Software-Verkauf.

Spam-Filter werden schon lange auf einzelnen Clients installiert, um eingehende Spam-Nachrichten zu entfernen, bevor sie den Posteingang erreichen. Dies ist eine wirksame Möglichkeit, um dafür zu sorgen, dass die einzelnen Benutzer keine Zeit mit dem Lesen und Entfernen dieser E-Mails verbringen müssen. Es ist aber erforderlich, dass jeder Client über Möglichkeiten zum lokalen Spam-Filtern verfügt, etwa eine netzwerk- oder clientspezifische Konfiguration, einen aktuellen Regelsatz von Spam-Definitionen und lokale Möglichkeiten zum Selbstlernen. Das Exchange-Plug-in liefert einen leistungsstarken Spam-Filter auf Server-Ebene und kümmert sich um unerwünschte Nachrichten, bevor diese die Clients erreichen. AntiSpam für Exchange ist nur für Exchange-Server verfügbar, auf denen Hub-Transportrollen ausgeführt werden.

Alle eingehenden E-Mails werden gescannt und als sicher, SPAMVERDACHT, HOHE SPAMWAHRSCHEINLICHKEIT oder SEHR HOHE SPAMWAHRSCHEINLICHKEIT kategorisiert. Sichere Nachrichten werden sofort zugestellt, aber für jede der drei anderen Kategorien können individuelle Aktionen konfiguriert werden. E-Mails können direkt zurückgewiesen werden; das ist zwar eine Möglichkeit, umfassend mit Spam fertigzuwerden, es könnten aber versehentlich auch Nachrichten blockiert werden, die kein Spam sind (false positive). Um

sicherzugehen, dass zulässige E-Mails nicht aus Versehen zurückgewiesen werden, kann stattdessen eingestellt werden, dass Spam in den Ordner „Spam“ oder „Quarantäne“ verschoben wird. Dadurch können Nachrichten manuell untersucht und anschließend zurück in den Posteingang verschoben oder dauerhaft entfernt werden. Alternativ kann dem Betreff auch ein Präfix vorangestellt werden. Die Nachrichten werden dann immer noch zugestellt, aber die Benutzer haben eine Möglichkeit, Spam zu erkennen. Außerdem ermöglichen es Präfixe (lokalen) Filterregeln, unerwünschte Nachrichten auszusortieren. Beim Verschieben von Spam in den Ordner „Spam“ oder „Quarantäne“ wird dem Modul SICHERHEITSEREIGNISSE automatisch ein Bericht hinzugefügt. Durch Verwendung der Option, E-Mails zuzustellen oder zurückzuweisen, kann der Administrator wählen, ob dem Modul SICHERHEITSEREIGNISSE ein Bericht hinzugefügt werden soll oder nicht. Diese Option sollte sorgfältig erwogen werden, da sie eine große Anzahl von Berichten erzeugen kann.

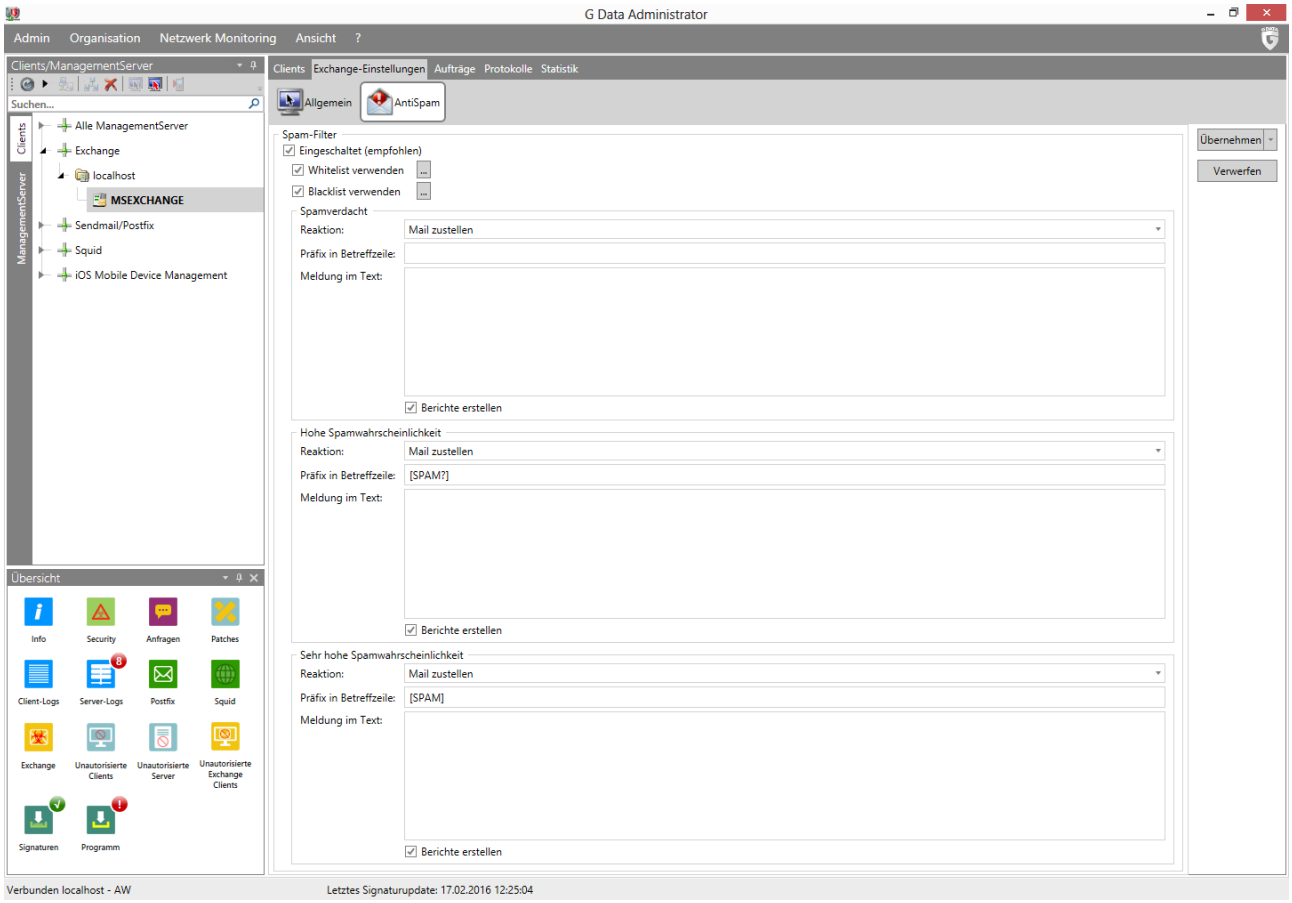

Abbildung 63: G DATA Administrator – Exchange-Einstellungen, AntiSpam

Wenn die Spam-Filtermaßnahme für eine oder mehrere Kategorien konfiguriert wurde, fügt die Exchange Mail Security jeder Spam-Nachricht in dieser Kategorie die Kopfzeile **X-G-Data-MailSecurity-for-Exchange-MoveToJunkFolder: True** hinzu. Dadurch werden die Nachrichten automatisch in den Spam-Ordner verschoben. Dieser Vorgang lässt sich beschleunigen, wenn man eine serverseitige Posteingangsregel erstellt. Die Regel sorgt dafür, dass der Exchange Server Nachrichten sofort in den Spam-Ordner verschiebt. Mithilfe vom Exchange Management Shell muss folgendes PowerShell-Skript ausgeführt werden, um die Regel für alle Postfächer aufzustellen. Im ersten Befehl muss **<Konto>** durch das Konto des Benutzers ersetzt werden, der das Skript ausführt:

[PS] $mailboxes = get-mailbox -resultsize unlimited | add-mailboxpermission -user <Konto> -accessrights fullaccess
[PS] $mailboxes | foreach { new-inboxrule -name "MoveToJunkFolder" -mailbox $($_.Alias) -MoveToFolder "$($_.Alias):\Junk-E-Mail" -HeaderContainsWords "X-G-Data-MailSecurity-for-Exchange-MoveToJunkFolder: True" -StopProcessingRules $true -confirm:$false -force }

Zusätzlich zu den drei Kategorien wird Spam auch mit einem Blacklist/Whitelist-Ansatz gefiltert. E-Mail-Adressen und Domänen können auf die Whitelist gesetzt werden, um den Spam-Filter zu umgehen. Alle eingehenden Nachrichten von Domänen oder Adressen auf der Whitelist gelten als sicher und werden sofort zugestellt. Nachrichten auf der Blacklist werden entsprechend der Konfiguration unter SEHR HOHE SPAMWAHRSCHEINLICHKEIT als Spam behandelt.

17.2. Linux Mail Security Gateway

Das Linux Mail Security Gateway-Modul ist optional verfügbar.

Das Linux Mail Security Gateway schützt vor Malware und filtert Sendmail- bzw. Postfix-Mail-Server auf Spam. Damit kann der Administrator umgehend die vorhandenen Mail-Server schützen. Er kann das Plug-in aber auch so einrichten, dass andere Mail-Server geschützt werden. Hierzu konfiguriert er einen Sendmail- oder Postfix-Mail-Server als Proxy zwischen dem Internet und dem eigentlichen Mail-Server. Weitere Informationen über die Installation des Linux Mail Security Gateway finden Sie in Abschnitt 4.8.3.3.

17.2.1. Virenschutz

Der Virenschutz für Sendmail- und Postfix-Mail-Server wird im Modul SENDMAIL/POSTFIX des G DATA Administrators konfiguriert. Der Virenschutz sollte immer aktiviert bleiben. Unter REAKTION kann der Administrator die Aktion festlegen, die beim Fund einer infizierten E-Mail ergriffen werden soll. In den meisten Fällen sollten infizierte Anhänge sofort gelöscht werden. Damit durch False-Positives keine Daten verloren gehen, können infizierte E-Mails auch in Quarantäne verschoben werden. In diesem Fall sollte in der Betreffzeile bzw. dem Nachrichtentext ein entsprechender Hinweis eingefügt werden, damit klar ist, dass der Virus bereits gefunden wurde.

17.2.2. AntiSpam

Ähnlich wie das Exchange-Plug-in unterstützt auch das Linux Mail Security Gateway die Erkennung von Spam. Bei aktiviertem Filter werden die eingehenden E-Mails als sicher, SPAMVERDACHT, HOHE SPAMWAHRSCHEINLICHKEIT oder SEHR HOHE SPAMWAHRSCHEINLICHKEIT kategorisiert. Sichere Nachrichten werden sofort zugestellt, aber für jede der drei anderen Kategorien können individuelle Aktionen konfiguriert werden. E-Mails können gelöscht oder zugestellt werden. Löschen ist besonders gründlich, sollte aber auf Fälle beschränkt bleiben, in denen sich der Administrator völlig sicher ist, dass es sich um Spam handelt. In anderen Fällen können die Nachrichten zugestellt werden, wenn in der Betreffzeile oder im Nachrichtetext ein Hinweis eingefügt wird. Dadurch können sich die Clients um die E-Mails kümmern und sie gemäß automatischen Filterregeln in einen Spam-Ordner verschieben. Zusätzlich zu den drei Kategorien wird Spam auch mit einem Blacklist/Whitelist-Ansatz gefiltert. E-Mail-Adressen und Domänen können auf die Whitelist gesetzt werden, um den Spam-Filter zu umgehen. Alle eingehenden Nachrichten

von Domänen oder Adressen auf der Whitelist gelten als sicher und werden sofort zugestellt. Nachrichten auf der Blacklist werden entsprechend der Konfiguration unter SEHR HOHE SPAMWAHRSCHEINLICHKEIT als Spam behandelt.

17.3. MailGateway

Das MailSecurity-Modul ist optional verfügbar.

MailSecurity MailGateway liefert Malware-Schutz und Spam-Filtermaßnahmen und ist mit allen Mail-Servern kompatibel[20]. Es kann in den E-Mail-Workflow integriert werden, indem es den Datenverkehr scannt, bevor dieser den Mail-Server selbst erreicht. Es sind verschiedene Umsetzungen möglich, etwa die Installation auf dem vorhandenen Mail-Server oder die Installation für einen speziellen E-Mail-Gateway-Server. In Abschnitt 17.3.1 werden die Möglichkeiten ausführlich erläutert. Es reicht aber nicht aus, nur das Gateway zu installieren. Der E-Mail-Verkehr muss über die MailSecurity geroutet werden, damit er gescannt werden kann. Nach Abschluss dieser Konfiguration können die einzelnen Komponenten für den Schutz des E-Mail-Verkehrs (Malware-Schutz und Spam-Filter) eingerichtet werden.

17.3.1. Installation

Wenn der Installationsassistent von MailSecurity MailGateway ausgeführt wurde, wird der MailGateway-Server automatisch gestartet. Wie der ManagementServer führt er seine Aufgaben im Hintergrund aus, ohne eine Interaktion des Benutzers zu verlangen. Er benötigt aber eine gewisse Erstkonfiguration, um mit dem Scannen des E-Mail-Verkehrs auf Malware und Spam zu beginnen. Alle Einstellungen für MailGateway lassen sich mit dem MailSecurity Administrator bearbeiten. Der MailGateway-Einrichtungsassistent installiert den MailSecurity Administrator automatisch auf demselben Computer. Wie die Administrator-Anwendung für den ManagementServer kann er aber von jedem Computer aus genutzt werden, der eine Verbindung zu dem Server herstellt, auf dem das MailGateway läuft.

Wenn der MailSecurity Administrator zum ersten Mal gestartet wird, müssen Name und Kennwort des Servers eingegeben werden. Das Feld „Servername“ wird automatisch mit dem Namen des Servers gefüllt, auf dem das MailGateway installiert wurde. Das Feld „Kennwort“ kann frei gelassen werden. Durch Klicken auf OK wird man zur Eingabe eines neuen Kennworts aufgefordert. Das Kennwort kann später durch Klicken auf die Schaltfläche KENNWORT ÄNDERN auf der Registerkarte ERWEITERT des Fensters OPTIONEN vom MailSecurity Administrator geändert werden. Wenn das Kennwort verloren gegangen und eine Anmeldung beim MailSecurity Administrator nicht mehr möglich ist, kann das Kennwort zurückgesetzt werden, wenn der Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\G DATA\AVKSmtp\pw (Windows 64 Bit-System) oder HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVKSmtp\pw (32-Bit-System) aus der Registry auf dem MailGateway-Server entfernt wird.

Der MailSecurity Administrator öffnet sich auf der Seite STATUS und zeigt Informationen über die wichtigsten Funktionen des Gateway-Servers an. Man kann auf jede Statusmeldung doppelklicken, um den entsprechenden Teil des Menüs OPTIONEN zu öffnen. Beim ersten Start des Programms sind manche

[20] Bei der Verwendung von Microsoft Exchange, Sendmail und Postfix lassen sich Malware- und Spam-Schutz am einfachsten durch die Installation des jeweiligen Plug-ins statt der MailSecurity umsetzen.

Funktionen deaktiviert. Als Teil der Aufgaben nach der Installation werden automatische Aktualisierungen der Virensignaturen und Porteinstellungen des Mail-Servers konfiguriert. Anschließend können Malware-Schutz, Spam-Filter und benutzerdefinierte Filter des MailGateways eingerichtet werden.

Abbildung 62: G DATA MailSecurity Administrator – Status

17.3.1.1. Virensignatur-Updates

Ein wichtiger erster Schritt ist die Konfiguration der automatischen Updates für die Virensignatur-Datenbank. Indem dazu in der oberen Menüleiste auf die Option UPDATE geklickt wird, öffnet sich das Fenster INTERNET-UPDATE und eine der beiden Aktualisierungsmethoden kann ausgewählt werden. Es wird empfohlen, erst den G DATA Security Client und dann die MailSecurity MailGateway zu bereitzustellen (siehe Abschnitt 4.8). Dadurch ist nicht nur gewährleistet, dass Malware den Gateway-Server nicht infizieren kann, sondern es wird auch dem MailGateway ermöglicht, ein- und ausgehende E-Mails mit den Virensignaturen vom Security Client zu scannen, sodass keine eigene Virensignatur-Datenbank gepflegt werden muss.

Wenn das MailGateway nicht in einem ManagementServer-Netzwerk läuft, kann es alternativ so konfiguriert werden, dass es sich seine eigenen Virensignaturen herunterlädt. Um Updates zu erhalten, meldet sich die MailSecurity online bei den G DATA Update-Servern an und benötigt dafür Zugangsdaten. Durch Klicken auf EINSTELLUNGEN UND ZEITPLANUNG öffnen sich die Update-Einstellungen, in denen die Registerkarte ZUGANGSDATEN ausgewählt werden kann. Wenn Benutzername und Kennwort bereits vorliegen (weil beispielsweise die Software bereits aktiviert wurde), können sie direkt eingegeben werden. Alternativ kann auf AM SERVER ANMELDEN geklickt werden, um seine Registrierungsnummer einzugeben. Nach der Anmeldung bei G DATA werden Benutzername und Kennwort automatisch generiert. Diese sollten unbedingt notiert werden, damit sie bei einer Neuinstallation verwendet werden können. Nach der Eingabe der Zugangsdaten muss auf der Registerkarte ZEITPLANUNG INTERNET-UPDATE ein Update-Zeitplan definiert werden. Damit das MailGateway die E-Mails auch mit den neuesten Virensignaturen scannen kann, sollte ein stündliches Update definiert werden. Wenn der Computer, auf dem MailGateway installiert wurde, für die Verbindung mit dem Internet einen Proxy-Server nutzt, muss dieser auf der Registerkarte INTERNET-EINSTELLUNGEN definiert werden. Dies ist auch der Ort, an dem die

Anmeldedaten eingegeben werden, falls sie für die Einrichtung einer Internetverbindung erforderlich sind.

17.3.1.2. E-Mail-Streams

Es ist wichtig, zwischen drei möglichen E-Mail-Streams zu unterscheiden, die vom MailGateway gescannt werden können: eingehende SMTP-E-Mails (vom Internet ins Netzwerk), ausgehende SMTP-E-Mails (vom Netzwerk ins Internet) und POP3 (nur für eingehende E-Mails). Nicht jedes Netzwerk verwendet jede Art der E-Mail-Kommunikation. Für die Protokolle, die in Gebrauch sind, ist eine Portkonfiguration auf dem MailGateway und dem Mail-Server unbedingt erforderlich, um E-Mail-Streams durch das MailGateway zu leiten, bevor sie dem Mail-Server zugestellt werden. Welche Ports geändert werden müssen, hängt von der Art der Installation ab.

Je nach Mail-Server kann der Zugriff auf die Protokoll- und Porteinstellungen schwierig sein. G DATA bietet in verschiedenen TechPapers zusätzliche Unterstützung bei der Konfiguration für bestimmte Produkte. Folgende TechPapers enthalten weitere Informationen: #0149 (Tobit David), #0150 (AVM Ken!), #0151 (Microsoft Exchange Server 2010) und #0152 (Microsoft Exchange Server 2007).

Installation 1: Auf dem Mail-Server (mit Portänderungen des Mail-Servers)

Der Vorteil der Installation vom MailGateway auf dem Mail-Server besteht darin, dass kein separater Server konfiguriert werden muss. Der Nachteil ist, dass die Ports für SMTP und POP3 sorgfältig konfiguriert werden müssen. Um Änderungen an lokalen Firewall- oder DNS-Einträgen zu vermeiden, sollten einige Ports des Mail-Servers geändert werden. Dies ist eine Beispielkonfiguration: Die MailSecurity empfängt Abrufanforderungen für POP3 an Port 7110 (von Clients oder von einem POP3-Connector auf dem Mail-Server), stellt eine Verbindung mit dem POP3-Mail-Server im Internet her, ruft die E-Mails ab, verarbeitet sie und stellt sie zu. Eingehende SMTP-E-Mails (aus dem Internet) werden von der MailSecurity an Port 25 empfangen, verarbeitet und an Port 7125 des internen Mail-Servers weitergeleitet. Ausgehende SMTP-Mails werden vom internen Mail-Server an Port 7125 empfangen und an Port 7025 von der MailSecurity weitergeleitet, verarbeitet und gesendet. Der interne Mail-Server arbeitet am SMTP-Port 7125. Exchange-Clients müssen nicht neu konfiguriert zu werden, aber Clients, die E-Mails mit SMTP-Einstellungen versenden, müssen so konfiguriert werden, dass sie eine Verbindung mit diesem Port herstellen. Die Porteinstellungen für die MailSecurity und den Mail-Server sehen wie folgt aus:

E-Mail-Verkehr	MailGateway	Mail-Server
SMTP (eingehend)	25	7125
SMTP (ausgehend)	7025	7125
POP3	7110	110

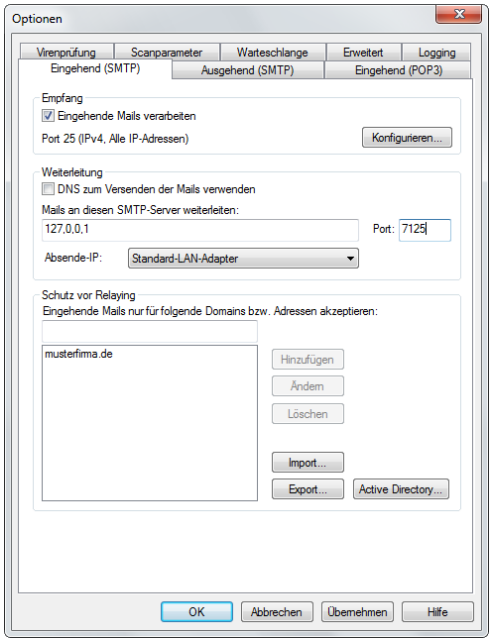

Abbildung 63: G DATA MailSecurity Administrator – Optionen, Eingehend (SMTP)

Damit das MailGateway die eingehenden SMTP-E-Mails scannen kann, muss im Dialog OPTIONEN die Registerkarte EINGEHEND (SMTP) ausgewählt werden. Unter EMPFANGEN wird die Option EINGEHENDE E-MAILS VERARBEITEN aktiviert. Das MailGateway arbeitet an Port 25 und der Mail-Server nutzt einen anderen Port (zum Beispiel 7125). Wurde die eingehende SMTP-E-Mail gescannt, wird sie entsprechend den Einstellungen unter Weiterleitung an den Mail-Server übertragen. Standardmäßig ist DNS ZUM VERSENDEN DER MAILS VERWENDEN aktiviert. Diese Option nutzt den lokalen MX-Eintrag, um zu entscheiden, wo die E-Mail zugestellt werden soll, was aber nur funktioniert, wenn der Mail-Server im MX-Eintrag aufgeführt ist. Da in vielen Fällen das MailGateway im MX-Eintrag aufgeführt ist, ist es sicherer, DNS ZUM VERSENDEN DER MAILS VERWENDEN zu deaktivieren. IP und Port des Mail-Servers können dann spezifisch definiert werden. Dazu gibt man **127.0.0.1** als IP-Adresse und den Mail-Server-Port im Feld „Port“ ein (in diesem Beispiel **7125**).

Um die ausgehenden E-Mails zu scannen, wird die Registerkarte AUSGEHEND (SMTP) geöffnet. Anschließend wird die Option VERARBEITUNG AUSGEHENDER MAIL aktiviert und die Portnummer eingegeben. Die einfachste Konfiguration besteht darin, einen anderen als den Port EINGEHEND (SMTP) zu definieren, in diesem Beispiel 7025. Wenn aber derselbe Port für ein- und ausgehenden SMTP-Verkehr genutzt werden soll, muss das MailGateway in der Lage sein, den ein- vom ausgehenden SMTP-Verkehr zu unterscheiden. Dies erreicht man, indem **127.0.0.1** und die IP-Adresse des Servers (zum Beispiel **192.168.1.2**) zu IP-ADRESSEN/TEILNETZE DER RECHNER, DIE AUSGEHENDE MAILS SENDEN hinzugefügt wird. Ausgehende E-Mails können auf zwei Arten zugestellt werden. Das MailGateway kann die E-Mails direkt mithilfe des DNS-Eintrags des Ziels zustellen. Dies ist die empfohlene Konfiguration. Wurde die Option DNS ZUM VERSENDEN DER E-MAILS VERWENDEN deaktiviert, kann ein SMTP-Server definiert werden, an den die ausgehenden E-Mails

weitergeleitet werden sollen. Wenn eine Authentifizierung erforderlich ist, muss das entsprechende Verfahren im Fenster AUTHENTIFIZIERUNG ausgewählt werden.

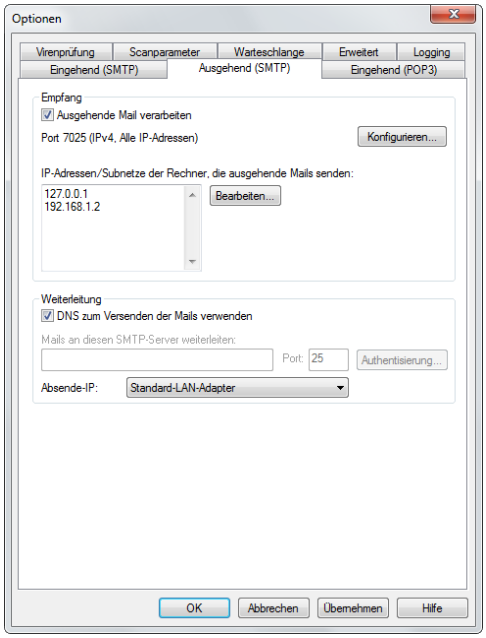

Abbildung 64: G DATA MailSecurity Administrator – Optionen, Ausgehend (SMTP)

POP3-Scans können auf der Registerkarte EINGEHEND (POP3) konfiguriert werden. Dazu wird die Option POP3-ANFRAGEN VERARBEITEN aktiviert und der Port eingegeben, an dem das MailGateway die POP3-Anfragen empfangen wird (**7110**). Damit die E-Mail-Software dem Empfänger keinen Zeitüberschreitungsfehler anzeigt, wenn der POP3-Abruf zu lange dauert, muss das Kontrollkästchen ZEITÜBERSCHREITUNG BEIM E-MAIL-PROGRAMM VERMEIDEN aktiviert werden. Unter ABHOLUNG wird der POP3-Server eingegeben, von dem die E-Mails abgeholt werden sollen. Das ist normalerweise der POP3-Server des Internetanbieters. Das MailGateway nutzt die gleiche Anmeldung, die der Client bei seiner POP3-Anfrage verwendet. Unter FILTER kann ein Ersatztext für E-Mails definiert werden, die vom Malware-Schutz oder Spam-Filter zurückgewiesen werden.

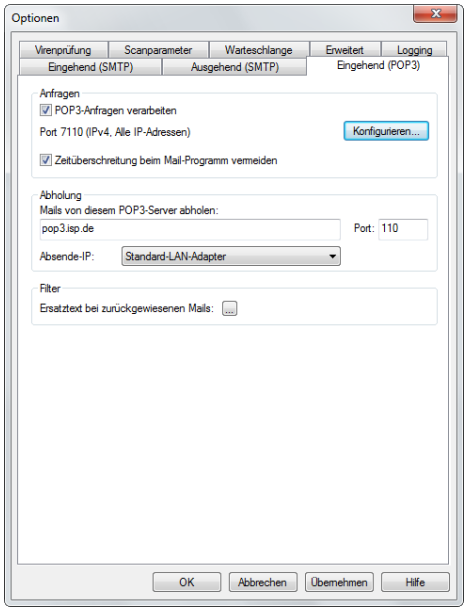

Abbildung 65: G DATA MailSecurity Administrator – Optionen, Eingehend (POP3)

Nach der Einrichtung des MailGateways müssen die Einstellungen des Mail-Servers aktualisiert werden. Dazu wird der Server für eingehende POP3-E-Mails in die IP-Adresse des Servers (**192.168.1.2**) geändert und der MailGateway-Port (**7110**) hinzugefügt. Der Port für ein- und ausgehende SMTP-E-Mails muss in **7125** geändert werden. Damit ausgehende E-Mails richtig geroutet werden, muss die Einstellung des Mail-Servers für ausgehende SMTP-E-Mails in die IP-Adresse des Servers geändert und der MailGateway-Port (**7025**) hinzugefügt werden. Anschließend wird die SMTP-Authentifizierung deaktiviert, da diese vom MailGateway durchgeführt wird.

Da der SMTP-Port des Mail-Servers geändert wurde, sollten Clients, die E-Mails mithilfe der SMTP-Einstellungen versenden, ausgehende E-Mails an den neuen Port senden. Die Einstellungen der lokalen E-Mail-Clients müssen ebenfalls entsprechend geändert werden (SMTP-Port 7125). Bei Clients, die E-Mails mit Exchange senden, müssen die Einstellungen nicht aktualisiert werden.

Installation 2: Auf dem Mail-Server (ohne Portänderungen des Mail-Servers)

Wenn Portänderungen des Mail-Servers nicht praktikabel sind, weil beispielsweise einfach zu viele Clients neu konfiguriert werden müssten, kann der Mail-Server weiter an Port 25 arbeiten und das MailGateway kann SMTP-E-Mails mithilfe der Ports 7025 und 7125 empfangen bzw. senden. Um aber zu gewährleisten, dass die MailSecurity auch weiterhin die erste Sicherheitsebene ist, muss die lokale Firewall so aktualisiert werden, dass sie eingehenden SMTP-Verkehr an den Nicht-Standardport 7025 von MailGateway weiterleitet. Die Porteinstellungen für dieses Szenario sehen wie folgt aus:

E-Mail-Verkehr	MailGateway	Mail-Server
SMTP (eingehend)	7025	25
SMTP (ausgehend)	7125	25
POP3	7110	110

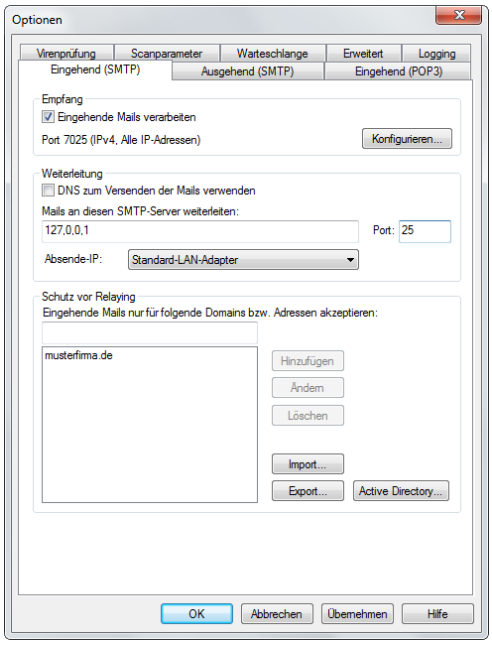

Abbildung 66: G DATA MailSecurity Administrator – Optionen, Eingehend (SMTP)

Damit das MailGateway die eingehenden SMTP-E-Mails scannen kann, muss im Dialog OPTIONEN die Registerkarte EINGEHEND (SMTP) ausgewählt werden. Unter Empfangen wird die Option EINGEHENDE E-MAILS VERARBEITEN aktiviert. Das MailGateway arbeitet am Nicht-Standardport 7025. Wurde die eingehende SMTP-E-Mail gescannt, wird sie entsprechend den Einstellungen unter Weiterleitung an den Mail-Server übertragen. Standardmäßig ist DNS ZUM VERSENDEN DER MAILS VERWENDEN aktiviert. Diese Option nutzt den lokalen MX-Eintrag, um zu entscheiden, wo die E-Mail zugestellt werden soll, was aber nur funktioniert, wenn der Mail-Server im MX-Eintrag aufgeführt ist. Da in vielen Fällen das MailGateway im MX-Eintrag aufgeführt ist, ist es sicherer, DNS ZUM VERSENDEN DER MAILS VERWENDEN zu deaktivieren. IP und Port des Mail-Servers können dann spezifisch definiert werden. Dazu wird **127.0.0.1** als IP-ADRESSE und der Mail-Server-Port im Feld PORT eingegeben (in diesem Beispiel **25**).

Um die ausgehenden E-Mails zu scannen, wird die Registerkarte AUSGEHEND (SMTP) geöffnet. Anschließend wird die Option VERARBEITUNG AUSGEHENDER MAIL aktiviert und die Portnummer eingegeben. Die einfachste Konfiguration besteht darin, einen anderen als den Port EINGEHEND (SMTP) zu definieren, in diesem Beispiel wird **7125** verwendet. Wenn aber derselbe Port für ein- und ausgehenden SMTP-Verkehr genutzt werden soll, muss das MailGateway in der Lage sein, den ein- vom ausgehenden SMTP-Verkehr zu unterscheiden. Dies erreicht man, indem **127.0.0.1** und die IP-Adresse des Servers (zum Beispiel **192.168.1.2**) zu IP-ADRESSEN/TEILNETZE DER RECHNER, DIE AUSGEHENDE MAILS SENDEN hinzugefügt wird. Ausgehende E-Mails können auf zwei Arten zugestellt werden. Das MailGateway kann die E-Mails direkt mithilfe des DNS-Eintrags des Ziels zustellen. Dies ist die empfohlene Konfiguration. Wurde die Option DNS ZUM VERSENDEN DER E-MAILS VERWENDEN deaktiviert, kann ein SMTP-Server definiert werden, an den die ausgehenden E-Mails weitergeleitet werden sollen. Wenn eine Authentifizierung erforderlich ist, muss das entsprechende Verfahren im Fenster AUTHENTIFIZIERUNG ausgewählt werden.

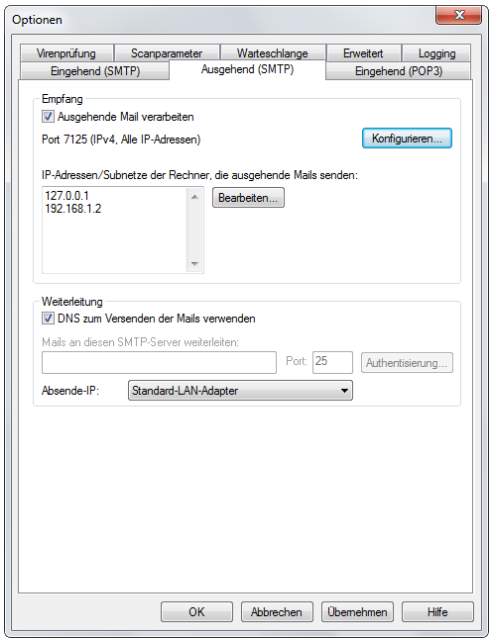

Abbildung 67: G DATA MailSecurity Administrator – Optionen, Ausgehend (SMTP)

Die Einstellungen zum Abruf von POP3-E-Mails sind identisch mit denen in der Installation 1.

Die Porteinstellungen für den Mail-Server selbst müssen nicht geändert werden, aber er muss das MailGateway finden können. Dazu wird der Server für eingehende POP3-E-Mails in die IP-Adresse des Servers (**192.168.1.2**) geändert und der MailGateway-Port (**7110**) hinzugefügt. Damit ausgehende E-Mails

richtig geroutet werden, muss die Einstellung des Mail-Servers für ausgehende SMTP-E-Mails in die IP-Adresse des Servers geändert und der MailGateway-Port (**7125**) hinzugefügt werden. Anschließend wird die SMTP-Authentifizierung deaktiviert, da diese vom MailGateway durchgeführt wird. Da der Mail-Server weiterhin Port 25 für ein- und ausgehende SMTP-E-Mails nutzt, muss mit einer Änderung auf Netzwerkebene sichergestellt werden, dass die MailSecurity die eingehenden SMTP-E-Mails empfängt. Der Router oder die Firewall müssen den an Port 25 eingehenden SMTP-Verkehr an das MailGateway an Port 7025 weiterleiten.

Installation 3: Spezieller Gateway-Server

Die Alternative zu einer Installation auf dem Mail-Server ist die Installation vom MailGateway auf seinem eigenen Server. Die Ports des Mail-Servers müssen dazu nicht geändert werden, aber eingehende E-Mails müssen zuerst dem MailGateway zugestellt werden, bevor sie am Mail-Server ankommen. Das lässt sich auf verschiedene Weisen erreichen. Der MX-Eintrag im DNS-Eintrag für die Domäne des Netzwerks kann von der IP-Adresse des Mail-Servers in die IP-Adresse vom MailGateway geändert werden; die Umleitung kann in der Firewall eingerichtet werden oder dem MailGateway kann die ursprüngliche IP-Adresse des Mail-Servers zugewiesen werden. In diesem Beispiel werden die Ports wie folgt konfiguriert:

E-Mail-Verkehr	MailGateway	Mail-Server
SMTP (eingehend)	25	25
SMTP (ausgehend)	7025	25
POP3	110	110

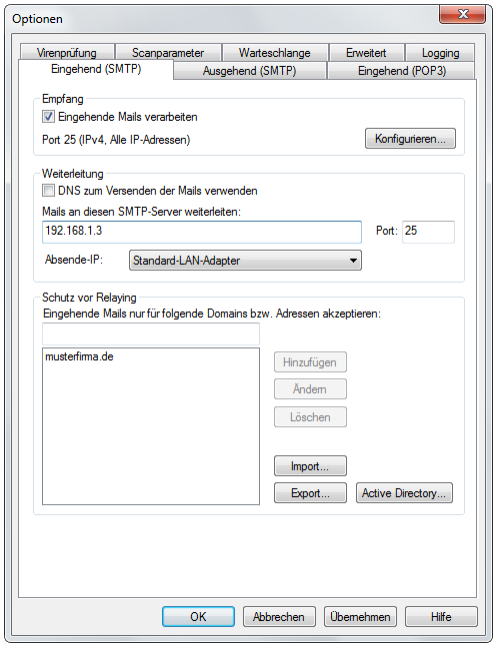

Abbildung 68: G DATA MailSecurity Administrator – Optionen, Eingehend (SMTP)

Damit das MailGateway die eingehenden SMTP-E-Mails scannen kann, muss im Dialog OPTIONEN die Registerkarte EINGEHEND (SMTP) ausgewählt werden. Unter EMPFANGEN wird die Option EINGEHENDE E-MAILS VERARBEITEN aktiviert. Das MailGateway arbeitet am Port **25**. Wurde die eingehende SMTP-E-Mail gescannt, wird sie entsprechend den Einstellungen unter WEITERLEITUNG an den Mail-Server übertragen.

Standardmäßig ist DNS ZUM VERSENDEN DER MAILS VERWENDEN aktiviert. Diese Option nutzt den lokalen MX-Eintrag, um zu entscheiden, wo die E-Mail zugestellt werden soll, was aber nur funktioniert, wenn der Mail-Server im MX-Eintrag aufgeführt ist. Da in vielen Fällen das MailGateway im MX-Eintrag aufgeführt ist, ist es sicherer, DNS ZUM VERSENDEN DER MAILS VERWENDEN zu deaktivieren. IP und Port des Mail-Servers können dann spezifisch definiert werden. Dazu werden die IP-Adresse des Mail-Servers (in diesem Beispiel **192.168.1.3**) und der Mail-Server-Port im Feld PORT (in diesem Beispiel **25**) eingegeben.

Um die ausgehenden E-Mails zu scannen, wird die Registerkarte AUSGEHEND (SMTP) geöffnet. Anschließend wird die Option VERARBEITUNG AUSGEHENDER MAIL aktiviert und die Portnummer eingegeben. Die einfachste Konfiguration besteht darin, einen anderen als den Port EINGEHEND (SMTP) zu definieren, in diesem Beispiel **7025**. Wenn aber derselbe Port für ein- und ausgehenden SMTP-Verkehr genutzt werden soll, muss das MailGateway in der Lage sein, den ein- vom ausgehenden SMTP-Verkehr zu unterscheiden. Dies erreicht man, indem die IP-Adresse des Mail-Servers (zum Beispiel **192.168.1.3**) zu IP-ADRESSEN/TEILNETZE DER RECHNER, DIE AUSGEHENDE MAILS SENDEN hinzufügt. Ausgehende E-Mails können auf zwei Arten zugestellt werden. Das MailGateway kann die E-Mails direkt mithilfe des DNS-Eintrags des Ziels zustellen. Dies ist die empfohlene Konfiguration. Wurde die Option DNS ZUM VERSENDEN DER E-MAILS VERWENDEN deaktiviert, kann ein SMTP-Server definiert werden, an den die ausgehenden E-Mails weitergeleitet werden sollen. Wenn eine Authentifizierung erforderlich ist, muss das entsprechende Verfahren im Fenster AUTHENTIFIZIERUNG ausgewählt werden.

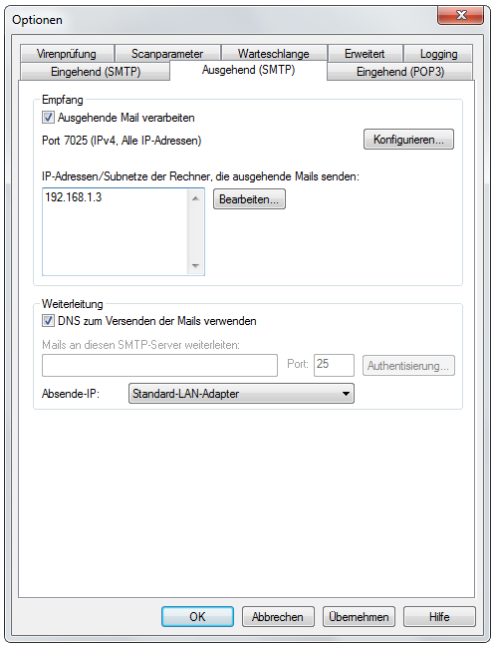

Abbildung 69: G DATA MailSecurity Administrator – Optionen, Ausgehend (SMTP)

POP3-Scans können auf der Registerkarte EINGEHEND (POP3) konfiguriert werden. Dazu wird die Option POP3-ANFRAGEN VERARBEITEN aktiviert und der Port eingegeben, an dem das MailGateway die POP3-Anfragen empfangen wird (**110**). Damit die E-Mail-Software dem Empfänger keinen Zeitüberschreitungsfehler anzeigt, wenn der POP3-Abruf zu lange dauert, muss das Kontrollkästchen ZEITÜBERSCHREITUNG BEIM E-MAIL-PROGRAMM VERMEIDEN aktiviert werden. Unter ABHOLUNG wird der POP3-Server eingegeben, von dem die E-Mails abgeholt werden sollen. Das ist normalerweise der POP3-Server des Internetanbieters. Das MailGateway nutzt die gleiche Anmeldung, die der Client bei seiner POP3-Anfrage verwendet. Unter FILTER

kann ein Ersatztext für E-Mails definiert werden, die vom Malware-Schutz oder Spam-Filter zurückgewiesen werden.

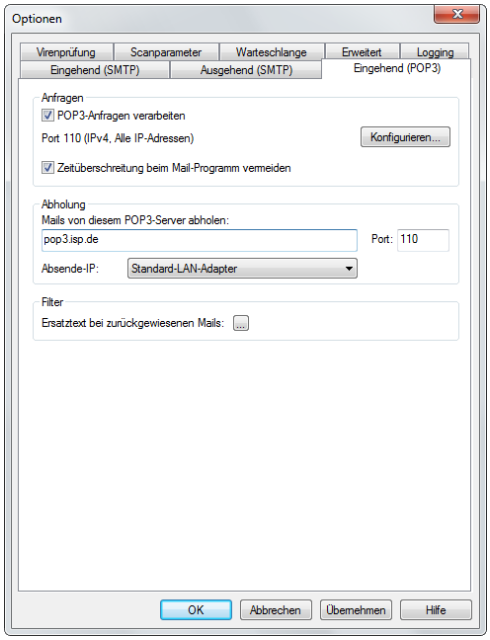

Abbildung 70: G DATA MailSecurity Administrator – Optionen, Eingehend (POP3)

Nach der Einrichtung vom MailGateway müssen auch die Einstellungen des Mail-Servers aktualisiert werden. Dazu wird der Server für eingehende POP3-E-Mails in die IP-Adresse des MailGateways (**192.168.1.2**) geändert und der MailGateway-Port (**110**) hinzugefügt. Damit ausgehende E-Mails richtig geroutet werden, muss die Einstellung des Mail-Servers für ausgehende SMTP-E-Mails in die IP-Adresse des MailGateways geändert und der MailGateway-Port (**25**) hinzugefügt werden. Anschließend wird die SMTP-Authentifizierung deaktiviert, da diese vom MailGateway durchgeführt wird.

Beim Empfang der eingehenden SMTP-E-Mails muss der MailGateway-Server den Mail-Server ersetzen. Dies lässt sich erreichen, indem der Router oder die Firewall so konfiguriert wird, dass eingehender SMTP-Verkehr an den MailGateway-Server (192.168.1.2) umgeleitet wird. Alternativ kann der DNS-MX-Eintrag in die (externe) IP-Adresse vom MailGateway geändert werden. Schließlich kann das MailGateway die IP-Adresse des Mail-Servers und dem Mail-Server eine neue IP-Adresse zugewiesen werden.

17.3.1.3. Schutz des SMTP-Relays

Bei Aktivierung der Verarbeitung von eingehenden SMTP-E-Mails sollte das MailGateway vor einem Relay-Missbrauch geschützt werden. Dazu werden auf der Registerkarte EINGEHEND (SMTP) unter SCHUTZ VOR RELAYING Domänen definiert, für die das MailGateway E-Mails akzeptiert. Wird keine Domäne hinzugefügt, werden keinerlei eingehende SMTP-E-Mails akzeptiert! Beim alleinigen Hinzufügen der Unternehmensdomänen werden E-Mails für andere Domänen automatisch verworfen und so wird sichergestellt, dass Spammer den MailGateway-Server nicht zum Verbreiten unerwünschter E-Mails nutzen können. Wenn eingehende E-Mails für alle Domänen akzeptiert werden sollen, muss die Domäne ***.*** hinzugefügt werden. Als Alternative zur manuellen Eingabe von Domänen kann mit dem Active Directory eine Adressliste importiert werden. E-Mails an Adressen, die nicht auf der Liste stehen, werden

automatisch verworfen. Zur Konfiguration der AD-Server-Einstellungen und des Update-Intervalls dient die Option ACTIVE DIRECTORY.

17.3.1.4. Mehrere POP3-Server

Sollen E-Mails von mehr als einem POP3-Server abgerufen werden, muss das standardmäßige Installationsszenario leicht abgewandelt werden. Anstatt in den MailGateway-Einstellungen einen einzigen POP3-Server zu definieren, kann der POP3-Server für jedes Konto auf dem Mail-Server (beispielsweise beim Abholen von POP3-E-Mails mit Exchange) oder Client (beim Abholen von POP3-E-Mails auf Clients) definiert werden. Dazu muss in dem MailSecurity Administrator die Registerkarte EINGEHEND (POP3) des Fensters OPTIONEN geöffnet werden. Anschließend muss die Adresse des POP3-Servers entfernt werden, die unter ABHOLUNG eingegeben wurde. In den Einstellungen des Mail-Servers oder lokalen Clients wird für jeden zu überprüfenden POP3-Server ein Konto definiert. Als POP3-Server werden die IP-Adresse und der Port vom MailGateway eingegeben. Anschließend muss das Feld „Benutzername“ für jedes Konto bearbeitet werden, indem der Name des POP3-Servers vor den Benutzernamen gesetzt wird und beide Werte durch einen Doppelpunkt voneinander getrennt werden. Um beispielsweise das Konto für den Benutzernamen **company** auf dem Server pop3.isp.com zu überprüfen, muss **pop3.isp.com:company** eingegeben werden. Das Feld „Kennwort“ sollte das Kontokennwort enthalten.

17.3.1.5. Warteschlange

Das MailGateway verarbeitet E-Mails sofort nach Erhalt. Malware-Scans und Spam-Filterungen werden durchgeführt und die Nachricht wird entsprechend den Installationseinstellungen an den Mail-Server weitergeleitet. Der empfangende Mail-Server ist aber möglicherweise nicht immer erreichbar. E-Mails, die nicht zugestellt werden können, werden in die Warteschlange gestellt. Das MailGateway wird über einen gewissen Zeitraum wiederholt versuchen, die Nachrichten in der Warteschlange zuzustellen. Mithilfe des Moduls WARTESCHLANGEN vom MailSecurity Administrator können die Nachrichten angezeigt werden, die sich aktuell in der Warteschlange befinden. Mithilfe der Schaltfläche EINGEHEND/AUSGEHEND kann zwischen der Anzeige von eingehenden und ausgehenden Nachrichten der Warteschlange umgeschaltet werden. Für jede Nachricht werden Ziel-Host, Sender, nächste Wiederholung und Status angezeigt. Die Nachrichten in der Warteschlange erfordern keinerlei Maßnahmen, das MailGateway kümmert sich automatisch um sie. Optional kann das MailGateway sofort versuchen, die Nachricht zuzustellen, indem auf JETZT WIEDERHOLEN geklickt wird. Mit der Schaltfläche LÖSCHEN können Nachrichten dauerhaft aus der Warteschlange gelöscht werden, wodurch eine Zustellung verhindert wird.

Der Umgang vom MailGateway mit Nachrichten in der Warteschlange kann im Fenster OPTIONEN auf der Registerkarte WARTESCHLANGE konfiguriert werden. Es wird regelmäßig versuchen, die Nachrichten in der Warteschlange zuzustellen, bis eine maximale Zeitspanne verstrichen ist. Dieses Maximum kann unter FEHLERWARTEZEIT (STUNDEN) definiert werden. Der Standardwert ist *24;* das bedeutet, wenn die Nachricht nach 24 Stunden noch nicht zugestellt ist, wird sie verworfen. Unter WIEDERHOLUNGSINTERVALL (STUNDEN) können Neuversuchsintervalle definiert werden. Das MailGateway wird versuchen, die Nachrichten in der Warteschlange in diesen Intervallen zuzustellen, bis die maximale Zeitspanne verstrichen ist. Die Standardwerte sind **0.25, 0.5, 1, 4**. Das bedeutet, dass der erste Neuversuch vom MailGateway nach 15 Minuten, der zweite nach einer halben Stunde und der dritte nach einer Stunde stattfinden werden.

Danach erfolgen weitere Neuversuche alle 4 Stunden, bis das Maximum erreicht ist. Die Standardwerte lassen sich an individuelle Bedürfnisse anpassen. Beispielsweise können kürzere Intervalle für die Neuversuche geplant werden (z. B. **0.25**, um es alle 15 Minuten erneut zu versuchen, bis das Maximum erreicht ist). Dies verhindert weitere Verzögerungen, wenn ein Mail-Server nur vorübergehend offline war, kann aber die Menge des E-Mail-Verkehrs vergrößern.

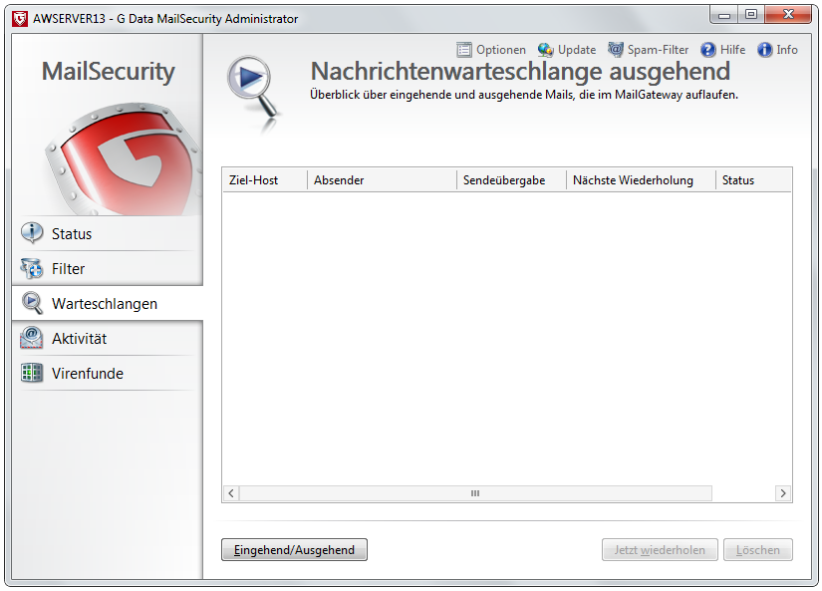

Abbildung 71: G DATA MailSecurity Administrator – Warteschlange

In jedem Fall sollten die Absender der E-Mails informiert werden, wenn ihre Nachricht (noch) nicht zugestellt werden konnte. Sie können im Abstand von wenigen Stunden (der Standardwert ist **4**) benachrichtigt werden. Es sollte vermieden werden, den Absendern zu viele Benachrichtigungen zu senden – nur bei einer Änderung der maximalen Wartezeit sollte das Benachrichtigungsintervall proportional geändert werden. Schließlich lässt sich die Anzahl der Nachrichten in der Warteschlange begrenzen. Diese Option ist standardmäßig deaktiviert, da eine Begrenzung der Warteschlange zu einem Verlust von Nachrichten führt, wenn das Maximum erreicht ist: E-Mails, die nicht zugestellt werden können, werden sofort gelöscht, wenn sich bereits zu viele Nachrichten in der Warteschlange befinden. Die Größenbegrenzung sollte nur aktiviert werden, wenn die Anzahl der Nachrichten in der Warteschlange die Leistung beeinträchtigt oder anderweitig Probleme verursacht.

17.3.2. Verwaltung und Migration

Wenn Malware-Schutz, Spam-Filter und benutzerdefinierte Filter bereitgestellt und konfiguriert wurden, führt das MailGateway seine Scans und Filterungen ohne Eingriff von außen durch. Das MailGateway benötigt keine Bestätigung, um E-Mails zurückzuweisen oder zu entfernen. Es empfiehlt sich aber, Leistung und Aktionen vom MailGateway zu überwachen, damit keine unerwarteten Schritte ergriffen werden. Die direkteste Methode, um den Umgang mit Spam durch das MailGateway zu überwachen, ist die Konfiguration der Weiterleitung von Spam-Nachrichten (siehe Abschnitt 17.3.4.10). Auf einer allgemeineren Ebene können die Administratoren den MailSecurity Administrator nutzen, um die Maßnahmen vom MailGateway zu überwachen. Das Modul AKTIVITÄT zeigt ein Protokoll der Schritte, die vom MailGateway unternommen werden, etwa das Empfangen, Verarbeiten oder Senden von E-Mails. Wurde die Datenbank für statistische Bewertung installiert (siehe Abschnitt 4.2.4.3), zeigt das Modul

STATUS die Schaltfläche STATISTIK an. Das Fenster „Statistik“ enthält eine allgemeine Statistik zu den verarbeiteten E-Mails sowie die Top-10-Listen für Spam-Adressen, Spam-IP-Adressen und erkannte Viren. Die Statistik lässt sich für jeden der Datenverkehrstreams anzeigen, die das MailGateway analysiert (SMTP eingehend, SMTP ausgehend bzw. POP3 eingehend). Die Statistik wird auf der Registerkarte LOGGING des Fensters OPTIONEN konfiguriert. Dazu wird die Option IN DER DATENBANK ABSPEICHERN ausgewählt, um eine Statistik über den E-Mail-Verkehr in der Datenbank zu speichern und eine Analyse zu ermöglichen. Alternativ können einige Einzelheiten zum Datenverkehr in einer Protokolldatei gespeichert werden (im Installationsordner vom MailGateway, standardmäßig C:\Programme (x86)\G Data\G DATA MailSecurity\maillog.txt). Die Protokolldatei enthält Zeitstempel, Absender, Empfänger, E-Mail-Größe und Spam-Wert (siehe Abschnitt 17.3.4.10). Um die Dateigröße zu begrenzen, kann das Protokollieren nur auf Junk-E-Mails oder auf eine maximale Anzahl von E-Mails beschränkt werden.

Falls das MailGateway auf einen anderen Server migriert wird, lassen sich seine Einstellungen mühelos exportieren. Im Menü OPTIONEN steht dazu auf der Registerkarte ERWEITERT die Schaltfläche EXPORTIEREN zur Verfügung. Sie ermöglicht es den Administratoren, eine XML-Datei mit den Einstellungen vom MailGateway zu speichern. Diese Datei kann mithilfe der Schaltfläche IMPORTIEREN auf den neuen Server importiert werden. Ebenso sollten vorhandene benutzerdefinierte Filter (siehe Abschnitt 17.3.4) exportiert werden. Mit den Schaltflächen IMPORTIEREN und EXPORTIEREN im Modul FILTER können Filtereinstellungen wie XML-Dateien verwaltet werden. Ist der Inhaltsfilter aktiviert (siehe Abschnitt 17.3.4.2), muss seine Konfiguration separat importiert werden, um seinen Fortschritt beizubehalten. Der MailGateway-Dienst muss im Windows-Bereich DIENSTE auf dem alten und neuen MailGateway-Server gestoppt werden. Die Konfigurationsdatei befindet sich im Ordner FILTER des MailGateways (standardmäßig: C:\Programme (x86)\G Data\G DATA MailSecurity\filter). Die Dateien „BayesSpam.txt“ und „BayesNotSpam.txt“ werden in den Ordner FILTER auf dem Zielserver kopiert, und der Dienst „MailGateway“ wird neu gestartet.

17.3.3. Malware-Schutz

E-Mails sind für Kriminelle nach wie vor ein sehr beliebter Angriffsvektor. Viele Formen von Malware werden per E-Mail verbreitet, in Form von allgemeinem Spam ebenso wie als gezielte Angriffe, um Zugang zu einem Unternehmensnetzwerk zu erhalten. Damit Schadprogramme keine Netzwerk-Clients infizieren können, sollten die eingehenden E-Mails von Malware befreit werden. Gleichzeitig müssen auch die von den Netzwerk-Clients gesendeten E-Mails überprüft werden. Infizierte Clients könnten unbemerkt mit Malware infizierte E-Mails versenden und damit externe E-Mail-Empfänger in Gefahr bringen. Das MailGateway scannt den ein- und ausgehenden E-Mail-Verkehr mit derselben Scan-Technologie auf Malware, die in seinem Security Client enthalten ist. Mithilfe von zwei Scan-Engines wird Malware erkannt, bevor sie den Empfänger erreicht. Anschließend können verschiedene Maßnahmen ergriffen werden, nämlich das Desinfizieren, Umbenennen oder Löschen des infizierten Objekts.

17.3.3.1. Ein- und ausgehende E-Mails

Die Malware-Erkennung kann im Fenster OPTIONEN vom MailSecurity Administrator konfiguriert werden. Auf der Registerkarte VIRENPRÜFUNG lassen sich Parameter für das Scannen von ein- und ausgehenden E-Mails definieren. Es wird empfohlen, die ein- und ausgehenden E-Mail-Streams auf Malware zu prüfen. Bei eingehenden E-Mails ist die wichtigste Entscheidung die, ob infizierte Nachrichten zugestellt werden

sollen oder nicht. Es sollte versucht werden, die infizierten Nachrichten oder Anhänge zu desinfizieren. Wenn keine Desinfizierung möglich ist, sollten sie gelöscht werden. Dadurch wird ein unnötiger Datenverlust verhindert und gleichzeitig dafür gesorgt, dass Endbenutzern niemals infizierte Inhalte zugestellt werden. Alternativ können infizierte Anhänge oder Nachrichten direkt gelöscht werden. Das ist die sicherste Maßnahme, kann aber zu einem Datenverlust führen, wenn ein Objekt fälschlicherweise als Malware erkannt wird. Die Umbenennung infizierter Anhänge ist die dritte Option, wird aber nicht empfohlen. Sie verhindert zwar einen direkten Zugriff auf die Malware, Endbenutzer könnten aber immer noch infiziert werden, wenn die Datei erneut umbenannt und geöffnet wird. Um den Empfänger der E-Mail darüber zu benachrichtigen, dass Malware gefunden wurde, kann eine Virenwarnung zum Betreff und Text der infizierten Nachricht hinzugefügt werden. Dies ist empfehlenswert, um den Empfänger darauf hinzuweisen, dass die Nachricht verändert wurde und nicht mehr die ursprünglich gesendete Nachricht ist. Dabei wird die Tatsache betont, dass das Virus entfernt wurde und eine Infektion nicht mehr möglich ist. Wenn die E-Mail einen kennwortgeschützten Anhang enthält, kann der Anhang nicht gescannt werden. Dem Nachrichtentext kann dann ein Hinweis hinzugefügt werden, der den Empfänger warnt und ihm erklärt, dass ein oder mehrere Anhänge nicht gescannt wurden. Zusätzlich zum Hinweis für den Empfänger lassen sich eine oder mehrere E-Mail-Adressen (mit Semikola getrennt) definieren, die bei der Erkennung von Malware eine Warnung erhalten sollen. Bei eigenständigen MailGateway-Installationen ist dies eine einfach konfigurierbare Möglichkeit, um sicherzustellen, dass der Administrator informiert wird. Wurde das MailGateway im selben Netzwerk wie eine bestehende ManagementServer-Installation bereitgestellt, sollte stattdessen die Option VIRENFUNDE AN G DATA MANAGEMENTSERVER MELDEN verwendet werden.

Bei ausgehenden E-Mails sind die Sicherheitsoptionen etwas anders. Ausgehende Nachrichten werden zwar von denselben Scan-Engines wie die eingehenden Nachrichten gescannt, die Reaktion auf infizierte Nachrichten ist aber eine andere: Sie werden nicht gesendet. Eine Desinfektion oder Umbenennung von Anhängen ist nicht möglich, da eine Zustellung von Nachrichten mit möglicher Malware um jeden Preis verhindert werden muss. Bei der Erkennung von Malware kann der Absender benachrichtigt werden. Es empfiehlt sich, eine Benachrichtigung zu versenden und zu erklären, dass die Nachricht nicht zugestellt wird. Wenn keine Malware erkannt wird, kann MailGateway ausgehenden Nachrichten einen Bericht mit den Versionsdaten hinzufügen. Damit wird der Empfänger benachrichtigt, dass die Nachricht vor dem Versand auf Malware gescannt wurde. Wie bei eingehenden Nachrichten können auch hier E-Mail-Adressen definiert werden, an die im Falle einer Malware-Infektion eine Warnung gesendet werden soll.

17.3.3.2. Scanparameter

Die Einstellungen für den Malware-Scan können auf der Registerkarte SCANPARAMETER individuell angepasst werden. Die Standardkonfiguration bietet optimalen Schutz. Die Scanparameter sollten nur geändert werden, wenn Probleme mit der Leistung oder mit einem der individuellen Schutzmodule auftreten. Wenn der Scan-Vorgang mit zwei Engines zu anspruchsvoll ist, kann eine der Engines deaktiviert werden. Dadurch wird die Leistung verbessert, aber auch der Grad der Sicherheit leicht verringert. Scans lassen sich auf bestimmte Dateitypen beschränken, etwa Programmdateien oder Dokumente, oder anhand einer benutzerdefinierten Liste von Dateierweiterungen durchführen. Die sicherste (und standardmäßig aktivierte) Option ist aber, alle Dateien zu scannen. Auch die Heuristik ist standardmäßig aktiviert und bietet zusätzliche Sicherheit, indem sie unbekannte Malware anhand typischer Merkmale erkennt. Durch Deaktivierung der Option ARCHIVE PRÜFEN können Archive aus den Scans ausgeschlossen werden. Wenn

eine Datei in einem Archiv infiziert ist, wird das ganze Archiv umbenannt oder entfernt. Um einen versehentlichen Datenverlust zu verhindern, kann die Überprüfung von Archiven auf Malware deaktiviert werden. Dies führt jedoch zu einer geringeren Sicherheit. OutbreakShield bietet Schutz vor Massen-E-Mails mit Malware, noch bevor die Virensignaturen verfügbar sind, und sollte in den meisten Fällen aktiviert werden. Es desinfiziert keine E-Mails, die Malware enthalten. Unter EINSTELLUNGEN kann ein Ersatztext für den E-Mail-Text eingegeben werden, damit die Empfänger wissen, dass eine E-Mail von OutbreakShield blockiert wurde. Ein Phishing-Schutz blockiert schließlich E-Mails, die versuchen, Kennwörter, Kreditkartennummern oder andere persönliche Daten zu erlangen, indem sie sich als E-Mails von seriösen Institutionen ausgeben.

17.3.4. Filter

Malware stellt eine Bedrohung für E-Mail-Empfänger dar, aber sie ist nicht die einzige Inhaltsart, die eine Filterung rechtfertigt. In vielen Unternehmensumgebungen sollen E-Mails nur für geschäftsbezogene Kommunikationen genutzt werden. Unangemessene, ungesetzliche, ablenkende oder allgemein unerwünschte Inhalte wie Spam müssen herausgefiltert werden. Zusätzlich zu seinem Schutz vor Malware bietet das MailGateway mehrere Filter, die zum Filtern von E-Mails genutzt werden können, die Unternehmensrichtlinien nicht erfüllen oder anderweitig überflüssig sind.

Die Filter werden im Modul FILTER vom MailSecurity Administrator verwaltet. Es enthält eine Übersicht über alle aktuellen Filter. Unter der Liste befindet sich eine Gruppe von Schaltflächen mit Funktionen für alle Filter. Die Einstellungen können für alle Filter auf einmal im- und exportiert werden (siehe Abschnitt 17.3.2). Mithilfe der Schaltfläche STATISTIK können für jeden Filter einige grundlegende Statistiken angezeigt werden: die Anzahl der E-Mails, die verarbeitet worden sind, und die Anzahl derer, die zum konkreten Filter gepasst haben. Zum Verwalten der Filter können die Schaltflächen NEU, BEARBEITEN und LÖSCHEN genutzt werden. Ein Filter wird mithilfe seines Kontrollkästchens aktiviert oder deaktiviert.

Jeder Filter hat bestimmte Optionen, die sich beim Hinzufügen des Filters oder durch Klicken auf die Schaltfläche BEARBEITEN ändern lassen. Alle Filter beinhalten die Felder NAME und BEMERKUNG. Der Filtername kann bearbeitet werden, um die Filter in der Filterliste unterscheiden zu können. Das ist besonders hilfreich für Filter, die mehrere Instanzen haben können, etwa der Filter ABSENDER und EMPFÄNGER. Die BEMERKUNG wird auch in der Liste angezeigt – ein praktischer Ort für Anmerkungen zu den konkreten Filtereinstellungen.

Ähnlich wie bei den Maßnahmen, die sich für mit Malware infizierte Dateien konfigurieren lassen, kann das MailGateway auch verschiedene Schritte unternehmen, wenn eine E-Mail zu einem Filter passt. Die meisten Filter lassen sich so konfigurieren, dass sie zum Filter passende Nachrichten zurückweisen. Zusätzlich kann der Absender der Nachricht mit einem individuell anpassbaren Text darüber informiert werden, dass der Empfänger die Nachricht nicht erhalten hat. Eine Warnung kann an eine oder mehrere Personen geschickt werden. Das ist eine leistungsstarke Maßnahme für Administratoren, die den Status des E-Mail-Verkehrs im Netzwerk nachverfolgen möchten. Die Warnungen können die E-Mail enthalten, die zum Filter passte. Das kann für die Analyse zwar praktisch sein, die Nachrichten könnten aber mit Malware infizierte oder anderweitig unangemessene Inhalte enthalten. Deshalb sollten alle weitergeleiteten Nachrichten mit Vorsicht behandelt werden.

Die meisten Filter lassen sich sowohl auf eingehende als auch auf ausgehende E-Mails anwenden (außer in Fällen, in denen der Filter logischerweise nur auf eine Art von E-Mail-Verkehr anwendbar ist, etwa beim Greylist-Filter). Für die Sicherheit der Endbenutzer im Unternehmen wird empfohlen, Filter für den eingehenden E-Mail-Verkehr zu aktivieren. Die Aktivierung von einem oder mehreren Filtern für ausgehende E-Mails stellt sicher, dass ausgehende Unternehmens-E-Mails die Sicherheitsanforderungen erfüllen.

17.3.4.1. Anhänge

Anhänge sind schon lange ein wichtiger Weg zur Verbreitung von Malware. Früher hat Malware sich selbst verbreitet, indem sie eine E-Mail mit einer bösartigen ausführbaren Datei im Anhang an alle Kontakte im Adressbuch des Opfers schickte. Heutige Malware-Autoren führen oft gezielte Angriffe aus, indem sie nur an eine ausgewählte Gruppe von Empfängern E-Mails mit Malware senden, in der Hoffnung, so Zugang zu wertvollen Dokumenten auf Computern zu erlangen. Malware wird normalerweise vom Dateisystemwächter des Zielcomputers erfasst. Das Risiko kann aber noch weiter gesenkt werden, indem das MailGateway risikoreiche Anhänge filtert.

Der Anhangsfilter kann im Blacklist- oder Whitelist-Modus ausgeführt werden. Im Blacklist-Modus sind Anhänge nicht zulässig, wenn sie auf der Liste stehen. Im Whitelist-Modus sind nur die aufgeführten Anhangsarten zulässig und alle anderen werden entfernt. Wie bei den meisten Filtermodulen bietet die Nutzung eines Whitelist-Modus auch hier die größte Sicherheit. Indem man alles außer zuvor genehmigten Dateierweiterungen untersagt, werden auch unbekannte Angriffsvektoren blockiert. Es kann aber auch zulässiger Inhalt blockiert werden, wenn sein Dateityp nicht ausdrücklich als sicher definiert wurde. Im Blacklist-Modus können alle bekannten gefährlichen Dateitypen ausdrücklich verboten werden. Er schützt vor den am häufigsten verwendeten Arten von Malware-Anhängen, kann aber Malware passieren lassen, wenn diese einen Angriffsvektor nutzt, der nicht ausdrücklich als unsicher definiert wurde.

Die zu filternden Anhangsarten können auf die Liste DATEIERWEITERUNGEN gesetzt werden. Mehrere Erweiterungen werden durch Semikola voneinander getrennt. Bei der Verwendung des Filters im Blacklist-Modus gehören üblicherweise ausführbare Dateien wie .exe, .scr und .com zu den Erweiterungen, die blockiert werden. Skripte können Erweiterungen wie .bat, .vbs, .js und .cmd tragen und sollten ebenfalls blockiert werden. Auch Registry-Einstellungsdateien (.reg) lassen sich blockieren. Archivdateien wie .zip, .rar und .7z könnten Malware enthalten und lassen sich filtern. Darüber hinaus kann jede andere Erweiterung blockiert werden, wenn sie beispielsweise die Unternehmensrichtlinien nicht erfüllt. Wenn man Erweiterungen auf die Whitelist setzt, sollte diese Liste auf den am häufigsten empfangenen Dateiformaten wie .txt, .doc oder .jpg basieren. Wenn Anhänge auf die Whitelist gesetzt werden, bedeutet es nicht unbedingt, dass sie sicher sind. Auch Dokumente können Malware enthalten. Der Malware-Schutz vom MailGateway sollte die Anhänge scannen und die Clients müssen den E-Mail-Scan oder den Dateisystemwächter aktivieren. Bei Aktivierung der Option AUCH ANHÄNGE IN EINGEBETTETEN MAILS FILTERN filtert das MailGateway sogar Anhänge, wenn diese in einer eingebetteten E-Mail-Datei verschachtelt sind. Diese Option sollte aktiviert bleiben, um zu gewährleisten, dass auch als eingebettete E-Mail-Datei weitergeleitete Nachrichten gesichert sind.

Wenn das MailGateway einen oder mehrere problematische Anhänge in einer E-Mail entdeckt, kann es mehrere Maßnahmen ergreifen. Durch die Aktivierung von ANHÄNGE NUR UMBENENNEN wird der Wert aus dem

Feld SUFFIX hinzugefügt, um den Anhang umzubenennen. Das ist praktisch, um die Ausführung von ausführbaren Dateien (auch Office-Dokumente) zu verhindern, da Benutzer die Datei speichern und umbenennen müssten, um sie auszuführen. Für zusätzliche Sicherheit kann die Option ANHÄNGE NUR UMBENENNEN deaktiviert werden. Das MailGateway löscht dann alle Anhänge, die mit der Erweiterungsliste übereinstimmen (Blacklist) bzw. die nicht mit der Liste übereinstimmen (Whitelist). Das Entfernen des Anhangs ist empfehlenswert, kann aber zu einem Datenverlust führen. Wenn alle Client-Computer durch einen Dateisystemwächter geschützt sind, können Anhänge umbenannt werden, anstatt sie zu entfernen. Dies wird jedoch nicht empfohlen. Zusätzlich zum Umbenennen oder Entfernen des Anhangs kann eine Nachricht in den E-Mail-Text eingefügt werden. Durch Hinzufügen einer Nachricht können die Empfänger darüber informiert werden, dass ein Virus gefunden wurde. Dadurch wird auch eine eventuelle Verwirrung behoben, die durch Verweise auf Anhänge im Nachrichtentext entstehen kann.

17.3.4.2. Inhalt

Der Inhaltsfilter kann als Erweiterung des eingebauten Spam-Filters vom MailGateway genutzt werden. Letzterer ist für die Erkennung von Spam optimiert worden und verfügt beispielsweise über spezielle Wortlisten und spam-zentrierte Module. Mithilfe des Inhaltsfilters lässt sich hingegen jede Art von Inhalt filtern. Beispielsweise kann nicht zur Arbeit gehörender Inhalt herausgefiltert werden, indem Filter für beliebte, nicht themenbezogene Ausdrücke hinzugefügt werden. Ein weiteres Beispiel ist das Filtern sensibler Inhalte, von denen Konkurrenten profitieren könnten.

Die Inhaltsart, die gefiltert werden soll, kann in Form eines regulären Ausdrucks eingegeben werden. Reguläre Ausdrücke sind sehr leistungsstarke Hilfsmittel für Übereinstimmungen mit komplexen Zeichensequenzen. Mit der Schaltfläche NEU kann ein regulärer Ausdruck aufgebaut werden, indem mehrere Suchbegriffe eingegeben und miteinander verglichen werden. Das hilft Administratoren, die mit regulären Ausdrücken nicht vertraut sind. Alternativ dienen Online-Ressourcen über reguläre Ausdrücke als Orientierung[21]. Der SUCHBEREICH kann so definiert werden, dass er KOPFZEILE, BETREFF, E-MAIL-TEXT, HTML-TEXT bzw. EINGEBETTETE E-MAIL der E-Mails enthält.

17.3.4.3. Externe Verweise

E-Mails enthalten oft HTML-Verweise auf externe Inhalte wie Bilder, Links oder Skripte. Externe Inhalte können nützlich sein, beispielsweise für Vorlagen eines E-Mail-Layouts, werden aber oft von Spammern und Malware-Verbreitern genutzt. Mithilfe von externen Bildern können Spammer die Aktivität des E-Mail-Kontos messen: Wenn der Spammer individualisierte Bildlinks in E-Mails einbettet, kann er beobachten, wie der E-Mail-Client das Bild herunterlädt. Dadurch weiß er, dass die E-Mail gelesen wurde. Außerdem könnte die IP-Adresse des Clients protokolliert werden. Um vollständig zu verhindern, dass externe Inhalte heruntergeladen werden, können externe Verweise komplett aus den eingehenden E-Mails herausgefiltert werden. Der Filter hat keine weiteren Optionen.

[21] Ein Ausgangspunkt ist der Wikipedia-Artikel über „Reguläre Ausdrücke“, der eine Reihe von Beispielen enthält: https://de.wikipedia.org/wiki/Regulärer_Ausdruck#Beispiele.

17.3.4.4. Greylist

Der Greylist-Filter macht sich die Tatsache zunutze, dass Spammer normalerweise kein E-Mail-Warteschlangensystem verwenden: Eine Spam-Nachricht wird normalerweise nur einmal versendet; der Mail-Server des Spammers versucht nicht, die Nachricht erneut zu versenden. Seriöse Mail-Server versuchen, E-Mails erneut zu senden, wenn sie beim ersten Versuch nicht zugestellt werden konnten. Wenn der Greylist-Filter aktiviert ist, akzeptiert das MailGateway eingehende E-Mails nicht sofort. Stattdessen zeigt es dem sendenden Server eine Aufforderung an, die Nachricht erneut zu versenden. Seriöse Mail-Server werden dieser Aufforderung nachkommen und die Nachricht erneut senden – Spam-Server nicht. Wenn die Nachricht erneut gesendet wird, passiert sie den Greylist-Filter. Zusätzlich wird die Kombination aus Absenderadresse, Empfängeradresse und Kennung des sendenden Mail-Servers auf die Greylist gesetzt, damit zukünftige E-Mails sofort zugestellt werden.

Zur Aktivierung des Greylist-Filters muss der Spam-Filter aktiv sein (siehe Abschnitt 17.3.4.10). Zusätzlich muss während der Installation von MailGateway Microsoft SQL Server 2008 SP3 Express installiert worden sein (siehe Abschnitt 4.2.4.3).

Nach der Aktivierung des Greylist-Filters können mehrere Optionen definiert werden. Unter WARTEZEIT kann die Zeitspanne bearbeitet werden, in der eine E-Mail zurückgehalten wird. Der Standard liegt bei 0 Minuten für normale E-Mails (die Greylist ist effektiv ausgeschaltet) und bei 30 Minuten für E-Mails, die als verdächtig klassifiziert wurden. Eine Nachricht gilt als verdächtig, wenn die E-Mail-Kopfzeile eventuell manipuliert wurde, beispielsweise dann, wenn eine Rückwärtssuche Abweichungen zwischen dem Namen und der IP-Adresse des Mail-Servers aufdeckt. Eine verdächtige Nachricht wird nur zugestellt, wenn der sendende Server die Nachricht nach mindestens 30 Minuten erneut sendet. Wenn der sendende Server die Nachricht erneut sendet, bevor die 30 Minuten verstrichen sind, wird ihm mitgeteilt, dass er es später noch einmal versuchen soll.

Damit die Greylist auf dem neuesten Stand bleibt, steht die Kombination aus Absenderadresse, Empfängeradresse und Kennung des sendenden Mail-Servers nur für eine bestimmte Zeit auf der Greylist. Es können zwei separate LEBENSZEITEN für die Whitelist festgelegt werden: mit oder ohne E-Mail-Austausch. Der Wert OHNE E-MAIL-AUSTAUSCH gilt für E-Mails auf der Greylist, die nicht erneut gesendet werden. Wenn der sendende Mail-Server die E-Mail innerhalb dieser Zeitspanne (Standard: 2 Tage) nicht erneut sendet, wird sie von der Greylist entfernt. Diese Maßnahme sorgt dafür, dass die Greylist nicht mit Einträgen von Spam-Servern gefüllt wird, die eine E-Mail nur einmal ohne erneuten Versuch versenden. Der Wert MIT E-MAIL-AUSTAUSCH regelt Greylist-Einträge, für die der sendende Mail-Server die E-Mail erneut gesendet hat. Jedes Mal, wenn eine empfangene E-Mail zum Greylist-Eintrag passt, wird sie sofort zugestellt und der Greylist-Timer wird zurückgesetzt. Dies gewährleistet eine rasche Zustellung von wiederholt eingehenden E-Mails wie etwa Newslettern.

17.3.4.5. HTML-Skripte

HTML kann in E-Mails zwar auf legitime Weise verwendet werden, beispielsweise zur Definition des Layouts, es gibt aber auch ein Sicherheitsrisiko. Nach dem Öffnen einer E-Mail können bösartige Skripte ausgeführt werden und einen Computer mit Malware infizieren oder anderes unerwünschtes Verhalten zeigen. Der HTML-Skript-Filter entfernt alle Skripte aus ein- bzw. ausgehenden E-Mails. Jedes Tag-Paar

eines HTML-Skripts (<script> und </script>) wird herausgefiltert, wodurch mögliche Bedrohungen beseitigt werden. Der Filter hat keine weiteren Optionen.

17.3.4.6. IP-Adressen

Der IP-Filter kann dazu genutzt werden, Mail-Server auf die Blacklist oder Whitelist zu setzen. Wenn bestimmte Server keine E-Mails an das Unternehmensnetzwerk senden sollen, kann ihre IP-Adresse zum IP-Filter hinzugefügt und so auf die Blacklist gesetzt werden. Umgekehrt können die entsprechenden IP-Adressen auf die Whitelist gesetzt werden, wenn nur wenige, bestimmte Mail-Server E-Mails senden dürfen. IP-Adressen können als einzelne Adressen oder mit der CIDR-Notation eingegeben werden. Bei einer Migration oder einem Import des Mail-Servers von einem anderen System lässt sich die Liste der IP-Adressen als einfache Textliste ex- und importieren.

17.3.4.7. Sprache

Wenn die Netzwerk-Clients im Allgemeinen nicht in einer bestimmten Sprache kommunizieren, kann angenommen werden, dass eingehende Nachrichten in dieser Sprache unerwünscht sind. Mit dem Sprachfilter können Nachrichten, die in einer bestimmten Sprache geschrieben sind, gefiltert werden. Beispielsweise könnte ein englischsprachiges Unternehmen, das keine Geschäftspartner oder Kunden in Japan hat, E-Mails in japanischer Sprache blockieren, um Spam einzuschränken.

Das Spracherkennungssystem vom MailGateway weist jeder E-Mail eine Spracherkennungsrate zu. Unter UNERWÜNSCHTE SPRACHEN können die Sprachen ausgewählt werden, für die E-Mails herausgefiltert werden sollen. Zusätzlich zu den Standardmaßnahmen kann das MailGateway dem Betreff und Text der E-Mail eine Spam-Warnung hinzufügen. Das Standardpräfix für den Betreff ist **[%L %P]**, wodurch dem Betreff Sprache und Prozentsatz der Sprachübereinstimmung hinzugefügt werden. Dem Betreff oder Text kann jede beliebige Nachricht hinzugefügt werden.

17.3.4.8. Lesebestätigungsanforderungen

Für viele E-Mail-Benutzer bietet die Praxis, Lesebestätigungen anzufordern, die Gewissheit, dass der Empfänger eine bestimmte E-Mail auch wirklich gelesen hat. Für die Empfänger hingegen können Lesebestätigungen ärgerlich sein, besonders dann, wenn die E-Mail ohnehin eine Antwort erfordert. Außerdem könnten Spammer Lesebestätigungen anfordern, um die Aktivität eines E-Mail-Kontos zu messen und das Spam-Volumen zu erhöhen, wenn das E-Mail-Konto aktiv genutzt wird. Der Filter hat keine weiteren Optionen.

17.3.4.9. Absender/Empfänger

E-Mails können abhängig von Absender oder Empfänger gefiltert werden. Wenn bestimmte Domänen unerwünschte E-Mails versenden, um die sich keiner der anderen Filter kümmert, kann die Domäne als Absenderfilter hinzugefügt werden, damit sie herausgefiltert wird. Gleiches gilt für E-Mails, die an bestimmte Empfängeradressen oder -domänen adressiert sind. Der Empfängerfilter wird im Kampf gegen unerwünschte E-Mails vielleicht nicht häufig verwendet, lässt sich aber so einrichten, dass er eine Warnung verschickt, wenn diesem konkreten Empfänger E-Mails zugestellt werden.

Der Absenderfilter lässt sich passend für E-Mails konfigurieren, die keinen Absender haben. Das ist eine praktische Maßnahme zur Abwehr von Spammern, die eine E-Mail-Kopfzeile manipulieren und die Absenderinformationen weglassen. Der Empfängerfilter kann optional auch Nachrichten mit einem leeren Empfängerfeld erfassen (Nachrichten, die nur CC- oder BCC-Empfänger enthalten).

17.3.4.10. Spam

Wie der Spam-Filter des Exchange-Plug-ins bietet auch das MailGateway zentralisierte Spam-Filter-Möglichkeiten, die Spam aus dem E-Mail-Verkehr entfernen, bevor er den Clients überhaupt zugestellt wird. Auf der Registerkarte FILTER kann der vollautomatische Spam-Filter vom MailGateway als Ganzer aktiviert oder deaktiviert werden. Standardmäßig ist er aktiviert. Damit der Filter in der Listenansicht des Moduls FILTER erkannt werden kann, wird ein Name und ein Hinweis hinzugefügt (siehe Abschnitt 17.3.4). Der Spam-Filter scannt alle E-Mails und weist sie einer von vier Kategorien zu: Kein Spam, Spamverdacht, Hohe Spamwahrscheinlichkeit und Sehr hohe Spamwahrscheinlichkeit. E-Mails, die als „Kein Spam“ klassifiziert wurden, werden sofort zugestellt. Für die anderen drei Kategorien können individuelle Reaktionen definiert werden. Die Reaktionseinstellungen für jede Kategorie können auf der Registerkarte FILTER mithilfe der Option ÄNDERN konfiguriert werden. E-Mails können zurückgewiesen oder mit einer Spam-Warnung im Betreff oder Text versehen werden bzw. kann der Absender der Nachricht informiert und die E-Mail an jemanden weitergeleitet werden. Es ist sicher, das MailGateway so zu konfigurieren, dass E-Mails mit einer hohen oder sehr hohen Spam-Wahrscheinlichkeit zurückgewiesen werden. Optional können die Nachrichten an einen Administrator weitergeleitet werden, der Feineinstellungen des Filters vornehmen kann, wenn die Nachrichten nicht korrekt kategorisiert werden. Vermuteter Spam sollte nicht sofort zurückgewiesen werden – wie auch bei den Malware-Scans besteht das Risiko von false positive Ergebnissen. Da nur eine geringe Anzahl von Nachrichten in diese Kategorie fällt, können sie dem Empfänger zugestellt werden. Als Warnung sollte der Nachricht ein Betreffpräfix oder ein Text hinzugefügt werden.

Wertbasierte Einstufung

Wenn die Maßnahmen konfiguriert wurden, die das MailGateway beim Erkennen von Spam ergreifen soll, können die Parameter, die diese Erkennung regeln, optimiert werden. Kern des automatischen Spam-Filters ist ein wertbasiertes Einstufungssystem, das eine Nachricht als Spam kategorisiert, sobald sie einen bestimmten Wert erreicht. Durch individuelle Kriterien wie Betreff, Text oder (das Fehlen einer) Nachrichtenkennung werden Punkte zum Spam-Indexwert einer Nachricht hinzugefügt. Durch Kriterien wie E-Mail-Größe oder Inhaltsfilterbewertung werden Punkte abgezogen. Nach der Addition der verschiedenen Werte bestimmt das Endergebnis darüber, ob die Nachricht als Spam gilt oder nicht. Auf der Registerkarte ERWEITERTE EINSTELLUNGEN können die einzelnen Bewertungskomponenten angepasst werden. Das sollte aber fast nie notwendig sein – nur dann, wenn Spam fälschlicherweise als sicher markiert wird oder wenn Nachrichten versehentlich als Spam behandelt werden. Zusätzlich zum Einstufungssystem können Nachrichten von einem der verschiedenen anderen Parameter des Spam-Filters als Spam markiert werden.

Blacklist/Whitelist

Mit der Registerkarte BLACKLIST können E-Mail-Adressen oder -Domänen als Spam definiert werden. Jede von einer der aufgeführten Adressen oder Domänen eingehende E-Mail wird sofort als Spam markiert. Die Registerkarte WHITELIST tut das Gegenteil: E-Mail-Adressen und -Domänen, die auf der Whitelist stehen, können immer E-Mails senden und diese werden nie als Spam markiert. Mit einer Kombination aus Black- und Whitelist können Administratoren den Spam-Filter optimieren. Wenn eine bestimmte Art von Nachricht, etwa ein wiederkehrender Newsletter, beständig als Spam markiert wird, kann er auf die Whitelist gesetzt werden. Umgekehrt kann eine wiederkehrende E-Mail, die unerwünscht ist, ausdrücklich auf die Blacklist gesetzt werden.

Schlüsselwörter

Anstatt eine E-Mail anhand ihrer Absenderadresse oder -domäne zu kategorisieren, kann das MailGateway sie auch auf bestimmte Schlüsselwörter hin scannen. Wenn eines davon in einer Nachricht erscheint, wird diese direkt als Spam markiert. Für Betreff und Text der Nachricht können separate Schlüsselwörterlisten definiert werden. Beide Listen sind standardmäßig aktiviert und bereits mit Begriffen gefüllt, die von Spammern häufig verwendet werden. Wenn ein bestimmter Inhalt immer als Spam gefiltert werden soll, können einer oder beiden Listen Schlüsselwörter hinzugefügt werden. Standardmäßig ist die Option NUR VOLLSTÄNDIGE WÖRTER SUCHEN aktiviert. Dadurch ist gewährleistet, dass eine Nachricht nicht als Spam kategorisiert wird, wenn sie ein Wort enthält, das teilweise mit einem Schlüsselwort übereinstimmt. Zum Beispiel: Um Nachrichten herauszufiltern, bei denen es um Bargeld geht, kann den Schlüsselwortlisten für Betreff und Text das Schlüsselwort „cash“ (Bargeld) hinzugefügt werden. Wenn die Option NUR VOLLSTÄNDIGE WÖRTER SUCHEN deaktiviert wäre, würde das MailGateway alle Vorkommen von „cash“ erkennen, also auch in Wörtern wie „cashew“ (Cashewnuss) oder „cashier“ (Kassierer). Um diese Art von unbeabsichtigtem Filtern zu vermeiden, sollte die Option aktiviert bleiben.

Realtime-Blacklists

Realtime-Blacklists (RBLs) können auf einer speziellen Registerkarte konfiguriert werden. Sie werden typischerweise von Anti-Spam-Online-Organisationen verwaltet und enthalten Listen von Mail-Servern, die bekanntermaßen von Spammern genutzt werden. Wenn das MailGateway so konfiguriert ist, dass es Realtime-Blacklists nutzt, konsultiert es eine Reihe von Online-Listen, um zu sehen, ob die Domäne des Absenders auf eine Blacklist gesetzt wurde. Wenn dies der Fall ist, werden dem Spam-Indexwert der Nachricht Punkte hinzugefügt. Das MailGateway kann die RBLs nutzen, die standardmäßig definiert wurden. Diese können aber bei Bedarf auch durch andere URLs ersetzt werden. Wenn eine Domäne unabhängig davon, ob sie auf einer RBL steht oder nicht, immer erlaubt werden soll, kann sie auf die Whitelist gesetzt werden.

Bayesscher Inhaltsfilter

Wenn alle Anti-Spam-Parameter definiert worden sind, kann der INHALTSFILTER aktiviert werden, um eine zusätzliche Schutzschicht hinzuzufügen. Es ist ein selbstlernender Filter, der auf dem Prinzip des Bayesschen Spam-Filters beruht. Wenn er aktiviert ist, werden die Merkmale jeder E-Mail, die als Spam gekennzeichnet wird, in einer Datenbank gespeichert. Zukünftige E-Mails werden auf der Grundlage

dieser Merkmale gescannt. Das hilft dabei, Spam-Nachrichten auch dann zu erkennen, wenn sie sich leicht von dem unterscheiden, was mit Parametern wie Whitelist, Blacklist und Schlüsselwörter definiert worden ist. Auf der Registerkarte INHALTSFILTER wird eine Statistik über die Menge der E-Mails angezeigt, die der Filterdatenbank hinzugefügt wurden – je mehr E-Mails gescannt werden, desto besser funktioniert der Bayessche Filter.

18. Erweiterte Konfiguration

Die Unternehmenslösungen von G DATA sind so konzipiert, dass sie direkt bereitgestellt werden können. Es ist keine erweiterte Konfiguration erforderlich, um Server- und Client-Komponenten in Gang zu bringen. Alle üblichen Einstellungen sind über die Benutzeroberflächen des G DATA Administrators und des G DATA MailSecurity Administrators verfügbar. Es stehen verschiedene erweiterte Konfigurationsmöglichkeiten zur Verfügung, damit die Lösungen von G DATA optimal in einem Unternehmensnetzwerk laufen. Diese Einstellungen müssen normalerweise nicht geändert werden und sie sollten nur bearbeitet werden, wenn der G DATA Support dazu auffordert.

Wie bei jeder erweiterten Konfiguration muss gewährleistet sein, dass ein Backup der Konfigurationsdateien existiert, bevor eine Neukonfiguration vorgenommen wird. Wenn eine der Komponenten der G DATA Lösung nach der Konfigurationsänderung ein unerwünschtes Verhalten zeigt, kann so auf das Backup zurückgegriffen werden. Es dürfen nur die Optionen bearbeitet werden, die für das zu behebende Problem gelten. Beim Ändern der Windows Registry kann die Bearbeitung der falschen Werte zu einer Instabilität des Systems oder anderen unvorhersehbaren Verhaltensweisen führen. Um sicherzugehen, dass unbeabsichtigte Änderungen rückgängig gemacht werden können, sollte mithilfe der Windows-Systemwiederherstellung ein Wiederherstellungspunkt erstellt oder der relevante bzw. die relevanten Registry-Schlüssel exportiert werden, bevor Änderungen erfolgen.

Um unerwünschtes Verhalten beim Bearbeiten von Konfigurationsdateien zu vermeiden, sollten die Hintergrunddienste der jeweiligen Software von G DATA, wie G DATA ManagementServer oder G DATA MailSecurity MailGateway geschlossen sein und nach deren Speicherung neu gestartet werden (mithilfe des Fensters „Dienste“: Start, Ausführen, **services.msc**).

18.1. GdmmsConfig.exe

Üblicherweise werden die Datenbankzugriffsdaten während der Installation vom ManagementServer automatisch konfiguriert. Für eine erweiterte Datenbankverwaltung ist jedoch GdmmsConfig.exe ein sehr wertvolles Hilfsmittel. Es kann zur Durchführung von Backups (siehe Abschnitt 4.7) sowie zur Wartung und Konfiguration verwendet werden. GdmmsConfig.exe befindet sich im Installationsordner vom G DATA ManagementServer (standardmäßig: C:\Programme (x86)\G Data\G DATA AntiVirus ManagementServer). Bei der Ausführung von GdmmsConfig.exe zeigt es die aktuellen Daten an, mit denen der ManagementServer eine Verbindung zu seiner Datenbank herstellt.

Unter SQL-SERVER zeigt GdmmsConfig.exe die aktuelle Instanz von SQL Server (Express) an. Sie kann manuell eingegeben oder aus einer Liste übernommen werden. Durch Klicken auf den Pfeil wird eine Dropdown-Liste mit allen erfassten Serverinstanzen im Netzwerk aufgedeckt. Der Standardwert bei der Verwendung einer Instanz von SQL-Server-Express ist **.\GDATA2014**. Ist der richtige Server ausgewählt, kann die Authentisierungsmethode unter AUTHENTISIERUNG definiert werden. Standardmäßig nutzt der ManagementServer die Methode WINDOWS-AUTHENTISIERUNG und meldet sich mit einem lokalen Systemkonto an. Es kann jedes Windows-(Domänen-)Konto mit den entsprechenden Berechtigungen auf dem Datenbankserver genutzt werden. Alternativ können mithilfe der Listenoption SQL SERVER-AUTHENTISIERUNG die Anmeldedaten eingegeben werden.

Wenn Datenbankserver und Authentifizierung konfiguriert worden sind, kann durch Klicken auf das Dropdown-Menü DATENBANK eine Liste der verfügbaren Datenbanken vom Server angefordert werden. Bei

Verwendung der Standardkonfiguration von SQL-Server-Express speichert der ManagementServer seine Daten in der Datenbank **GData_AntiVirus_MMS**. Wenn eine andere vorhandene ManagementServer-Datenbank verwendet werden soll, muss diese aus der Liste ausgewählt werden. Eine leere ManagementServer Datenbank wird einfach durch Angabe eines Namens im Textfeld erstellt. Um zu überprüfen, ob der ManagementServer eine Verbindung mit seiner Datenbank herstellen kann, kann die Option ÜBERPRÜFEN verwendet werden. In einem Upgrade-Szenario muss das Datenbank-Layout möglicherweise aktualisiert werden, um mit der neuesten Version vom ManagementServer kompatibel zu sein. Sie wird automatisch durch Klicken auf ÜBERNEHMEN aktualisiert.

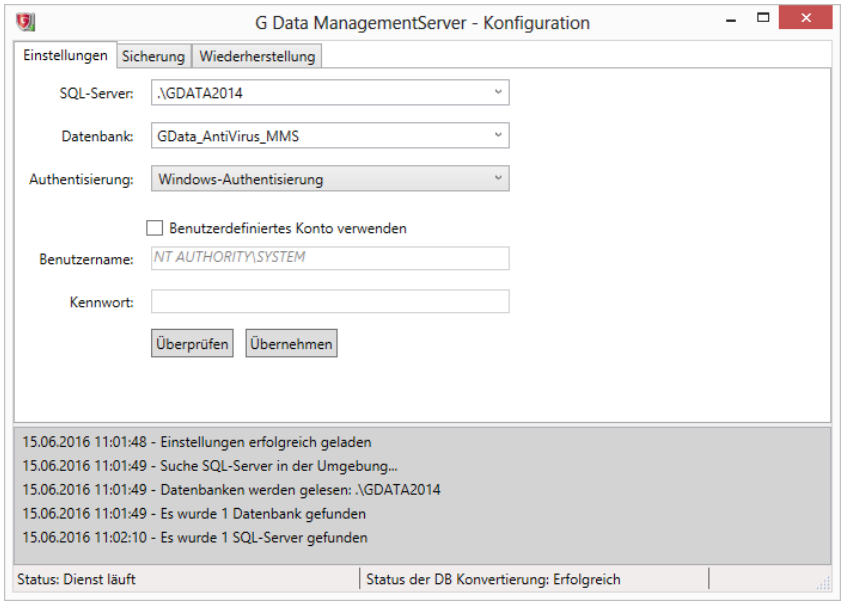

Abbildung 72: GdmmsConfig.exe

Bei der Installation des ManagementServers für eine vorhandene Datenbankinstanz (siehe Abschnitt 4.2.1) müssen die Datenbankeinstellungen während der Installation eingegeben werden. Müssen danach Einstellungen angepasst werden, steht GdmmsConfig.exe hierzu nach der Installation zur Verfügung. Mithilfe des Tools können die passende Instanz und Datenbank vom SQL Server (Express) ausgewählt werden. Wenn der ManagementServer auf einem Computer neu installiert wurde, auf dem eine Instanz von SQL Server Express mit einer ManagementServer-Datenbank vorhanden ist, sollten die Standardeinstellungen korrekt sein. Wenn der ManagementServer eine Instanz vom SQL Server auf einem anderen Server nutzen soll, werden die Server- und Anmeldedaten eingegeben und das Dropdown-Menü DATENBANK genutzt, um eine Liste der Datenbanken anzufordern und die Datenbank aus der Liste auszuwählen.

GdmmsConfig.exe kann auch für eine Datenbankmigration verwendet werden. Für Installationen mit bis zu eintausend Clients bringt eine lokale Installation vom SQL Server Express eine gute Leistung (je nach Hardware-Konfiguration). Wenn der ManagementServer eintausend Clients erreicht, kann es für eine anhaltende Leistungsfähigkeit notwendig sein, die Datenbank auf einem eigenen Server zu migrieren. Mit GdmmsConfig.exe ist dieser Prozess relativ einfach. Dazu müssen mithilfe der aktuellen Datenbankzugriffsdaten ein Datenbank-Backup erstellt, die Daten des neuen Servers eingegeben und die Datenbank auf dem neuen Server wiederhergestellt werden (siehe Abschnitt 4.7).

18.2. Datenbankvoraussetzungen

Bei der Installation kann der G DATA ManagementServer so konfiguriert werden, dass er entweder einen lokalen Microsoft SQL-Server-Express oder einen vorhandenen Microsoft SQL-Server verwendet. In beiden Fällen wird automatisch eine Datenbank erstellt und konfiguriert (siehe Abschnitt 4.2.1). Bei Verwendung eines vorhandenen SQL-Servers ist mindestens ein Microsoft SQL Server 2005 erforderlich.

Treten bei der Verwendung eines vorhandenen SQL-Servers Probleme auf, sollte sichergestellt werden, dass die Kollationseinstellungen für die Datenbank unversehrt sind. Bei der Installation wird die Datenbank für den ManagementServer mit der Einstellung KOLLATION gleich **Latin1_General_CI_AS** erstellt. Dies kann mithilfe von Microsoft SQL Server Management Studio in den Eigenschaften der Datenbank überprüft werden. Außerdem arbeitet die ManagementServer-Datenbank mit dem Datenbankschema **dbo**. Wurde die Benutzerzuordnung auf dem SQL-Server geändert, sollte das STANDARDSCHEMA von Benutzern der ManagementServer-Datenbank immer noch **dbo** lauten.

18.3. Config.xml

Die komplexesten Einstellungen für den G DATA ManagementServer können in der Konfigurationsdatei Config.xml im Installationsordner des G DATA ManagementServers gespeichert werden, üblicherweise ist dies C:\Programme (x86)\G Data\G DATA AntiVirus ManagementServer. Die Dateien können mit Notepad oder einem anderen textbasierten Editor bearbeitet werden. Beim Bearbeiten der Datei Config.xml muss darauf geachtet werden, dass der Texteditor die Datei nicht mit der Erweiterung .txt speichert. Dazu muss als Dateityp ALLE DATEIEN (*.*) gewählt und sichergestellt werden, dass der Dateiname unverändert bleibt.

Die Struktur der Datei „Config.xml“ wird Administratoren vertraut sein, die bereits Konfigurationsdateien im XML-Stil bearbeitet haben. Die Datei definiert verschiedene Einstellungsgruppen und listet Einstellungen in dieser Gruppe mit dem Tag-Paar <setting></setting>. Jede Einstellung hat einen Namen, einen Typ und einen Wert, die als Attribute im Tag <setting> definiert sind. Die Werte sind typischerweise ganze Zahlen, boolesche Werte (true/false), Zeichenfolgen oder TimeSpan-Werte. In der Tabelle in diesem Abschnitt sind der Name der Einstellung und die zugehörigen möglichen Werte aufgeführt. Der Name der Einstellung sollte niemals bearbeitet werden. Es wird nur der Wert auf die gewünschte Einstellung geändert.

```
<?xml version="1.0" encoding="utf-8"?>
<config>
        <group name="Database">
                <setting name="DbServer" type="string" value=".\GDATA2014" />
                ...
        </group>
</config>
```

Abbildung 73: Config.xml

Die verschiedenen Einstellungen von Config.xml sind nach Thema gruppiert. In der folgenden Tabelle sind die verschiedenen Gruppen und ihre wichtigsten Einstellungen aufgeführt:

Gruppe	Einstellung	Standard	Beschreibung
Datenbank			

Konfiguration der ManagementServer Datenbank. Diese Einstellungen sollten über GdmmsConfig.exe konfiguriert werden (siehe Abschnitt 18.1).

DbServer	.\GDATA2014	Die Instanz der Datenbank.
Database	GData_AntiVirus_MMS	Der Name der Datenbank.
DbUser	<leer>	Der Benutzername der Datenbank.
DbPassword	<leer>	Das Kennwort der Datenbank.
UseSQLWindowsAuth	True	Der Authentisierungstyp.

Kultur

Regionsspezifische Einstellungen.

EmailCodePage	<leer>	Codeseite für ausgehende E-Mails. Wenn hier keine Codeseite definiert ist, wird UTF-8 verwendet.

P2P

Einstellungen für Peer-to-Peer-Updateverteilung (siehe Abschnitt 7.3). Deshalb wurden manche Parameter deaktiviert, um zu verhindern, dass Clients fälschlicherweise als außerhalb der Nachbarschaft eines anderen Clients erkannt werden (DHCP-Server, Standard- und Teilnetz). Bei der Verwendung eines Nur-IPv4- oder Nur-IPv6-Netzwerks können diese Parameter manuell aktiviert werden, um die Auswahl der aktualisierten Clients zu verbessern, die Dateien verteilen können. Wenn eine der Einstellungen für die Peer-to-Peer-Verteilung aktualisiert wird, müssen die Änderungen durch Bearbeitung eines Registry-Schlüssels bestätigt werden, bevor der Dienst „ManagementServer“ neu gestartet wird. Dazu wird mithilfe des Registrierungs-Editors der Wert DoNotConsiderP2PConfigToDB aus dem Schlüssel „HKEY_LOCAL_MACHINE\Software\G DATA\AVK ManagementServer“ entfernt (bei Verwendung eines 64-Bit-Systems befindet sich der Schlüssel unter Software\Wow6432Node\G DATA). Dies zwingt den ManagementServer dazu, die Konfigurationswerte für die Peer-to-Peer-Updateverteilung aus Config.xml zu importieren.

P2PMaxNumberOfHops	1	Maximale Anzahl der Hops zwischen zwei Clients, damit gilt, dass sie sich in der Nachbarschaft des jeweils anderen befinden.
P2PConnectRetries	3	Maximale Anzahl der Verbindungsneuversuche, bevor ein Client eine Verbindungsanforderung an einen anderen Peer weiterleitet.
P2PClientMaxServedPeers	5	Maximale Anzahl der Clients, die gleichzeitig von einem Peer versorgt werden.
P2PClientAbandonedConnectionThresholdMin	1	Maximale Zeitspanne der Inaktivität, bevor eine Verbindung als abgebrochen gilt (auf der Client-Seite).
P2PConsiderClientsOnBattery	False	Clients, die mit Batterieleistung laufen, werden als Quelle für Updates ausgeschlossen.
P2PConsiderClientsLastAccess	True	Während der Bestimmung eines Clients als Quelle für ein Update wird der letzte Zugriff des Clients berücksichtigt.
P2PConsiderClientsSubnet	False	Clients befinden sich in der Nachbarschaft eines anderen, wenn beide aus demselben Teilnetz stammen.
P2PConsiderClientsDomain	True	Clients befinden sich in der Nachbarschaft eines anderen, wenn beide dieselbe Domäne besitzen.

P2PConsiderClients DHCP	False	Clients befinden sich in der Nachbarschaft eines anderen, wenn beide ihre dynamischen IP-Adressen vom selben DHCP-Server beziehen.
P2PConsiderClients Gateway	False	Clients befinden sich in der Nachbarschaft eines anderen, wenn beide denselben Standard-Gateway nutzen.
P2PMmsMaxServed Peers	50	Maximale Anzahl der gleichzeitigen Client-Verbindungen, die vom ManagementServer bedient werden (Verbindungen, über die ein Signatur-/Programm-Update heruntergeladen wird).
P2PMmsAbandonedConnectionThresholdMin	1	Maximale Zeitspanne der Inaktivität, bevor eine Verbindung als abgebrochen gilt (auf der ManagementServer-Seite).
P2PDisablePGM UpdateDistribution	False	Aktiviert oder deaktiviert die Peer-to-Peer-Verteilung von Programmdatei-Updates. (Bei Deaktivierung werden nur Signatur-Updates per Peer-to-Peer verteilt.)

Programupdate

Einstellungen für die stufenweise Update-Verteilung (siehe Abschnitt 7.3.2). Viele Teile der Berechnung lassen sich perfekt an die jeweiligen Umstände in jedem Unternehmensnetzwerk anpassen. Für verschiedene Einstellungen wurden Standardwerte für die ersten sechs Stufen definiert. Wenn mehr Stufen verwendet werden, können der Konfigurationsdatei zusätzliche Werte hinzugefügt werden. Wenn es mehr Stufen als Werte für eine bestimmte Einstellung gibt, werden die nächsten Werte aus dem Bereich extrapoliert.

SPUEnable	3	Bitmaske für zwei Einstellungen im Fenster Updates > Stufenweise Verteilung des G DATA Administrators: Automatische Programm-Updates stufenweise verteilen (1) und Clients für die erste Stufe automatisch zuordnen (2).
SPUStopAbsolute	5,15,20,30,40,50	Die Anzahl der fehlerhaften Clients pro Stufe, bei der die stufenweise Softwareverteilung angehalten werden soll (absolute Zahl). Verwendet, wenn kleiner als SPUStopPromille.
SPUStopPromille	25,75,100,150,200,250	Die Anzahl der fehlerhaften Clients pro Stufe, bei der die stufenweise Softwareverteilung angehalten werden soll (pro Tausend). Verwendet, wenn kleiner als SPUStopAbsolute.
SPUStepsTimespan	3.00:00:00 (3 Tage)	dd.hh:mm:ss. Zeitspanne bis zur Freigabe der folgenden Stufe. Entspricht der Einstellung „Nächste Gruppe freigeben nach“ im G DATA Administrator.
SPUZombieTimespan	14.00:00:00 (14 Tage)	dd.hh:mm:ss. Clients, die in einer bestimmten Zeitspanne keine Verbindung mit dem ManagementServer hergestellt haben, werden in der mathematischen Berechnung, die die stufenweise Softwareverteilung regelt, nicht mitgerechnet.

SPUFirstStepLimit	5,20	Minimale und maximale Anzahl der Clients, die in die erste Stufe aufgenommen werden sollen.
SPUTotalSteps	3	Anzahl der Stufen. Entspricht der Einstellung ANZAHL DER GRUPPEN im G DATA Administrator.
SPUSyncTimespan	00:30:00 (30 Minuten)	dd.hh:mm:ss. Synchronisation des Status der stufenweisen Softwareverteilung zwischen Clients, Subnet-Servern und ManagementServer.
SPUMinClients	10	Minimale Anzahl der Clients im Netzwerk, die erforderlich sind, damit die stufenweise Softwareverteilung anläuft.

Ordner

Speicherorte für Dateien verschiedener ManagementServer Komponenten. Bei der Neudefinition von Ordnern sollten die in diesen Ordnern vorhandenen Dateien in den neuen Ordner verschoben werden, bevor der Dienst „ManagementServer“ neu gestartet wird.

LogFileFolder	<Ordner>	Protokolldateien werden standardmäßig unter %ProgramData%\G DATA\AntiVirus ManagementServer\Log gespeichert.
QuarantineFolder	<Ordner>	In Quarantäne verschobene Dateien werden standardmäßig unter %ProgramData\G DATA\AntiVirus ManagementServer\Quarantine gespeichert.
UpdateDistribution Folder	<Ordner>	Virensignatur- und Programmdatei-Updates werden standardmäßig unter %ProgramData\G DATA\AntiVirus ManagementServer\Updates gespeichert. Dieser Wert wird bei jedem Start des ManagementServer mit der IUpdateCfg.xml-Datei synchronisiert.
InternetUpdatePgm Folder	<Ordner>	Der Ordner, in dem die Internet-Update-Komponente (IUpdate.exe) gespeichert wird, standardmäßig C:\Programme (x86)\G Data\G DATA AntiVirus ManagementServer. Dieser Wert sollte nicht geändert werden.
BackupFolders	<Ordner>	Backups werden standardmäßig unter %ProgramData%\G Data\AntiVirus ManagementServer\Backup gespeichert. Wird ignoriert, wenn im G DATA Administrator Pfade für Server-Backups definiert wurden (siehe Abschnitt 12.1).
DBBackupFolder	<leer>	Der zuletzt verwendete Datenbank-Backup-Ordner in GdmmsConfig.exe. Die Ordnereinstellung sollte nur über die Benutzeroberfläche von GdmmsConfig.exe geändert werden.
PatchFilesFolder	<Ordner>	PatchManager-Dateien werden standardmäßig unter %ProgramData%\G Data\AntiVirus ManagementServer\Patches gespeichert.

InstallPackagesFolder	<Ordner>	Client-Installationspakete (Windows) werden in diesem Ordner gespeichert, wenn sie mit dem Tool Gdata.Business.Server.Cli.exe angelegt wurden.
InstallScriptsFolder	<Ordner>	Client-Installationsskripte (Linux/Mac) werden in diesem Ordner gespeichert, wenn sie mit dem Tool Gdata.Business.Server.Cli.exe angelegt wurden.

Server

Einstellungen, die bestimmen, ob der ManagementServer als Haupt-, Sekundär- oder Subnet-Server ausgeführt wird. Die möglichen Werte für MainMms, SubnetMms und IsSecondaryMMS sind in der Datei Config.xml hinterlegt.

Patch

Einstellungen des PatchManagers.

UpdateClientPatch ServerLog	0	Bitmaske für die Art der Einträge im Patchverwaltungsprotokoll, die unter Server > Infrastruktur-Logs in G DATA Administrator angezeigt werden: Keine (0); Softwareerkennungsaufträge (1); Softwareverteilungsaufträge (2).
AutoPatchJobsBatch SizeDaily	5000	Anzahl der automatischen Patch-Aufträge, die gleichzeitig an einem Tag existieren können
AutoPatchJobsBatch SizeNightly	10000	Anzahl der automatischen Patch-Aufträge, die gleichzeitig in der Nacht existieren können

Netzwerk

Einstellungen des Netzwerks. Wird der Wert für den ClientHttpPort oder den ClientHttpsPort geändert, muss die HTTPS-Sicherheitskonfiguration für den Port erneut initialisiert werden. Dazu wird die Eingabeaufforderung mit Administratorrechten geöffnet und *C:\Programme (x86)\G Data\G DATA AntiVirus ManagementServer\gdmmsconfig.exe /installcert* ausgeführt. Nach dem Ändern der Ports muss der Dienst G DATA ManagementServer neu gestartet werden. Hierbei gilt, dass nach dem Ändern des Werts für AdminPort der Server beim Anmelden beim G DATA Administrator ausdrücklich im Format *servername:port* definiert werden muss.

DisableActiveDirectory Search	False	Synchronisation von Active Directory deaktivieren
AdminPort	0	Port für TCP-Kommunikation mit dem G DATA Administrator. Es kann eine beliebige Portnummer eingegeben werden. Mit dem Wert 0 wird der Port auf die Standardnummer 7182 eingestellt.
ClientHttpPort	80	Port für TCP-Kommunikation mit Android-Clients (Verteilung von Installationsdateien). Es kann eine beliebige Portnummer eingegeben werden.
ClientHttpsPort	443	Port für TCP-Kommunikation mit Android-Clients. ClientHttpsPort sollte nicht verändert werden, da Android-Clients keinen alternativen Port akzeptieren. Es kann eine beliebige Portnummer eingegeben werden.

Allgemein

Verschiedene Einstellungen.

MaxUpdateThreads	300	Die maximale Anzahl der Clients, die gleichzeitig eine Verbindung mit dem ManagementServer herstellen können.
MaxSubnetUpdate Threads	100	Die maximale Anzahl der Subnet-Server, die zwecks Update oder Synchronisation gleichzeitig eine Verbindung mit dem ManagementServer herstellen können.
PerformStartupDB CheckAndRepair	True	Entfernt beim Starten des Dienstes „ManagementServer“ überflüssige Datenbankeinträge.
DisplayLicenseLimit	True	Die Anzahl der zulässigen Lizenzen und das Lizenzablaufdatum werden im Modul LIZENZÜBERSICHT angezeigt.
MaxParallelClient Installation	5	Die maximale Anzahl der Clients, die gleichzeitig per Fernzugriff installiert werden können. Große Zahlen können zu einer Überlastung des Netzwerks führen. Minimal 5, maximal 1000.
UseAsyncAwait	True	Asynchrone Verarbeitung für eingehende Verbindungen aktivieren. Erfordert Microsoft .NET Framework 4 mit Update KB2468871.
SyncReportDays	90	Maximales Alter (in Tagen) der Berichte, die zwischen ManagementServer und Subnet-Server synchronisiert werden.
SyncNumberOfRows PerBatch	200	Anzahl der Datenbankzeilen pro Batch, die zwischen ManagementServer und Subnet-Server synchronisiert werden sollen (beeinflusst die Leistung und sollte nicht unter 100 liegen).
SoftwareInventory Enabled	True	Synchronisation der Daten des Client-Softwareinventars vom Subnet-Server zum Haupt-ManagementServer. Wenn eine sehr große Anzahl von Subnet-Servern verwendet wird, könnte sich dies auf die Netzwerkleistung auswirken. Die Funktion kann deaktiviert werden.
QueryPageSize	10000	Leistung bei der Abfrage großer Datenbanken. Eine hohe Zahl verlängert die anfängliche Wartezeit, verkürzt aber die Gesamtwartezeit. Durch Verringerung der Zahl wird die anfängliche Wartezeit verkürzt, aber die Gesamtwartezeit verlängert.

18.4. G DATA Exchange Mail Security

Die Exchange Mail Security schützt E-Mails nicht nur bei Erhalt und Versand, sondern auch, wenn sie erstellt, geändert, kopiert und verschoben werden. Bei der Verwendung vom Microsoft Exchange Server 2013 SP1 und höher stellt die Exchange Mail Security die Verbindung zu Postfächern mithilfe des Push-Benachrichtigungssystems vom Exchange her, um den letztgenannten Schutz zu leisten. Zur

Optimierung der Leistung des Push-Benachrichtigungssystems und seiner Proxy-Einstellungen können mehrere Parameter konfiguriert werden.

18.4.1. Leistung der Push-Benachrichtigungen

Bei jedem Start des Hintergrunddienstes der Exchange Mail Security abonniert dieser jedes einzelne Exchange-Postfach. Je nach Anzahl der Postfächer auf dem Server kann die Dauer dieses Prozesses zwischen wenigen Sekunden und bis zu einer Stunde liegen. Während die Exchange Mail Security Postfächer abonniert, wird kein Schutz für E-Mails bereitgestellt, die in diesem Postfach angelegt oder geändert bzw. zwischen Postfächern kopiert oder verschoben werden. Allerdings werden diese E-Mails bei Versand bzw. Erhalt gescannt.

Die Leistung der Push-Benachrichtigung kann in einer Umgebung mit vielen öffentlichen Postfächern optimiert werden, damit neu erstellte E-Mails NACH DEM Start des Hintergrunddienstes schneller geschützt werden. Diese Einstellungen lassen sich mithilfe des Registrierungs-Editors bearbeiten. Folgende Werte befinden sich im Schlüssel „HKEY_LOCAL_MACHINE\Software\G DATA\Exchange“ und können erstellt werden, wenn sie noch nicht existieren:

Wert	Typ	Wertdaten	Beschreibung
DefaultConnectionLimit	DWORD (32 Bit)	15 (dezimal)	Die Anzahl der gleichzeitigen Anforderungen eines Abonnements von Push-Benachrichtigungen, die Exchange Mail Security einleiten kann. Bei Erhöhung dieser Zahl wird der Abonnementprozess beschleunigt. Es kann jedoch zu Problemen mit der Stabilität und Zuverlässigkeit von Exchange kommen.
DefaultSubscribeDelay	DWORD (32 Bit)	65 (dezimal)	Die Anzahl der Millisekunden zwischen Anforderungen eines Abonnements von Push-Benachrichtigungen. Bei Verringerung dieser Zahl wird der Abonnementprozess beschleunigt. Es kann jedoch zu Problemen mit der Stabilität und Zuverlässigkeit von Exchange kommen.
PushNotificationLimit	DWORD (32 Bit)	10000 (dezimal)	Das Maximum an öffentlichen Ordnern, für die Push-Benachrichtigungen ausgeführt werden sollten. Liegt die tatsächliche Zahl höher, werden keinerlei Push-Benachrichtigungen zugestellt. Der Wert kann auch -1 (Push-Benachrichtigung immer aktiviert) oder 0 (Push-Benachrichtigung immer deaktiviert) lauten.

18.4.2. Proxy-Bypass für Push-Benachrichtigungen

In Netzwerken, die einen Proxy-Server nutzen, werden die Push-Benachrichtigungen vom Microsoft Exchange Server an den Proxy-Server und nicht direkt an die Exchange Mail Security geschickt. Der Exchange kann so konfiguriert werden, dass es den Proxy-Server umgeht und Push-Benachrichtigungen direkt an die Exchange Mail Security schickt. Diese Einstellung lässt sich in der entsprechenden Konfigurationsdatei für Microsoft .NET Framework (web.config) auf dem betroffenen Server aktivieren.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    ...
    <system.net>
```

```
        <defaultProxy>
            <proxy usesystemdefault="true" bypassonlocal="true" />
                <bypasslist>
                    <add address="exchangeserver.domain.com" />
                </bypasslist>
        </defaultProxy>
    </system.net>
    ...
```

Abbildung 74: web.config

„web.config“ ist eine XML-Datei mit einer kaskadierten Struktur ähnlich wie Config.xml. Alle Einstellungen sind vom Tag-Paar <configuration> </configuration> umschlossen. Standardmäßig existiert der Knoten <system.net> bereits. Um die Einstellungen in der obigen Abbildung wiederzugeben, müssen die Werte <defaultProxy> geändert und die Adresse **exchangeserver.domain.com** durch die Adresse des Exchange-Servers ersetzt werden. Anforderungen an diesen Server werden den Proxy-Server nun umgehen.

18.5. Client-basierte Tools

Es stehen verschiedene Tools zur Verfügung, mit denen sich die Software von G DATA noch feiner abstimmen lässt. Ebenso wie die erweiterten Konfigurationsdateien müssen auch die Software-Tools mit Vorsicht genutzt werden. Vor einer Änderung der Konfiguration sollte ein Backup aller betroffenen Dateien und Ordner erstellt werden. Außerdem wird davon abgeraten, auf einem aktiven Netzwerk oder Netzwerk-Client zu experimentieren. Vor der Installation von Änderungen durch ein Konfigurationstool sollten seine Auswirkungen auf einem (virtuellen) Testnetzwerk oder -Client getestet werden.

18.5.1. Aktivität des Dateisystemwächters

Der Dateisystemwächter ist eine der umfassendsten Komponenten der Sicherheitslösung von G DATA. Er erkennt eine große Menge an Malware, braucht dazu jedoch beträchtliche Systemressourcen. Wenn die Client-Leistung deutlich beeinträchtigt ist, kann das Tool „MonActivityCS“ (Wächteraktivität) herausfinden, ob der Dateisystemwächter Probleme mit einer bestimmten Datei hat. Das Tool kann von https://secure.gd/ukdls und ohne Extrahierung oder Ausführung eines Installationsassistenten direkt ausgeführt werden. Das Tool lässt sich in zwei Modi ausführen: Echtzeit oder Hitliste. Im Echtzeitmodus werden die Dateien aufgeführt, sowie sie vom Dateisystemwächter überprüft werden. Das ist praktisch, wenn sich das Problem mit dem Dateisystemwächter leicht reproduzieren lässt. Die Trefferliste zeigt, wie oft bestimmte Dateien überprüft wurden, was dabei hilft, problematische Dateien herauszustellen.

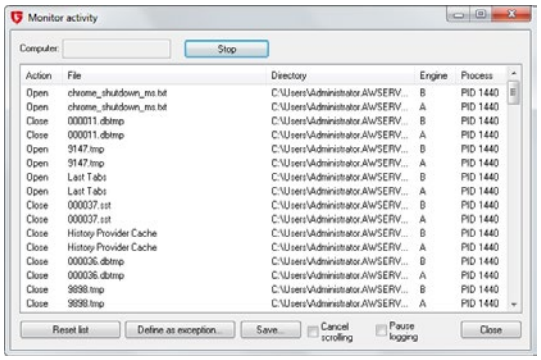

Abbildung 75: MonActivityCS (Wächteraktivität)

Wenn der Modus ausgewählt ist, erscheint das Hauptfenster der Wächteraktivität. Zum Starten der Überwachung auf dem lokalen Computer dient die Option VERBINDEN (das Textfeld COMPUTER kann leer bleiben). Durch Klick auf STOPPEN wird die Überwachung angehalten. Die Liste wird befüllt, wenn das Tool läuft. Durch Klicken auf AKTUALISIEREN wird die Liste manuell aktualisiert (im Modus HITLISTE). Mithilfe der Option LISTE ZURÜCKSETZEN wird die Liste zurückgesetzt (im Modus ECHTZEIT), und mithilfe von SPEICHERN wird die Dateiliste als Textdatei gespeichert. Mithilfe der Option ALS AUSNAHME DEFINIEREN kann eine Datei sofort als Ausnahme für die Dateisystemüberwachung definiert werden.

18.5.2. Quarantäne

Wenn eine der Sicherheitsebenen von G DATA eine Bedrohung erkennt, werden automatisch die notwendigen Schritte ergriffen. Wenn der Administrator definiert hat, dass die Dateien in Quarantäne gebracht werden sollen, werden sie umbenannt und in einen sicheren Ordner verschoben. Mit dem Modul SICHERHEITSEREIGNISSE vom G DATA Administrator können die Dateien dann analysiert, gesäubert und wieder zurückverschoben werden. Für die lokale Handhabung der Quarantäne eines Clients kann das Tool „Quarantine“ genutzt werden. Es kann unter https://secure.gd/ukdls (Quarantine Generation 2011) heruntergeladen und sollte auf dem betroffenen Client ausgeführt werden. Das Tool kann ebenfalls für die Überprüfung von Dateien genutzt werden, die sich im Quarantäneordner des Servers befinden, falls eine Analyse durch den G DATA Administrator nicht möglich ist.

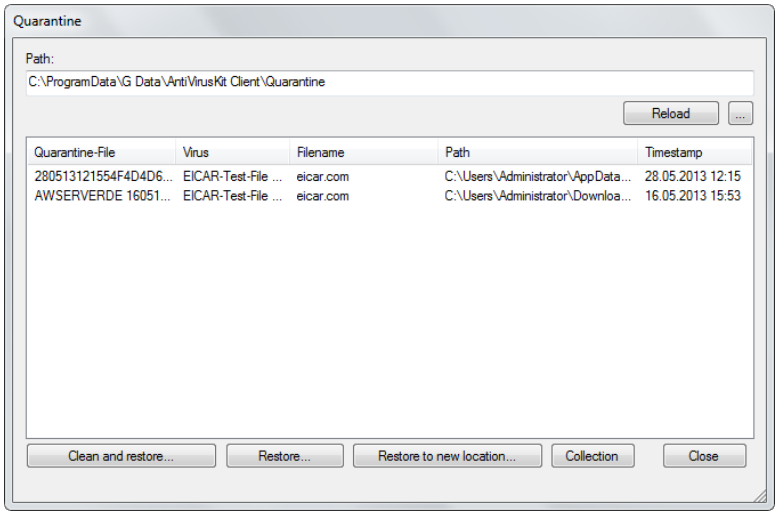

Abbildung 76: Quarantine

Nach seinem Start zeigt das Modul „Quarantine“ sofort die lokale Quarantäne an. Es nutzt den standardmäßigen Quarantänepfad und führt alle Dateien zusammen mit einigen Metadaten auf. Wenn es nicht automatisch den richtigen Ordner wählt, kann dieser manuell eingestellt werden. Standardmäßig werden die Client-Quarantänedateien unter %ProgramData%\G Data\AntiVirusKit Client\Quarantine gespeichert. Bei der Untersuchung der Server-Quarantäne lautet der Standardordner %ProgramData%\G Data\AntiVirus ManagementServer\Quarantine, falls in Config.xml kein anderer Pfad angegeben wurde (siehe Abschnitt 18.2).

Bei der Auswahl einer Datei in Quarantäne stehen mehrere Optionen zur Verfügung. Die empfohlene Option ist SÄUBERN UND ZURÜCKBEWEGEN. Dadurch wird versucht, die Malware aus der Datei zu entfernen und diese an ihrem ursprünglichen Speicherort wiederherzustellen. Andere Optionen sind die

Wiederherstellung der Datei an ihrem ursprünglichen Speicherort ohne Säuberung und die Wiederherstellung der Datei an einem neuen Speicherort ohne Säuberung. Beide Optionen sind nicht empfehlenswert: Die Malware ist immer noch in der Datei vorhanden und stellt ein Risiko dar. Wenn eine Datei nicht gesäubert werden kann, muss sie möglicherweise gelöscht werden. Dazu muss der Quarantine-Ordner in Windows Explorer geöffnet und die zugehörige .q-Datei gelöscht werden.

18.6. Protokollierung

Zur Erweiterung der Konfiguration und zur Problembehandlung kann es hilfreich sein, die Protokolle zu untersuchen. Viele der Client-seitigen Sicherheitsmodule erstellen eigene Protokolle, die im G DATA Administrator gelesen werden können: z. B. Virenscans, Backup-Aufträge oder Wiederherstellungsaufträge. Mithilfe mehrerer konfigurierbarer Protokolle ist eine zusätzliche Auswertung möglich. Die inneren Mechanismen der meisten Sicherheitsmodule können mit diesen Dateien analysiert werden. Verhält sich ein Teil der Software unerwartet, liefert das Protokoll wertvolle Einblicke. Erhält ein Client keine aktualisierten Einstellungen, verursacht ein Subnet-Server Probleme oder beansprucht der ManagementServer außergewöhnlich große Anteile der RAM- oder CPU-Zyklen, kann das Protokoll einen Hinweis darauf geben, welche Art von Problemen aufgetreten ist. Auch wenn eine direkte Analyse nicht möglich ist, können die Protokolldateien unserer Supportabteilung bei der Untersuchung des Problems helfen.

18.6.1. (De)installation

Der Installationsassistent des G DATA ManagementServers, G DATA Administrators, G DATA WebAdministrators, G DATA MobileAdministrators, G DATA Security Clients, G DATA Bootmedium Wizards und der G DATA Exchange Mail Security hilft dem Administrator mit entsprechenden Hinweisen am Bildschirm, die Software ohne Probleme zu installieren. Falls nach Abschluss des Installationsassistenten einzelne Komponenten Probleme verursachen oder gar nicht ausgeführt werden, sollte überprüft werden, ob der Assistent alle Komponenten richtig installiert hat oder ob Ausnahmen auftreten. Protokolldateien für alle Setup-Vorgänge (Installation, Deinstallation, Update) sind unter %ProgramData%\G Data\Setups\Logs gespeichert. Während des Setups wird der Fortschritt in einer Protokolldatei mit dem Namen der Komponente und einem Zeitstempel protokolliert. Nach Abschluss oder Abbruch des Setups wird die Protokolldatei als Zip-Datei mit der gleichen Dateinamenstruktur komprimiert.

Die Installation vom G DATA Security Client für Linux wird lokal unter /var/log/gdata_install.log protokolliert. Bei einer Installation per Fernzugriff wird die Protokolldatei auch im Fenster INSTALLATIONSÜBERSICHT des G DATA Administrators angezeigt.

18.6.2. ManagementServer

Protokolldateien für den ManagementServer werden automatisch erstellt. Der Protokollordner befindet sich standardmäßig unter %ProgramData%\G DATA\AntiVirus ManagementServer\Log. Die Protokolldateien sind mit einem Zeitstempel versehen und kategorisiert:

- Gdmms.log: Alle Debug-Meldungen des ManagementServers.
- GdmmsError.log: Fehler des ManagementServers.

- Startup\GdmmsStart.log: Datenbankanalyse des ManagementServer Starts.

Alte Protokolldateien werden im Unterordner \Archive aufbewahrt (maximal 99 Dateien).

18.6.3. Security Client und MailSecurity MailGateway

Der Security Client und das MailSecurity MailGateway können mit dem von Sysinternals entwickelten Tool „DebugView“ analysiert werden. In Kombination mit der Festlegung eines Registry-Schlüssels für das Modul, das man debuggen möchte, generiert DebugView umfangreiche Protokolle.

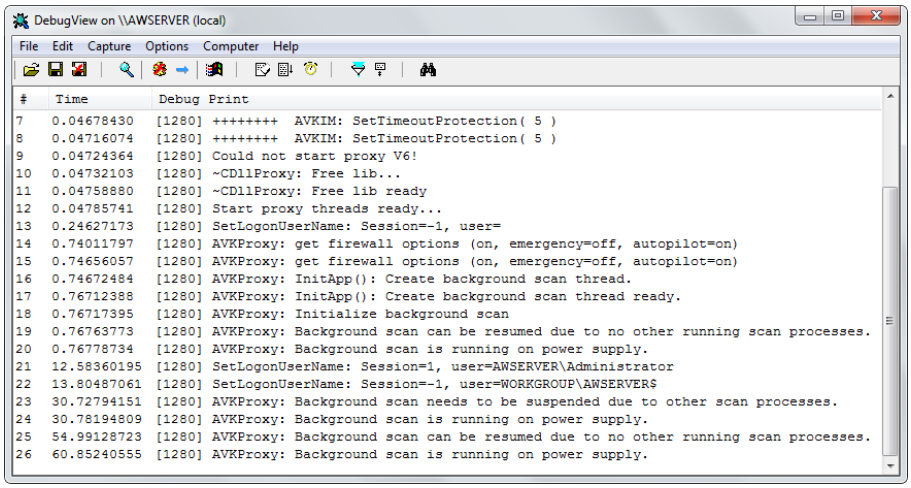

Abbildung 77: DebugView

Dazu werden mithilfe des Registrierungs-Editors folgenden Schlüsseln folgende DWORD-Werte mit dem Wert **7** hinzugefügt, um das Debuggen für die entsprechenden Module zu ermöglichen:

Modul	**Schlüssel**[22]	**DWORD-Wert**
MailSecurity MailGateway	HKEY_LOCAL_MACHINE\Software\G DATA\AVKSmtp	DebugLevel
Security Client (allgemein)	HKEY_LOCAL_MACHINE\Software\G DATA\AVKClient	DebugLevel
Datenverkehr-Scans	HKEY_LOCAL_MACHINE\Software\G DATA\AVKProxy	DebugLevel
Updates	HKEY_LOCAL_MACHINE\Software\G DATA\InternetUpdate	IUpdateDebugLevel
Virenscans	HKEY_LOCAL_MACHINE\Software\G DATA\AVKScanP	DebugLevel

Nach der Registry-Änderung muss der Computer neu gestartet und das Tool DebugView unter http://technet.microsoft.com/en-us/sysinternals/bb896647 heruntergeladen werden. Nach dem Herunterladen der Datei wird sie extrahiert, und DebugView.exe wird mit Administratorberechtigungen ausgeführt. Aktiviere unter ERFASSEN die Option GLOBAL WIN32 ERFASSEN. Bei der Ausführung von DebugView erfasst es die Debug-Ausgabe der Module, für die der Registry-Schlüssel „DebugLevel“ festgelegt wurde. Das Fenster „DebugView“ zeigt die gesamte Ausgabe an, die sich in einer Textdatei speichern lässt. Bei der Verwendung von DebugView zur Untersuchung eines Fehlers wird es ausgeführt, bis der Fehler reproduziert werden kann. Anschließend wird das Protokoll gespeichert. Das Protokoll kann

[22] Bei 64-Bit-Systemen befindet sich der Schlüssel von G DATA in HKEY_LOCAL_MACHINE\Software\Wow6432Node\G DATA.

anschließend für weitere manuelle Analysen verwendet oder an unsere Supportmitarbeiter geschickt werden.

Eine Ausnahme der allgemeinen Debug-Anweisungen ist die Gerätekontrolle (eines der Module vom PolicyManager). Da die Gerätekontrolle einen in die Tiefe gehenden Zugriff auf die Geräteeinstellungen von Windows erfordert, sind zusätzliche Registry-Einstellungen notwendig, um das Debuggen zu ermöglichen. Dazu muss im Registrierungs-Editor zum Schlüssel HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\GDDevCtrl navigiert bzw. der Schlüssel angelegt werden, falls er noch nicht existiert. Anschließend wird der DWORD-Wert **DebugLevel** mit dem Wert **7** hinzugefügt. Daraufhin wird zum Schlüssel „HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Debug Print Filter“ navigiert bzw. wird dieser angelegt, falls er noch nicht existiert. Es werden zwei neue DWORD-Werte hinzugefügt: **Default** mit den Daten **ffffffff** (hexadezimal) und **IHVDRIVER** mit den Daten **ffffffff** (hexadezimal). Nun wird DebugView als Administrator gestartet und die Option WAGENRÜCKLAUF ERZWINGEN unter OPTIONEN und KERNEL ERFASSEN sowie AUSFÜHRLICHE KERNELAUSGABE AKTIVIEREN unter ERFASSEN aktiviert. Anschließend werden der Client und DebugView neu gestartet. Dadurch wird das Debuggen für die Gerätekontrolle aktiviert und es werden relevante Protokolle geliefert, wenn das Problem erneut auftritt.

18.6.4. Security Client für Linux

Während seiner Laufzeit protokolliert der G DATA Security Client für Linux Debug-Informationen in verschiedenen Protokolldateien. Die Protokolldateien befinden sich im Ordner /var/log/gdata. Die Datei Avclient.log enthält Debug-Informationen vom Daemon „gdavclientd“ (wie etwa Signatur-Updates). Die Debug-Informationen vom gdavserver werden in „Gdavserver.log“ protokolliert. Die Datei Systeminfo.txt enthält Hardware-Informationen, die dem ManagementServer gemeldet werden.

18.7. Deinstallation

Die G DATA Komponenten kann per Fernzugriff oder lokal deinstalliert werden. Bei der Deinstallation per Fernzugriff muss der Administrator nicht physisch an den verwalteten Geräten präsent sein. Dies spart also Zeitaufwand. Manchmal ist ein Gerät jedoch nicht über das Netzwerk erreichbar. In diesem Fall wird alternativ eine lokale Deinstallation durchgeführt.

18.7.1. Deinstallation per Fernzugriff

Der G DATA Security Client kann (unter Windows, Linux und Mac) per Fernzugriff deinstalliert werden, indem der entsprechende Client im Module CLIENTS des G DATA Administrators ausgewählt und die Option G DATA SECURITY CLIENT DEINSTALLIEREN genutzt wird. Bei Verwendung eines oder mehrerer Subnet-Server kann mit der Funktion SERVER > ÜBERSICHT eine Remote-Deinstallation eingeleitet werden.

18.7.2. Lokale Deinstallation

Der G DATA ManagementServer, G DATA Administrator, G DATA WebAdministrator, G DATA MobileAdministrator, G DATA Security Client, G DATA Bootmedium Wizard und die G DATA Exchange Mail Security lassen sich mithilfe des Deinstallationsassistenten (SYSTEMSTEUERUNG > PROGRAMME

HINZUFÜGEN/ENTFERNEN) mühelos lokal deinstallieren. Bietet die Systemsteuerung keinen Shortcut, kann der Deinstallationsassistent auch über die Datei Setup.exe im Ordner der entsprechenden Komponente gestartet werden:

Komponente	Ordner
G DATA ManagementServer	%ProgramData%\G Data\Server
G DATA Administrator	%ProgramData%\G Data\Setups\G DATA ADMINISTRATOR
G DATA WebAdministrator	%ProgramData%\G Data\SLAdmin
G DATA MobileAdministrator	%ProgramData%\G Data\MobileAdmin
G DATA Security Client (Windows)	%ProgramData%\G Data\client
G DATA Exchange Mail Security	%ProgramData%\G Data\Setups\G DATA MAILSECURITYFOR EXCHANGE
G DATA Bootmedium Wizard	%ProgramData%\G Data\Setups\G DATA BOOTMEDIUM

Befindet sich Setup.exe nicht in dem entsprechenden Ordner, kann stattdessen das ursprüngliche G DATA Installationsmedium verwendet werden. Über die Eingabeaufforderung wird das erforderliche Installationsprogramm mit dem Parameter **/@InstallMode="Uninstall"** gestartet, beispielsweise **D:\Setup\SecurityClient\Setup.exe /@InstallMode="Uninstall"**, um mit der Deinstallation des G DATA Security Clients zu beginnen.

Der G DATA Security Client für Linux kann mit dem Skript „gdata_uninstall.sh“ (üblicherweise unter /usr/sbin/gdata_uninstall.sh) lokal deinstalliert werden. Das Skript entfernt alle installierten Pakete, Programmdateien, temporäre Dateien, Konfigurationsdateien und Protokolldateien (außer /var/log/gdata_uninstall.log).

Bei der lokalen Deinstallation einer Komponente werden zugehörige Daten in der ManagementServer-Datenbank nicht automatisch entfernt. Inaktive Subnet-Server müssen unbedingt mit dem Modul SERVER entfernt werden. Inaktive Clients können in der Ansicht CLIENTS gelöscht werden.

Akronyme

AD	Active Directory
API	Programmierschnittstelle
APK	Anwendungspaketdatei (Android)
AV	AntiVirus
BCC	Blindkopie
BIOS	Basic Input/Output System
CC	Kopie
CPU	Prozessor
CVE	Common Vulnerabilities and Exposures
DMZ	Entmilitarisierte Zone (Netzwerk)
DNS	Domain Name System
ERP	Enterprise-Resource-Planning
EULA	Endbenutzer-Lizenzvereinbarung
FTP	File Transfer Protocol
GPS	Global Positioning System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IIS	Microsoft-Internetinformationsdienste
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IT	Informationstechnik
JS	JavaScript
MD5	Message-Digest Algorithm 5
MMS	G DATA ManagementServer
MX	Mail Exchanger (Record)
OE	Organisationseinheit
PC	Personal Computer
POP3	Post Office Protocol Version 3
F&E	Forschung und Entwicklung
RAM	Random-Access Memory
RBL	Realtime-Blacklist
SD	Secure Digital
SIM	Subscriber Identity Module
KMU	Kleine und mittlere Unternehmen
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
SQL	Structured Query Language
SSID	Service Set Identification
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UAC	User Account Control
UDP	User Datagram Protocol
UNC	Uniform Naming Convention
URL	Uniform Resource Locator
UTF-8	Universal Character Set Transformation Format – 8 Bit
VBS	Visual Basic Script
WAN	Wide Area Network
WCF	Windows Communication Foundation
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

Stichwortverzeichnis