Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.2: Ordnungsgemäße IT-Administration

1 Beschreibung

1.1 Einleitung

Die fortlaufende Administration von IT-Systemen und -Komponenten ist für den IT-Betrieb grundlegend. Die Systemadministratoren richten dabei IT-Systeme und Anwendungen ein, beobachten den Betrieb und reagieren mit Maßnahmen, welche die Funktion und die Leistungsfähigkeit der IT-Systeme erhalten. Darüber hinaus passen sie die IT-Systeme an veränderte Bedürfnisse an. Dabei erfüllen Systemadministratoren auch eine Reihe von Aufgaben für die Sicherheit. Sie sorgen nicht nur dafür, dass die IT-Systeme verfügbar bleiben, sondern setzen auch Sicherheitsmaßnahmen um und überprüfen, ob sie wirksam sind. Dazu verfügen sie über sehr weitreichende Berechtigungen, sodass es für die Sicherheit des Informationsverbunds auch sehr wichtig ist, die Systemadministration selbst vor unbefugten Zugriffen abzusichern.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie mit einer ordnungsgemäßen IT-Administration die Sicherheitsanforderungen von IT-Anwendungen, -Systemen und Netzen erfüllt werden.

Mit der Umsetzung dieses Bausteins sorgt die Institution einerseits dafür, dass die für die Sicherheit des Informationsverbunds erforderlichen Tätigkeiten in der Systemadministration ordnungsgemäß und systematisch durchgeführt werden. Andererseits reagiert die Institution damit auch auf die besonderen Gefährdungen, die sich aus dem Umgang mit Administrationsprivilegien und aus dem Zugang zu schützenswerten Bereichen der Institution zwangsläufig ergeben.

1.3 Abgrenzung und Modellierung

Der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* ist auf den gesamten Informationsverbund anzuwenden.

Gegenstand des Bausteins sind übergreifende Anforderungen an den Administrationsprozess als solchen. Bei der Fernadministration von IT-Systemen über externe Schnittstellen sowie bei der Fernwartung von Geräten und Komponenten durch die jeweiligen Hersteller oder Zulieferer ist zusätzlich der Baustein OPS.1.2.5 *Fernwartung* anzuwenden.

Die weiteren Bausteine der Schicht OPS.1.1 *Kern-IT-Betrieb* beschreiben Aspekte des IT-Betriebs, die zusätzlich zum vorliegenden Baustein relevant sind. Sie sollten daher in Ergänzung zu diesem Baustein zusätzlich betrachtet und modelliert werden.

Die ordnungsgemäße Verwaltung von Benutzern und Rechten hat eine besondere Sicherheitsrelevanz in einer Institution. Deshalb wird dieses Thema in einem eigenen Baustein behandelt (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*).

Die im vorliegenden Baustein beschriebenen Anforderungen sind auch dann anzuwenden, wenn IT-Systeme, Anwendungen oder Plattformen durch Dritte administriert werden. Besondere Anforderungen für solche Fälle werden zusätzlich in den Bausteinen OPS.2.1 *Outsourcing für Kunden* und OPS.3.1 *Outsourcing für Dienstleister* beschrieben.

Weiterhin bezieht sich der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* auf den Regelbetrieb. In Ausnahmesituationen, insbesondere bei einem möglichen IT-Angriff und der Kompromittierung von IT-Systemen, sind abweichende Anforderungen zu beachten, die in den entsprechenden Bausteinen aus dem Bereich DER.2 *Security Incident Management* beschrieben werden.

Aspekte des Patch- und Änderungsmanagement sind ebenfalls nicht Inhalt dieses Bausteins, sie sind im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* zu finden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* von besonderer Bedeutung:

2.1 Versäumnisse durch ungeregelte Zuständigkeiten

Hat der IT-Betrieb die administrativen Zuständigkeiten z. B. in den Bereichen Planung, Installation, Dokumentation und Überwachung nicht klar geregelt, können sicherheitsrelevante Aufgaben aus diesen Bereichen nicht oder nicht systematisch durchgeführt werden. Das Gleiche gilt, wenn die Regelungen den beteiligten Mitarbeitern nicht bekannt und verständlich sind. Typische Beispiele hierfür sind eine unklare Abgrenzung der Zuständigkeiten zwischen IT und Telekommunikationstechnik, zwischen Büro-IT und Fertigungsanlagen oder zwischen Anwendungs- und Plattformbetrieb.

2.2 Personalausfall von Kernkompetenzträgern

Auch Administratoren können ungeplant oder längerfristig ausfallen. Ohne eingearbeitete Vertreter ist nicht sichergestellt, dass die von ihnen betreuten IT-Systeme und Anwendungen ordnungsgemäß und sicher weiterbetrieben werden können. Administratoren bauen zum Teil sehr umfangreiches Detailwissen zu den von ihnen betreuten IT-Systemen und Anwendungen auf. Dies umfasst einerseits die eingesetzten Produkte und Lösungen, andererseits aber gerade auch Besonderheiten der Einsatzumgebung und der spezifischen Konfiguration. Mit diesem Wissen können Administratoren Fehler schnell erkennen und Anforderungen einfacher umsetzen. Häufig führt dies jedoch dazu, dass gerade komplexe IT-Systeme und Anwendungen oft von einzelnen Personen administriert werden. Fällt diese Person aus, ist auch das Wissen für die Institution nicht mehr verfügbar.

2.3 Missbrauch von administrativen Berechtigungen

Administrative Berechtigungen erlauben es, umfassend auf vertrauliche Informationen wie Dokumente, Kommunikationsinhalte oder Datenbanken zuzugreifen. Administratoren können diese weitreichenden Berechtigungen nicht nur dazu benutzen, die ihnen übertragenen Aufgaben zu erfüllen, sondern auch für eigene Zwecke oder im Sinne von Dritten. So könnten sie z. B. Personalunterlagen einsehen oder Kommunikationsvorgänge von Kollegen mitlesen. Weiterhin könnten auch Dritte Druck auf Administratoren ausüben oder Anreize für diese schaffen, um mit ihrer Hilfe missbräuchlich auf Daten oder IT-Systeme zuzugreifen.

2.4 Mangelhafte Berücksichtigung von administrativen Aufgaben

Die privilegierten Systemzugänge der Administratoren stehen häufig im Fokus von Angreifern. Werden

administrative Aufgaben nicht ordnungsgemäß erfüllt, dann werden dadurch Angriffe auf den Informationsverbund erheblich erleichtert. So können durch Fahrlässigkeit Fehler in der Konfiguration entstehen, vorgesehene Schutzmaßnahmen nicht oder nur unzulänglich umgesetzt oder auftretende Verdachtsmomente nicht verfolgt werden. Ursachen dafür sind z. B. ein fehlendes Sicherheitsbewusstsein, hoher Zeitdruck oder fehlende Prozesse und Verfahrensweisen. Daraus können sich Schwachstellen ergeben, die von Angreifern ausgenutzt werden könnten.

2.5 Störung des Betriebs

Administrative Tätigkeiten können unmittelbar den Betrieb von IT-Systemen und Anwendungen beeinflussen. So können zum Beispiel laufende Benutzersitzungen abgebrochen werden, wenn IT-Systeme neu gestartet werden oder berechtigte Zugriffe verhindert werden, während ein Firewall-Regelwerk angepasst wird. Werden solche Vorgänge ausgeführt, ohne zu berücksichtigen, wie sie sich auf die Benutzer auswirken und ohne sie mit den betroffenen Bereichen abzustimmen, kann der Betrieb erheblich gestört werden.

2.6 Fehlende Aufklärungsmöglichkeiten bei Vorfällen

Mängel in der Dokumentation des IT-Betriebs oder fehlende Aufzeichnungen können dazu führen, dass Sicherheitsvorfälle nicht aufgeklärt oder nachverfolgt werden können. Da bei Sicherheitsvorfällen häufig nicht einfach erkennbar ist, wie z. B. der Angriff durchgeführt wurde, welches Ausmaß er hatte oder wie manipuliert wurde, muss dies erst durch geeignete Untersuchungen ermittelt werden. Das setzt jedoch voraus, dass beispielsweise der Sollzustand von IT-Systemen vor dem Sicherheitsvorfall dokumentiert und prüfbar ist. Auch müssten ordnungsgemäße von unbefugten Änderungen an IT-Systemen anhand geeigneter Aufzeichnungen unterschieden werden können. Fehlen entsprechende Informationen, können Vorfälle nur schwer oder überhaupt nicht mehr aufgeklärt werden. Auch eine gerichtsfeste Beweisführung gegenüber den Tätern ist in solchen Fällen nicht mehr möglich.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Personalabteilung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* vorrangig erfüllt werden:

OPS.1.1.2.A1 ENTFALLEN (B)
Diese Anforderung ist entfallen.

OPS.1.1.2.A2 Vertretungsregelungen und Notfallvorsorge (B)
Es MUSS sichergestellt sein, dass benannte Vertreter auf die zu betreuenden IT-Systeme zugreifen können. Für Notfälle SOLLTEN Notfalluser mit Administrationsrechten eingerichtet werden.

OPS.1.1.2.A3 Geregelte Einstellung von IT-Administratoren (B)

Wenn Mitarbeiter administrative Aufgaben innerhalb einer IT-Umgebung übernehmen, MÜSSEN sie in ihre Tätigkeit eingewiesen werden, insbesondere in die vorhandene IT-Architektur und die von ihnen zu betreuenden IT-Systeme und Anwendungen. Die in der Institution gültigen und für ihre Tätigkeit relevanten Sicherheitsbestimmungen MÜSSEN den Administratoren bekannt sein.

OPS.1.1.2.A4 Beendigung der Tätigkeit als IT-Administrator [Personalabteilung] (B)

Wenn Administratoren von ihren Aufgaben wieder entbunden werden, MÜSSEN alle ihnen zugewiesenen persönlichen Administrationskennungen gesperrt werden. Es MUSS geprüft werden, welche Passwörter die ausscheidenden Mitarbeiter darüber hinaus noch kennen. Solche Passwörter MÜSSEN geändert werden.

Weiterhin MUSS geprüft werden, ob die ausscheidenden Mitarbeiter gegenüber Dritten als Ansprechpartner benannt wurden, z. B. in Verträgen oder als Admin-C-Eintrag bei Internet-Domains. In diesem Fall MÜSSEN neue Ansprechpartner festgelegt und die betroffenen Dritten informiert werden. Die Benutzer der betroffenen IT-Systeme und Anwendungen MÜSSEN darüber informiert werden, dass der bisherige Administrator ausgeschieden ist.

OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten (B)

Die Institution MUSS jederzeit nachweisen können, welcher Administrator welche administrativen Tätigkeiten durchgeführt hat. Dazu SOLLTE jeder Administrator über eine eigene Benutzerkennung verfügen. Auch Vertreter von Administratoren SOLLTEN eigene Benutzerkennungen erhalten.

Jeder Anmeldevorgang (Login) über eine Administrationskennung MUSS protokolliert werden.

OPS.1.1.2.A6 Schutz administrativer Tätigkeiten (B)

Administratoren MÜSSEN sich durch geeignete Verfahren authentisieren, bevor sie Aktionen mit administrativen Rechten durchführen.

Aktionen und Tätigkeiten, für die keine erhöhten Berechtigungen erforderlich sind, DÜRFEN NICHT mit administrativen Berechtigungen durchgeführt werden.

Die Institution MUSS sicherstellen, das nur Administratoren Zugriff auf administrative Schnittstellen und Funktionen haben. Insbesondere MUSS die Institution sicherstellen, dass nur Administratoren sicherheitsrelevante Änderungen an IT-Systemen und Anwendungen vornehmen können.

Die Administration MUSS über sichere Protokolle erfolgen. Es SOLLTE überlegt werden, ein eigenes Administrationsnetz einzurichten.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration*. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.2.A7 Regelung der IT-Administrationstätigkeit (S)

Die Befugnisse, Aufgaben und Pflichten der Administratoren SOLLTEN in einer Arbeitsanweisung oder Richtlinie verbindlich festgeschrieben werden. Die Aufgaben zwischen den einzelnen Administratoren SOLLTEN so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Administrationslücken entstehen. Die Regelungen SOLLTEN regelmäßig aktualisiert werden. Die Vorgaben SOLLTEN insbesondere eigenmächtige Änderungen der Administratoren im Informationsverbund ausschließen, soweit diese über die ihnen explizit übertragenen Aufgaben hinausgehen und nicht notwendig sind, um einen Sicherheitsvorfall oder Störfall abzuwenden.

OPS.1.1.2.A8 Administration von Fachanwendungen (S)

Die in diesem Baustein aufgeführten Basisanforderungen SOLLTEN auch für Mitarbeiter mit

administrativen Aufgaben für einzelne Fachanwendungen durchgängig umgesetzt werden. Die Aufgabenteilung zwischen Anwendungs- und Systemadministration SOLLTE klar definiert und schriftlich festgehalten werden. Zwischen den Verantwortlichen für die System- und Fachanwendungsadministration SOLLTEN Schnittstellen definiert sein.

Wenn administrativ in den Anwendungsbetrieb eingegriffen wird, SOLLTE das im Vorfeld mit dem Fachbereich abgestimmt sein. Dabei SOLLTEN die Bedürfnisse des Fachbereichs berücksichtigt werden.

OPS.1.1.2.A9 Ausreichende Ressourcen für den IT-Betrieb (S)

Es SOLLTEN ausreichende Personal- und Sachressourcen bereitgestellt werden, um die anfallenden administrativen Aufgaben ordnungsgemäß zu bewältigen. Dabei SOLLTE berücksichtigt werden, dass auch für unvorhersehbare Tätigkeiten entsprechende Kapazitäten vorhanden sein müssen.

Die Ressourcenplanung SOLLTE in regelmäßigen Zyklen geprüft und den aktuellen Erfordernissen angepasst werden.

OPS.1.1.2.A10 Fortbildung und Information (S)

Für die eingesetzten Administratoren SOLLTEN geeignete Fort- und Weiterbildungsmaßnahmen ergriffen werden. Dabei SOLLTEN auch technische Entwicklungen berücksichtigt werden, die noch nicht aktuell sind, aber für die Institution in absehbarer Zeit wichtig werden könnten. Die Fortbildungsmaßnahmen SOLLTEN durch einen Schulungsplan unterstützt werden. Dieser Schulungsplan SOLLTE das gesamte Team berücksichtigen, sodass alle erforderlichen Qualifikationen im Team mehrfach vorhanden sind.

Administratoren SOLLTEN sich regelmäßig über die Sicherheit der von ihnen betreuten Anwendungen, IT-Systeme, Dienste und Protokolle informieren, insbesondere über aktuelle Gefährdungen und Sicherheitsmaßnahmen.

OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten (S)

Systemänderungen SOLLTEN in geeigneter Form nachvollziehbar dokumentiert werden. Aus der Dokumentation SOLLTE hervorgehen,

- welche Änderungen erfolgt sind,
- wann die Änderungen erfolgt sind,
- wer die Änderungen durchgeführt hat sowie
- auf welcher Grundlage bzw. aus welchem Anlass die Änderungen erfolgt sind.

Sicherheitsrelevante Aspekte SOLLTEN nachvollziehbar erläutert und hervorgehoben werden.

OPS.1.1.2.A12 Regelungen für Wartungs- und Reparaturarbeiten (S)

IT-Systeme SOLLTEN regelmäßig gewartet werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind. Hierüber hinaus SOLLTE festgelegt werden, wer für die Wartung oder Reparatur von Geräten zuständig ist. Durchgeführte Wartungsarbeiten SOLLTEN dokumentiert werden.

OPS.1.1.2.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A20 Verwaltung und Inbetriebnahme von Geräten (S)

Es SOLLTE eine Übersicht aller Geräte vorhanden sein, die in der Institution genutzt werden und Einfluss auf die Informationssicherheit haben können. Dazu SOLLTEN neben IT-Systemen und ICS-Komponenten auch Geräte aus dem Bereich „Internet der Dinge“ (engl. „Internet of Things“, IoT) berücksichtigt werden. Vor der ersten Inbetriebnahme der Geräte SOLLTEN geeignete Prüf- und Genehmigungsverfahren vorgeschaltet werden. Die Übersicht SOLLTE stets aktuell gehalten werden und mit der Dokumentation von administrativen Tätigkeiten korrespondieren.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

OPS.1.1.2.A14 Sicherheitsüberprüfung von Administratoren [Personalabteilung] (H)
Bei erhöhtem Schutzbedarf SOLLTEN Administratoren einer zusätzlichen Sicherheitsüberprüfung unterzogen werden.

OPS.1.1.2.A15 Aufteilung von Administrationstätigkeiten (H)
Es SOLLTEN unterschiedliche Administrationsrollen für Teilaufgaben eingerichtet werden. Bei der Abgrenzung der Aufgaben SOLLTEN die Art der Daten und die vorhandene Systemarchitektur berücksichtigt werden.

OPS.1.1.2.A16 Zugangsbeschränkungen für administrative Zugänge (H)
Der Zugang zu administrativen Oberflächen oder Schnittstellen SOLLTE mit Filter- und Separierungsmaßnahmen technisch beschränkt werden. Oberflächen und Schnittstellen SOLLTEN für Personen außerhalb der zuständigen Administrationsteams nicht erreichbar sein. Auf IT-Systeme in anderen Schutzzonen SOLLTE ausschließlich über einen Sprungserver in der jeweiligen Sicherheitszone administrativ zugegriffen werden. Zugriffe von anderen Systemen oder aus anderen Sicherheitszonen heraus SOLLTEN abgewiesen werden.

OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip (H)
Bei besonders sicherheitskritischen IT-Systemen SOLLTE der Zugang zu Kennungen mit administrativen Berechtigungen so realisiert werden, dass dafür zwei Mitarbeiter erforderlich sind. Dabei SOLLTE jeweils ein Administrator die anstehenden administrativen Tätigkeiten ausführen, während er von einem weiteren Administrator kontrolliert wird.

OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (H)
Administrative Tätigkeiten SOLLTEN protokolliert werden. Bei besonders sicherheitskritischen IT-Systemen SOLLTEN alle administrativen Zugriffe durchgängig und vollständig protokolliert werden. Die ausführenden Administratoren SOLLTEN dabei selbst keine Berechtigung haben, die aufgezeichneten Protokolldateien zu verändern oder zu löschen. Die Protokolldateien SOLLTEN für eine angemessene Zeitdauer aufbewahrt werden.

OPS.1.1.2.A19 Berücksichtigung von Hochverfügbarkeitsanforderungen (H)
Die Administratoren SOLLTEN analysieren, für welche der von ihnen betreuten IT-Systeme und Netze Hochverfügbarkeitsanforderungen bestehen. Für diese Bereiche SOLLTEN sie sicherstellen, dass die eingesetzten Komponenten und Architekturen sowie die zugehörigen Betriebsprozesse geeignet sind, um diese Anforderungen zu erfüllen.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in der Area SY System Management, Vorgaben für die ordnungsgemäße IT-Administration vor.

Das BSI hat das vierbändige „Hochverfügbarkeitskompendium“ veröffentlicht.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den

Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.35 Nötigung, Erpressung oder Korruption

G 0.37 Abstreiten von Handlungen

G 0.42 Social Engineering