7 Sicherheitsverwaltung

Als R/3-Systemadministrator tragen Sie hinsichtlich von Sicherheitsfragen eine hohe Verantwortung. Hierzu gehört der Schutz des R/3-Systems und die Vorbereitung für eine Sicherheitsprüfung.

Wird ein R/3-Systems geprüft, ist der Systemadministrator für die Berücksichtigung der Prüfungsergebnisse verantwortlich. Jedes Prüfunternehmen verfügt über eigene Prozeduren und prüft möglicherweise ganz unterschiedliche Aspekte. Dieses Kapitel soll Sie daher auf die Kernpunkte vorbereiten, die normalerweise von allen Unternehmen kontrolliert werden.

Weitere Informationen finden Sie unter *www.service.sap.com/security*.

Das Thema Computersicherheit ist so umfassend, dass Ihnen dieses Kapitel lediglich eine Einführung dazu geben kann. Wir empfehlen Ihnen, mit allen Personen (externe Prüfer, interne Prüfer, Finanzabteilung, Rechtsabteilung usw.) zusammenzuarbeiten, die mit der Sicherheit des Systems zu tun haben.

Andere Sicherheitsaspekte sind besonders wichtig für die Installation von mySAP.com-Komponenten. Themen wie *Single Sign-On, zentrale Benutzerverwaltung* und *Netzwerksicherheit* werden allerdings im Rahmen unseres Buches nicht weiter behandelt.

Zentrale Benutzerverwaltung (ZBV)

Vor Version 4.5A musste die Verwaltung einzelner Benutzer in jedem einzelnen System durchgeführt werden. Ab Version 4.5A können Benutzer in einem einzigen zentralen System erstellt und verwaltet und dann auf die verschiedenen Client-Systeme verteilt werden. Dies stellt sicher, dass die Benutzer in allen Systemen konsistent sind, und vereinfacht die Verwaltung mehrerer Systeme.

Weitere Informationen finden Sie unter *www.service.sap.com/security* oder im SAP-Hinweis 159885.

Single Sign-On (SSO)

Benutzer müssen häufig auf verschiedene Services und Informationen innerhalb eines Intranet-Portals zugreifen, d.h., sie benötigen Zugriff auf verschiedene Systeme (SAP-Systeme oder andere) mit unterschiedlichen

Benutzerverwaltungsstrategien. Mit Hilfe von SSO kann eine Umgebung geschaffen werden, in der sich der Benutzer innerhalb des Portals bewegen kann, ohne seine Benutzerdaten zur Authentifizierung mehrfach eingeben zu müssen. Dies gilt auch für den Zugriff auf verschiedene Systeme.

Weitere Informationen finden Sie unter *www.service.sap.com/security* oder im SAP-Hinweis 318515.

7.1 Was bedeutet Sicherheit?

Das Thema Sicherheit umfaßt weit mehr als nur die Vergabe von R/3-Zugriffsrechten oder das Fernhalten von nicht autorisierten Benutzern. *Sicherheit* umfasst im Zusammenhang mit Daten vielmehr auch die folgenden Aspekte:

- Schutz der Daten vor Hardwareproblemen
- Sicherung der Datenintegrität
- Wiederherstellung von Daten nach einem Ausfall

In diesem Kapitel werden folgende Aspekte aus dem Bereich Sicherheit behandelt:

- Fernhalten von nicht autorisierten Benutzern
- Erteilen von beschränkten Zugriffsrechten
- Schützen der Daten vor Schaden oder Verlust
- Einhalten von rechtlichen, gesetzlichen oder sonstigen Bestimmungen

Nicht autorisierte Benutzer fernhalten

Viele denken im Zusammenhang mit Sicherheit als erstes an dieses Thema. Es umfasst Folgendes: R/3-Berechtigungskonzept, Sicherheit bei der Betriebssystem- und Netzwerkanmeldung sowie die physische Sicherheit.

Beschränkte Zugriffsrechte erteilen

Dieses Thema bezieht sich auf Benutzer, die Zugriff auf Teile des Systems und auf Daten haben, die sie nicht für ihren Job benötigen. Die Daten werden möglicherweise nicht direkt beschädigt, aber die Verbreitung dieser Daten könnte Schaden anrichten.

Beispiele für sensitive Daten:

- Kundenliste, Kontakte und Umsatz.
  Ein Konkurrent könnte sich diese Daten zunutze machen.

- Persönliche Daten der Mitarbeiter.
  Diese Daten fallen unter das Datenschutzgesetz.
- Finanzdaten, z.B. der vierteljährliche Finanzbericht.
  Für den Insiderhandel gibt es strenge Sicherheitsgesetze (siehe *Rechtliche, gesetzliche und andere Bestimmungen*).
- Vertragliche Vereinbarungen mit Kunden, Lieferanten und anderen.

Daten vor Schaden oder Verlust schützen

Die Ursachen für Schaden oder Verlust lassen sich in zwei Kategorien aufteilen:

- Unbeabsichtigt hervorgerufener Schaden oder Verlust, z.B.:
  - Laden von Testdaten in das Produktivsystem
  - Hardwareausfall
  - Zerstörung des Datencenters durch Feuer
  - Hochwasser, Orkane, Erdbeben oder andere Naturgewalten
- Vorsätzlich hervorgerufener Schaden oder Verlust, z.B.:
  - Löschen oder Beschädigen von Dateien durch einen Mitarbeiter
  - Löschen oder Beschädigen von Dateien durch einen Hacker

Rechtliche, gesetzliche oder sonstige Bestimmungen einhalten

In Gesetzen, Verträgen und anderen Bestimmungen werden andere Gründe für Sicherheit definiert.

Sicherheit ist ein sensibles Thema, das auch rechtliche Asspekte umfasst. Ein gutes Beispiel für die Bedeutung von Sicherheitsaspekten ist der Insiderhandel. Insiderwissen oder Insiderinformationen sind Informationen, die der Öffentlichkeit nicht zur Verfügung stehen. Wenn die Öffentlichkeit informiert wäre, hätte dies möglicherweise Auswirkungen auf den Aktienkurs. Beim Insiderhandel werden Insiderinformationen beim Kauf oder Verkauf von Aktien eingesetzt, um einen Gewinn zu erzielen oder einen Verlust zu beschränken. Selbst wenn Sie persönlich nicht von diesem Aktienkauf profitieren, können Sie dafür haftbar gemacht werden. Wenden Sie sich in Fällen von Insiderhandel an Ihre Rechtsabteilung.

Beispiel: Die Frau eines Mitarbeiters hat Insiderinformationen an einen Verwandten weitergegeben, der daraufhin Aktien gekauft und anschließend gewinnbringend verkauft hat. Der Verwandte hat durch den Ver-

kauf der Aktien noch vor der Gewinnverkündung einen Gewinn erzielt (Insiderhandel). Die Börsenaufsichtsbehörde hat die Ehefrau und den Verwandten mit einer Geldbuße bestraft. Die Ehefrau wurde schuldig befunden, die Insiderinformationen an den Verwandten weitergegeben zu haben, der daraufhin mit dem Verkauf der Aktien einen Gewinn erzielen konnte. Beide haben sich daher des Insiderhandels schuldig gemacht.

Beispiel: Der IS-Direktor eines Unternehmens hat um die Zugriffsberechtigung für das R/3-Produktivsystem gebeten. Diese Anfrage hat Besorgnis bei der Buchhaltung/Finanzabteilung hervorgerufen. Der Zugriff auf Finanzdaten wird normalerweise nur denjenigen Mitarbeitern gewährt, die damit arbeiten müssen. Der IS-Direktor benötigt für seine tägliche Arbeit allerdings keine Daten aus dem R/3-Produktivsystem. Als er anfing, Fragen zur Finanzsituation des Unternehmens (vierteljährliche Gewinne) zu stellen, bevor diese veröffentlicht wurden, wurde das Misstrauen der anderen Mitarbeiter geweckt. Der IS-Direktor hat sich nach Insiderinformationen erkundigt.

7.2 Prüfungen

Zwei verschiedene Prüfungsarten betreffen Sie als Systemadministrator:

- Die Sicherheitsprüfung
- Die Buchprüfung

7.2.1 Buchprüfung

Bei einer Buchprüfung werden die Bilanzen Ihres Unternehmens von einem Wirtschaftsprüfer geprüft. Zweck dieser Prüfung ist es, sich ein Bild von den Bilanzen des Unternehmens zu machen. Die Bilanz spiegelt im Wesentlichen die Finanzlage des Unternehmens wider. Eine Buchprüfung ist in der Regel obligatorisch, z.B. wenn die Aktien des Unternehmens an der Börse gehandelt werden. Wenn es sich bei Ihrem Unternehmen um ein Privatunternehmen handelt, können die Kreditoren eine Buchprüfung veranlassen.

Als Teil der Buchprüfung führt der Wirtschaftsprüfer normalerweise eine Sicherheitsprüfung von SAP R/3 und den verknüpften Systemen durch. Zweck der Sicherheitsprüfung ist es festzustellen, wie vertrauenswürdig die Daten des R/3-Systems sind. Die externen Prüfer evaluieren Ihr System und legen fest, welche Tests durchgeführt werden müssen und wie umfangreich die Tests sein sollen.

Sind die Evaluierungsergebnisse nicht zufriedenstellend, müssen möglicherweise umfangreichere Prüfungen durchgeführt werden. Dies hat zur Folge, dass sich die Kosten der Prüfung erhöhen und die Prüfungen durch den zusätzlichen Aufwand möglicherweise erst zu einem späteren Zeitpunkt abgeschlossen werden können. Im schlimmsten Fall kann festgestellt werden, dass die Sicherheitsvorkehrungen so schlecht sind, dass es nicht möglich ist, eine Aussage über die Finanzsituation des Unternehmens zu machen.

7.2.2 Sicherheitsprüfung

Eine Sicherheitsprüfung wird in erster Linie mit dem Ziel durchgeführt, die Sicherheit der R/3-Umgebung zu testen. Diese Prüfung wird normalerweise im Rahmen einer Buchprüfung vorgenommen, aber auch, um die Übereinstimmung mit gesetzlichen Vorgaben zu gewährleisten. Auch die unternehmensinternen Prüfungsverantwortlichen können eine Sicherheitsprüfung durchführen.

Geprüft wird die Sicherheit von vertraulichen Daten wie:

- Finanzdaten
- Kundendaten
- Produktdaten
- Mitarbeiterdaten (aus dem Modul HR)

7.2.3 Prüfungsaspekte

Bei Buch- oder Sicherheitsprüfungen berücksichtigen die Prüfer bestimmte Prüfungsaspekte.

Zu diesen Aspekten gehören unter anderem:

- Physische Sicherheit
- Netzwerksicherheit
- Benutzerverwaltungsprozeduren
  - Geeignete Aufgabenverteilung
  - Geeignete Schulung
  - Kennwörter
- Datensicherheit
  - Schutz vor Hardwarefehlern, gespiegelte Laufwerke, RAID, Failover, Hochverfügbarkeit usw.
  - Sicherungs- und Wiederherstellungsprozeduren

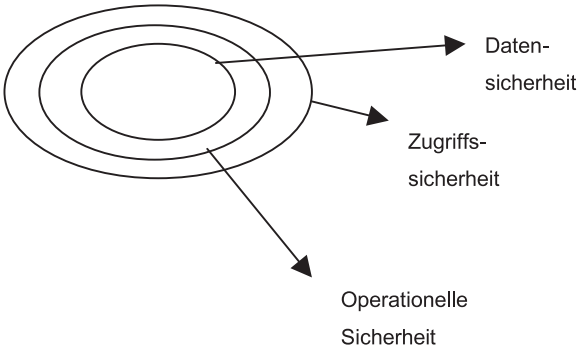
- Schutz des Produktivsystem vor unberechtigten Änderungen
- Sperren von gefährlichen Transaktionen

Diese Aufgaben unterstützen die Buch- oder Sicherheitsprüfung. Ohne zu wissen, was die Prüfer testen, können Sie sich nicht ausreichend vorbereiten und das System entsprechend schützen.

Dieser Teil behandelt nicht alle Fragen der SAP-Sicherheitsprüfung. Es werden lediglich einige Aspekte genannt, die im Rahmen einer Sicherheitsprüfung von Bedeutung sein können. Wir empfehlen Ihnen, vor der Buchprüfung mit den Prüfern zusammenzuarbeiten, um das System vorab zu testen und entsprechend auf die Prüfung vorbereiten zu können.

7.3 Sicherheitsebenen

Um Ihnen die Sicherheitsverwaltung zu erleichtern, haben wir uns entschlossen, mit einem der bereits vorhandenen Sicherheitsmodelle zu arbeiten: dem Sicherheitsebenenmodell. Dieses Modell setzt sich aus drei Hauptebenen zusammen:



- Zugriffssicherheit
  - Physische Sicherheit
  - Netzwerksicherheit
  - Anwendungssicherheit
- Operationelle Sicherheit
- Datensicherheit

7.3.1 Zugriffssicherheit

Physische Sicherheit

Bei der physischen Sicherheit wird der physische Zugriff auf SAP R/3 und die Netzwerkumgebung kontrolliert. Wie die Grafik verdeutlicht, muss sich ein Eindringling zunächst Zugang zur Anlage, zum Gebäude und zu den Bereichen des Gebäudes verschaffen, in denen sich die Benutzer oder die Geräte befinden (z.B. Finanzbereich, MIS oder Computerservice), oder zu den Computerräumen des Gebäudes (z.B. zum Serverraum, Kabelschrank oder Netzwerkraum), um dann zu dem inneren Kreis zu gelangen.

Diese Ebene ist wahrscheinlich auch die wichtigste. Wenn ein Eindringling sich erst einmal Zugang zu Ihren Geräten verschafft hat, kann er theoretisch auch die übrigen Sicherheitsebenen durchbrechen.

Wenn die physische Sicherheitsebene durchbrochen wurde, kann Folgendes passieren:

- Geräte können physisch beschädigt oder zerstört werden.
- Von der Bedienerkonsole kann auf das System zugegriffen werden (was zur Folge haben kann, dass die Netzwerksicherheit durchbrochen wird).
- Geräte können gestohlen werden.
- Daten können von Hackern missbraucht werden.

Ohne physischen Zugang zu dem Gebäude muss sich der Eindringling auf elektronischem Wege über das Netzwerk Zugriff auf das System verschaffen.

Die Geräte, auf dem das R/3-System läuft, sollten sich in einem gesicherten Raum befinden. Der Zugang zu diesem Raum sollte durch eine abschließbare Tür gesichert sein. Außerdem sollte unbedingt der Zugang zum Serverraum kontrolliert werden.

Wenn Sie ein Zugangssystem mit elektronischem Kartenschlüssel einsetzen, sollten Sie in regelmäßigen Abständen das Zugangsprotokoll für den Serverraum prüfen. Die regelmäßige Prüfung des Zugangsprotokolls könnte auch ein Aspekt sein, der von den Prüfern untersucht wird.

Netzwerksicherheit

Die Netzwerksicherheit umfasst ebenfalls untergeordnete Sicherheitsebenen. Ziel dieses Sicherheitstyps ist es, den externen Zugriff auf das Netzwerk und die Anmeldungen am Netzwerk zu kontrollieren. Der Anmeldezugriff kontrolliert den Zugriff vor Ort und den remoten Zugriff. Außerdem wird festgelegt, worauf der einzelne Benutzer zugreifen kann.

Wenn Eindringlinge auf Ihr Netzwerk zugreifen, verfügen sie möglicherweise über eine elektronische Verbindung zu Ihren Computern. Die verschiedenen Zugangspunkte zu Ihrem Netzwerk sollten von Spezialisten für die Netzwerksicherheit konfiguriert werden. Darüber hinaus sollten die Aktivitäten der Benutzer verfolgt werden.

Die folgenden Zugangspunkte sollten beispielsweise überprüft werden:

- Zugriff von außerhalb
  - Einwählzugriff
  - Internetzugriff
  - andere remote Zugriffsmethoden, z.B. VPN
- Netzwerkanmeldezugriff
  Diese Zugangsmethode stellt die tatsächliche Anmeldung am Netzwerk (z.B. der NT-Domäne) dar.
- Zugang zu Teilen des Netzwerks
  - NT-Domänen

Für NT-Domänen wird Folgendes empfohlen:

- Sie sollten über eine eigene SAP-Domäne verfügen, bei der sich nur Systemadministrator direkt anmelden können.
- Sie sollten über weitere Domänen verfügen, bei denen sich Benutzer anmelden können. Diese Domänen sollten der SAP-Domäne »vertrauen«, jedoch nicht umgekehrt.

  - Routertabellen
    Mit Hilfe dieser Tabellen können Sie anhand der IP-Adresse kontrollieren, welche Benutzer auf die SAP-Server zugreifen können.

Anwendungssicherheit

Wie die anderen Ebenen umfasst auch die Anwendungssicherheit weitere Unterebenen, die Folgendes kontrollieren:

- den Zugang zur Anwendung, z.B. die Anmeldung bei SAP R/3
- den Zugriffspunkt des Benutzers auf die Anwendung
- die Berechtigungen des Benutzers innerhalb der Anwendung
- die Berechtigungen des Benutzers auf der Basis der Systemdaten in der Anwendung (z.B. im R/3-System durch die Beschränkung des Benutzers auf *company* `001` und *Kostenstelle* `200`)
- die R/3-Sicherheitsfunktionen auf dieser Ebene
  Auf dieser Ebene werden die Funktionen festgelegt, auf die der Benutzer zugreifen kann (z.B. Lesen – nicht Ändern! – von Buchungsdaten nur für *Kostenstelle 200* in *company 001*).
- Verwendung von R/3-Anwendungstools, z.B.:
  - Profilgenerator (Transaktion `PFCG`; weitere Informationen enthält das Handbuch *Authorizations Made Easy*)
  - Audit Information System (Transaktion `SECR`)
  - Security-Audit-Log (Transaktion `SM19`/`SM20`)
  - Löschen alter Audit-Dateien (Transaktion `SM18`)

7.3.2 Operationelle Sicherheit

Diese Ebene bietet Sicherheit auf operationeller Ebene sowie auf der Benutzerebene. Hier geht es hauptsächlich um Fragen hinsichtlich von Prozeduren und Kontrollfunktionen und weniger um Computer und Systeme.

Diese Prozeduren und Kontrollfunktionen betreffen Organisation und Mitarbeiter und können sich problematisch gestalten: Die Mitarbeiter müssen sich hierfür an Vorschriften und Regeln halten, tun dies aber nicht immer.

Methoden der operationellen Kontrolle sind z.B.:

- Die Aufgabenverteilung
- Die Vermeidung der gemeinsamen Nutzung von Benutzer-IDs
- Die Standards für Kennwörter
- Das Abmelden bei Arbeitspausen (z.B. während der Mittagspause) oder zum Feierabend

7.3.3 Datensicherheit

Diese Ebene ist eng mit der Desaster-Recovery verbunden (siehe Kapitel 2). Die Desaster-Recovery stellt einen wichtigen Teil der Datensicherheit dar. Mit Hilfe der Datensicherheit wird Folgendes geschützt:

- Serverdaten
  Die Daten auf dem Server werden vor Beschädigung oder Verlust geschützt. Dieser Schutz wird mit unterschiedlichen Mitteln erreicht, das Ziel ist es jedoch immer, den durch einen Störfall verursachten Datenverlust so gering wie möglich zu halten bzw. ganz zu vermeiden.
- Sicherungsdaten
  Auf dieser Ebene werden die Anwendungsdaten normalerweise auf einem Band gesichert, mit dem das System wiederhergestellt werden kann.

  Die Sicherungsbänder müssen aus folgenden Gründen sicher gelagert werden:
  - Um sie im Falle eines Desasters einsetzen zu können
  - Um sie vor Diebstahl zu schützen
- Zur Desaster-Recovery

Ergreifen Sie die Initiative, um Problemen vorzubeugen:

- Verringern Sie die Wahrscheinlichkeit eines Datenverlusts
  Der Server sollte für Sie der wichtigste Ort ist, an dem die Daten gesichert werden
- Schützen Sie die Sicherungsdaten vor Schaden oder Verlust
- Stellen Sie sicher, dass das System nach einem Ausfall vollständig wiederhergestellt werden kann.

Daten auf den Servern sichern:

- Im Fall einer Notsituation müssen Sie den Datenverlust so weit wie möglich verhindern. Diese Optionen gewährleisten die Hochverfügbarkeit (High Availability, HA):
  - RAID-Arrays für Laufwerke
  - Redundante Geräte
  - Zuverlässige Geräte und Lieferanten
  - Support-Verträge für die Hardware des Produktivsystems
- Die folgenden Optionen beziehen sich auf die Einrichtungen:
  - Unterbrechungsfreie Stromversorgung (USV)
  - Feuermelder und Geräte für den Feuerschutz
  - Alarmanlage
  - Umgebungsalarm

- Sicherungen
  - Sicherungsbänder sollten an einen sicheren Ort außerhalb des Unternehmens geschickt werden.
    Durch diese Maßnahme werden die Sicherungsdaten im Falle eines Störfalls vor Beschädigung oder vollständiger Zerstörung geschützt.
  - Die Lagerorte der Sicherungsbänder – sowohl vor Ort als auch außerhalb des Unternehmens – müssen gesichert werden, um die Bänder vor Diebstahl zu schützen.
    Im Falle eines Diebstahls der Bänder können die Daten wiederhergestellt und missbraucht werden. Werden Datenbanktools eingesetzt, ist es möglich, die meisten R/3-Sicherheitsfunktionen zu umgehen, da die Tabellen direkt gelesen werden können.

7.3.4 Mehrfache Benutzeranmeldungen verhindern

Mehrfache Benutzeranmeldungen zu verhindern bedeutet, dass immer nur eine Anmeldung einer Benutzer-ID beim R/3-System zulässig ist. Mehrfache Benutzeranmeldungen treten auf, wenn Benutzer eine Benutzer-ID gemeinsam einsetzen oder aber wenn jemand die Benutzer-ID eines Benutzers ohne dessen Wissen verwendet.

Wenn mehrere Mitarbeiter eine Benutzer-ID gemeinsam verwenden, werden Sie mit folgenden Problemen konfrontiert:

- Sie wissen nicht, wer für das Problem verantwortlich ist.
- Die Situation würde im Fall einer Sicherheitsprüfung negativ bewertet werden.

Deaktivieren Sie daher den Parameter für die mehrfache Benutzeranmeldung *login/disable_multi_gui_login* im Systemprofil.

7.3.5 Änderungen im Produktivsystem verhindern

Für das Produktivsystem sollte der Parameter *nicht änderbar* eingestellt sein. Die Sperren im System sollten so eingestellt sein, dass die Konfiguration (mandantenunabhängig und mandantenabhängig) nicht direkt im Produktivsystem geändert werden kann. Mit dieser Einstellung wird sichergestellt, dass die Änderungen kontrolliert durchgeführt werden.

In der Entwicklungspipeline durchlaufen die Änderungen folgende Stadien:

1. Durchführen im Entwicklungssystem
2. Testen im Entwicklungssystem

3. Transportieren vom Entwicklungssystem in das Testsystem
4. Testen im Testsystem
5. Transportieren vom Testsystem in das Produktivsystem

Durch diese Vorgehensweise werden Änderungen ordnungsgemäß in der Pipeline getestet und auf die Systeme angewandt. Eine Pipeline ist die Umgebung, in der Änderungen vom Entwicklungssystem ins Qualitätssicherungs- und schließlich ins Produktivsystem übertragen werden.

Die Konfigurationsänderungen sollten nicht direkt im Produktivsystem vorgenommen werden, denn so wird die Integrität des Produktivsystems nicht gefährdet. Andernfalls kann es zum Zusammenbruch des Produktivsystems kommen, da die Änderungen nicht getestet wurden oder nicht mit den Änderungen im Entwicklungssystem übereinstimmen.

Das Produktivsystem sollte vor Änderungen geschützt werden. Vor der Übertragung von Änderungen in das Produktivsystem sollten diese ausreichend getestet werden, um die Integrität der Pipeline sicherzustellen. Wenn Änderungen direkt im Produktivsystem durchgeführt werden, ist die Entwicklungs- und Test-Pipeline nicht mehr mit dem Produktivsystem synchron. Wenn die Pipeline nicht mehr synchron ist, können keine verlässlichen Tests mehr durchgeführt werden.

Alle Änderungen sollten im Entwicklungssystem vorgenommen werden und dann über die Pipeline zum Produktivsystem transportiert werden. Auf diese Weise werden für alle Systeme die gleichen Änderungen vorgenommen. Oft werden Änderungen direkt im Produktivsystem damit begründet, dass der Transport der Änderung zu lange dauert. Die Folge ist aber eine nicht synchrone Systemlandschaft, in der die Änderungen des Produktivsystems nicht mit denen des Entwicklungs- oder Testsystems übereinstimmen. Darüber hinaus lösen sie häufige Notfalltransporte aus.

Exceptions

Unregelmäßige Exceptions treten auf, wenn kein Mechanismus für den Transport der Änderungen verfügbar ist oder aufgrund eines SAP-Hinweises eine direkte Änderung erforderlich ist.

Wenn eine Änderung nicht transportiert werden kann, muss die folgende Prozedur durchgeführt werden:

1. Überprüfen Sie, ob die Änderung tatsächlich nicht transportiert werden kann. Einige Objekte benötigen für den Transport möglicherweise ein ABAP-Programm.
2. Entsperren Sie das System, damit Änderungen vorgenommen werden können.
3. Nehmen Sie die Änderung vor.
4. Sperren Sie das System sofort wieder.
5. Führen Sie **dieselben** Änderungen für **alle** anderen Systeme durch.

Führen Sie diese Prozedur **nur** dann durch, wenn eine Änderung nicht transportiert werden kann.
Manuelle Änderungen erhöhen die Fehlerwahrscheinlichkeit.

Produktivsystem auf »nicht änderbar« setzen (Transaktionen SE03, SCC4)

Schalter können verhindern, dass Änderungen im System vorgenommen werden. Im Produktivsystem sollten diese auf *nicht änderbar* gesetzt sein. Dadurch wird sichergestellt, dass Änderungen über die Entwicklungspipeline vorgenommen werden. Durch diese Vorgehensweise werden Änderungen ordnungsgemäß in der Pipeline getestet und auf die Systeme angewandt.

Objekte sollten im Produktivsystem nicht änderbar sein. Dies verhindert, dass im Produktivsystem Objekt- oder Konfigurationsänderungen vorgenommen werden, bevor diese getestet wurden. Wenn Sie das Produktivsystem auf *nicht änderbar* setzen, schützen Sie die Integrität der Pipeline.

Mit den Transaktionen *SE03* und *SCC4* können Sie das System auf *nicht änderbar* setzen. Diese Transaktionen können auch für andere Aufgaben genutzt werden.

Mandantenunabhängige Änderungen (Transaktion SE03)

1. Geben Sie in das Befehlsfeld *Transaktion* `SE03` ein, und drücken Sie *Enter*.
2. Wählen Sie *Systemänderbarkeit setzen*.
3. Wählen Sie  .

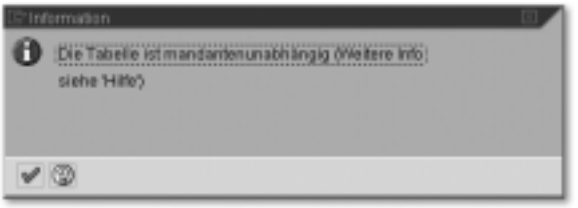
4. Wählen Sie unter *Globale Einstellung* :
   - *nicht änderbar*, wenn Sie das System sperren wollen.
   - *änderbar*, wenn Sie das System entsperren wollen (in diesem Beispiel ausgewählt).
5. Wählen Sie .

Mandantenunabhängige und mandantenabhängige Änderungen (SCC4)

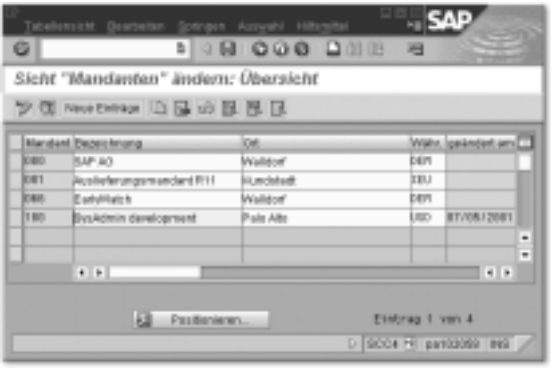
Bei dieser Methode werden auch die mandantenabhängigen Änderungen gesperrt.

1. Geben Sie in das Befehlsfeld *Transaktion* `SCC4` ein, und wählen Sie *Enter* (alternativ können Sie auch im *SAP-Standardmenü* den folgenden Menüpfad wählen: *Werkzeuge* • *Administration* • *Verwaltung* • *Mandantenverwaltung* • *SCC4-Mandantenpflege*).
2. Wählen Sie .

3. Wählen Sie zum Fortfahren .



4. Wählen Sie die Mandantennummer (z.B. `100`).
5. Wählen Sie .



So sperren Sie einen Mandanten (nicht änderbar):

1. Wählen Sie unter *Änderungen und Transporte für mandantenunabhängige Objekte* die Option *keine Änderungen erlaubt*.
2. Wählen Sie unter *Änderungen an mandantenübergreifenden Objekten* das Symbol und dann *keine Änderungen an Repository- und mand.unabh. Cust.-Obj.*
3. Wählen Sie unter *Schutz bzgl. Mandantenkopierer und Vergleichstool* das Symbol und dann *Schutzstufe 2: kein Überschreiben, keine ext. Verfügbarkeit*.
4. Wählen Sie *Sichern*.

So entsperren Sie einen Mandanten (änderbar):

1. Wählen Sie unter *Änderungen und Transporte für mandantenunabhängige Objekte* die Option *Automatische Aufzeichnung von Änderungen*.
2. Wählen Sie unter *Änderungen an mandantenübergreifenden Objekten* das Symbol und dann *Änderungen an Repository- und mand.unabh. Customizing erlaubt*.
3. Wählen Sie unter *Schutz bzgl. Mandantenkopierer und Vergleichstool* das Symbol und dann *Schutzstufe 0: keine Beschränkung*.
4. Wählen Sie *Sichern*.

7.3.6 Sperre von gefährlichen Transaktionen prüfen

Gefährliche Transaktionen können das System beschädigen, stellen ein Sicherheitsrisiko dar oder beeinträchtigen die Performance.

- Der Zugriff auf gefährliche Transaktionen ist im Produktivsystem kritischer als im Entwicklungs- oder Testsystem. Dies ist auf das Vorliegen von Live-Daten und die Tatsache zurückzuführen, dass die Geschäftsabläufe vom R/3-System abhängig sind.
- Einige Transaktionen sollten im Produktivsystem, nicht jedoch im Entwicklungs-, Test- oder Schulungssystem, gesperrt werden. Die Standardsicherheit unterbindet normalerweise den Zugriff auf diese Trans-

aktionen, jedoch können einige Administratoren, Programmierer, Berater und wichtige technische Benutzer Zugriff auf diese Transaktionen haben, was im Einzelfall vom jeweiligen System abhängig ist. In solchen Fällen bietet die Transaktionssperre eine Art »zweite Verteidigungslinie«.

Es gibt über 51.000 englische Transaktionscodes im SAP R/3-System. Zwecks Überschaubarkeit sollten nur die gefährlichen Transaktionscodes gesperrt werden. Ihre technischen Berater können Ihnen weitere kritische Transaktionen in Ihren Modulen nennen.

Die Tabelle unten wurde in Zusammenarbeit mit Basis-Beratern und Benutzern erstellt und enthält die Transaktionen, die gesperrt werden sollten. Die Transaktionen sind in folgende Risikokategorien eingeteilt:

- Gefährlich
- Die Sicherheit beeinträchtigend
- Die Performance beeinträchtigend

Transaktion	Beschreibung	Gefährlich	Sicherheit beeinträchtigend	Performance beeinträchtigend
F040	Reorganisation	X		
F041	Archivierung Bankstammdaten	X		
F042	Archivierung Sachkonten	X		
F043	Archivierung Debitoren	X		
F044	Archivierung Kreditoren	X		
F045	Archivierung Belege	X		
F046	Archivierung Verkehrszahlen	X		
GCE2	Profile		X	
GCE3	Objektklassen		X	
KA10	Kostenstellen archivieren (gesamt)	X		
KA12	Kostenstellen archivieren (Plan)	X		
KA16	Kostenstellen archivieren (Einzelp.)	X		
KA18	Archivverwaltung: Umlage, Vert., …	X		

Transaktion	Beschreibung	Gefährlich	Sicherheit beeinträchtigend	Performance beeinträchtigend
KA20	Archivierung Kostenstellen (gesamt)	X		
O001	C CL Benutzerpflege		X	
O002	C CL Benutzerprofile		X	
O016	C CL Berechtigungen		X	
OBR1	Belege löschen	X		
OBZ7	C FI Benutzer		X	
OBZ8	C FI Profile		X	
OBZ9	C FI Berechtigungen		X	
OD02	Rolle für DVS definieren		X	
OD03	CV Benutzerprofile		X	
OD04	CV Benutzerpflege		X	
OIBA	Berechtigungen		X	
OIBB	Benutzerpflege		X	
OIBP	Benutzerprofile		X	
OMDL	C MM-MRP Benutzerpflege		X	
OMDM	C MM-MRP Benutzerprofile		X	
OMEH	C MM-PUR Benutzerpflege		X	
OMEI	C MM-PUR Benutzerprofile		X	
OMG7	C MM-PUR Berechtigungen		X	
OMI6	C MM-MRP Berechtigungen		X	
OML0	MM: Benutzerpflege Lagerverwaltung		X	
OMM0	MM: Benutzerprofile Lagerverwaltung		X	
OMNP	Berechtigungen im MM-WM		X	
OMSN	C MM-BD Benutzerpflege		X	
OMSO	C MM-BD Benutzerprofile		X	
OMSZ	C MM-BD Berechtigungen		X	
OMWF	C MM-IV Benutzerpflege		X	

Transaktion	Beschreibung	Gefährlich	Sicherheit beeinträchtigend	Performance beeinträchtigend
OMWG	C MM-IV Benutzerprofile		X	
OMWK	C MM-IV Berechtigungen		X	
OOPR	Berechtigungsprofilpflege		X	
OOSB	Benutzer (strukturelle Berechtigung)		X	
OOSP	Berechtigungsprofile		X	
OOUS	Benutzer pflegen		X	
OP15	Produktion Benutzerprofile		X	
OP29	Produktion Benutzerpflege		X	
OPCA	Benutzerpflege		X	
OPCB	Benutzerprofile		X	
OPCC	Berechtigungen		X	
OPE9	Pflege Ben. Profile		X	
OPF0	Benutzerpflege		X	
OPF1	C CAP Berechtigungen		X	
OPJ0	Benutzerpflegen		X	
OPJ1	Pflege Ben. Profile		X	
OPJ3	Pflege Berechtigungen		X	
OSSZ	C PP Berechtigungen		X	
OTZ1	C FI Benutzer		X	
OTZ2	C FI Profile		X	
OTZ3	C FI Berechtigungen		X	
OVZ5	C RV Benutzerpflege		X	
OVZ6	C RV Benutzerprofil v_sd_all pflg.		X	
OY20	Berechtigungen Customizing		X	
OY21	Benutzerprofile Customizing		X	
OY22	Unterverwalter anlegen Customizing		X	
OY27	Superuser anlegen Customizing		X	

Transaktion	Beschreibung	Gefährlich	Sicherheit beeinträchtigend	Performance beeinträchtigend
OY28	SAP* deaktivieren		X	
OY29	Dokumentationsentwickler		X	
OY30	Dokumentationsentwickler		X	
SARA	Archivadministration	X		
SCC5	Mandanten löschen	X		
SE01	Transport Organizer (Erw. Sicht)			
SE06	Einrichten Transport Organizer	X	X	
SE09	Transport Organizer			
SE10	Transport Organizer			
SE11	R/3-Data-Dictionary	X		
SE13	Speicher-Param. für Tabellen pflegen	X		
SE14	Utilities für Dictionary-Tabellen	X		
SE15	Dictionary-Infosystem			
SE16	Data Browser			X
SE17	Allgemeine Tabellenanzeige			X
SE38	ABAP-Editor	X		
SM49	Ausführen externer OS-Kommandos	X	X	
SM59	RFC-Destinations (Anzeige u. Pflege)			
SM69	Ausführen externer OS-Kommandos	X	X	
ST05	Performance Trace			X
SU12	Massenänderungen Benutzerstamm	X	X	

Die folgende Tabelle enthält Transaktionen, die möglicherweise nicht gesperrt werden können, da sie regelmäßig eingesetzt werden. Diese Transaktionen werden aus bestimmten Gründen in einem Produktivsystem verwendet. Da sie aber gefährlich sind, sollte der Zugriff auf diese Transaktionen eingeschränkt sein.

Transaktion	Beschreibung	Gefährlich	Sicherheit beeinträchtigend	Performance beeinträchtigend
RZ10	Pflege von Profilparametern	X		
SA38	ABAP/4 Reporting	X		
SM04	Benutzerliste		X	
SM12	Sperren anzeigen und löschen	X		
SM13	Verbuchungssätze anzeigen	X		
SM30	Aufruf View-Pflege	X		
SM31	Aufruf View-Pflege analog SM30	X		
STMS	Transport Management System	X		
SU01	Benutzerpflege		X	
SU02	Pflege Berechtigungsprofile		X	
SU03	Pflege Berechtigungen		X	

Tabelle *TSTCT* enthält die Transaktionscodes und den Namen der Transaktion. Die Tabelle umfasst zurzeit über 98.000 Einträge (bei einer englischen Benutzeroberfläche), davon sind 51.000 in englischer Sprache.

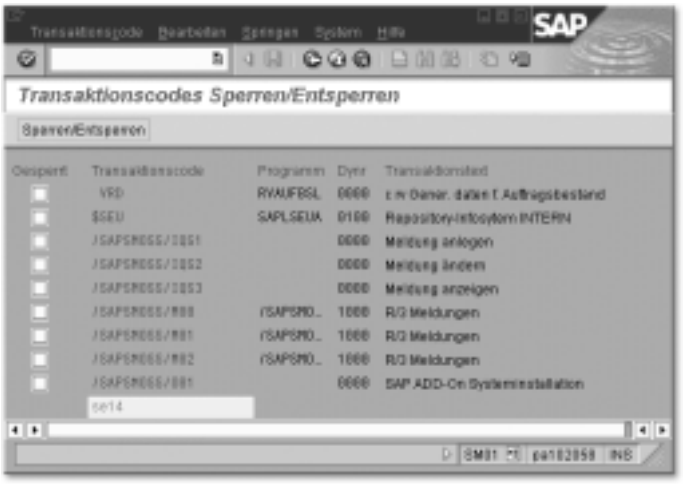
Erstellen und verwalten Sie eine Liste auf Grundlage der folgenden Informationen:

- Welche Transaktionen sind gesperrt?
- Warum sind diese gesperrt?
- Wer hat sie gesperrt?
- Wann wurden sie gesperrt?

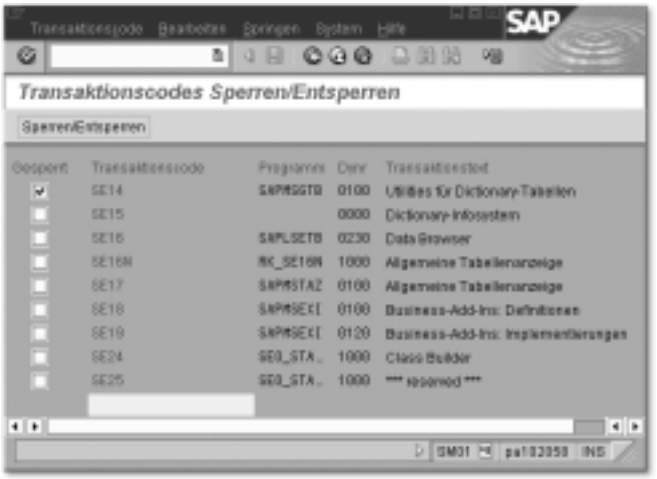
Die Pflege der oben genannten Informationen ist wichtig für den Fall, dass jemand wissen möchte, wer die Transaktion gesperrt hat und warum sie gesperrt wurde.

1. Geben Sie in das Befehlsfeld *Transaktion* `SM01` ein, und wählen Sie *Enter* (oder wählen Sie im SAP-Menü *Werkzeuge* • *Administration* • *Verwaltung* • *SM01 Tcode-Verwaltung*).

2. Geben Sie den Transaktionscode, den Sie sperren möchten (z.B. `SE14`), in das Suchfeld unterhalb der Spalte *Transaktionscode* ein.
3. Wählen Sie .



4. In Spalte *Gesperrt*:
   - Markieren Sie zum Sperren einer Transaktion das Feld links neben der Transaktion.
   - Deaktivieren Sie zum Entsperren einer Transaktion das Feld links neben der Transaktion.
5. Wählen Sie .
6. Wählen Sie *Zurück*.



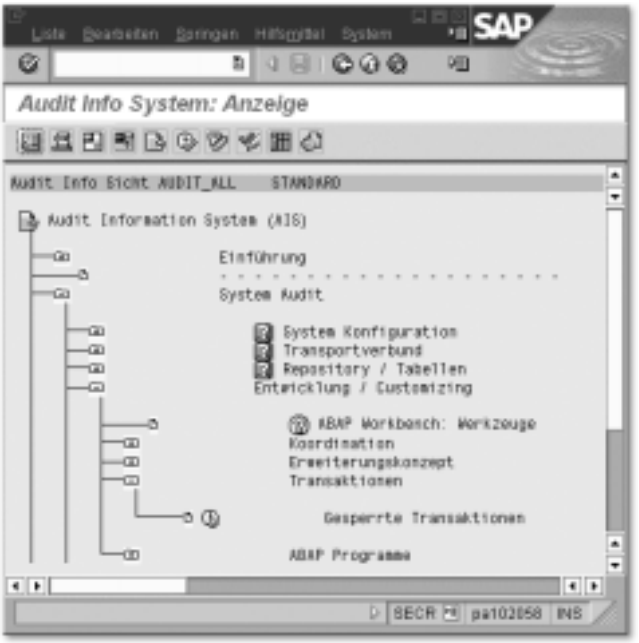
Prüfen Sie, welche Transaktion Sie sperren. Es besteht die Gefahr, dass Sie versehentlich eine wichtige Transaktion sperren. Dies kann zur Folge haben, dass Sie diese Transaktion oder andere Transaktionen nicht mehr entsperren können.

Mit Hilfe von Sicherheitsberechtigungen im Sicherheitsobjekt S_TCODE unter den anwendungsübergreifenden Berechtigungsobjekten kann auch der Transaktionszugriff kontrolliert werden.

So erstellen Sie eine Liste mit gesperrten Transaktionen

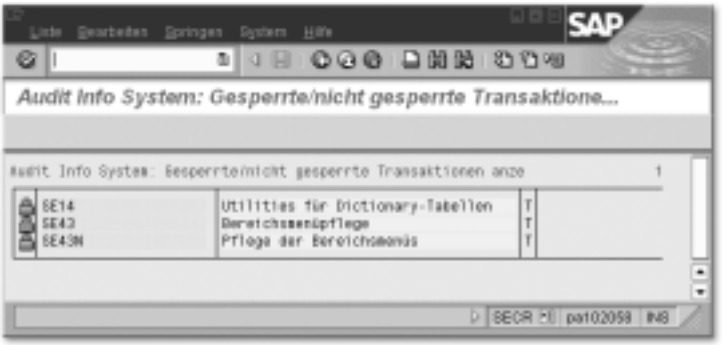
1. Geben Sie in das Befehlsfeld *Transaktion* `SECR` ein, und wählen Sie *Enter*.
2. Wählen Sie *Komplettes Audit*.
3. Wählen Sie .

4. Expandieren Sie den folgenden Menüpfad: *Audit Information System (AIS)* • *System Audit* • *Entwicklung/Customizing* • *Transaktionen* • *Gesperrte Transaktionen*.
5. Wählen Sie neben *Gesperrte Transaktionen*.



6. Markieren Sie folgende Kästchen:
   - *Gesperrt*
   - *Transaktionen*
   - *Menütransaktionen*
   - *Parametertransaktionen*
   - *Reporttransaktionen*
7. Wählen Sie .

8. Das folgende Bild zeigt eine Liste mit den gesperrten Transaktionen.



7.4 Operationelle Sicherheit

In diesem Abschnitt werden ausgewählte Themen aus dem Bereich operationelle Sicherheit beschrieben.

7.4.1 Aufgabenverteilung

Für Aufgabenkombinationen, die als risikoreich erachtet werden oder die die internen Kontrollen vermindern, sind standardmäßige Prüfungsrichtlinien vorhanden. Zu diesen Kombinationen gehören unter anderem:

- Kreditoren und Scheckerstellung
- Debitoren und Geldeingang
- ABAP-Entwicklung und Transportsteuerung

Ihre externen Prüfer sollten Sie bei der Definition dieser risikoreichen Kombinationen unterstützen. Zu den Standardprüfungsprozeduren gehört das Prüfen der Aufgabenverteilung.

Debitoren und Eingang von Barmitteln

Der Mitarbeiter, der für den Zahlungseingang zuständig ist, sollte nicht gleichzeitig für die Erfassung der Kundenfinanzdaten zuständig sein. Hier besteht die Gefahr, dass der Mitarbeiter das vom Kunden erhaltene Bargeld nicht weiterleitet, den Betrag aber dem Kundenkonto gutschreibt.

Im Rahmen der Prüfung der Aufgabenverteilung sollten auch die verschiedenen Benutzereigentümer (Schlüsselbenutzer jedes Funktionsbereichs) geprüft werden.