Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitshinweise für Administratoren

- Beispiel -

Stand: Dezember 2008

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

INHALTSVERZEICHNIS

1 Einleitung

Durch den zunehmenden Einsatz und die daraus resultierende Abhängigkeit von der Informationstechnologie können Bedrohungen für die Institution entstehen. Neben dem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener, vertraulicher und weiterer sensitiver Informationen durch IT-Fehlfunktionen und durch menschliches Fehlverhalten (bewusst oder unbewusst), kann das ganze System Ziel von Angriffen sein (von innen und außen).

Diese Sicherheitshinweise basieren auf den BSI Sicherheitsstandards und den IT-Grundschutz-Katalogen des BSI. In der rechten Spalte befinden sich Verweise zu Hintergrundinformationen und zu Maßnahmenvorschlägen innerhalb der IT-Grundschutz-Kataloge.

M x.xx

2 Verantwortungsbereich

Der Administrator ist innerhalb seines zugewiesenen Bereichs dafür verantwortlich, dass durch wirksame Maßnahmen die Sicherungsziele realisiert werden und ihre Einhaltung kontrolliert werden kann.

Dabei sind neben geltenden, einschlägigen Gesetzen und Vorschriften die folgenden Richtlinien zu befolgen und technisch durch den Administrator zu unterstützen bzw. zu ermöglichen (siehe Musterdokumente des BSI):

- Leitlinie zur Informationssicherheit
- Sicherheitsrichtlinie zur IT-Nutzung
- Sicherheitsrichtlinie zur Internetnutzung
- Sicherheitsrichtlinie für Outsourcing
- Viren-Schutzkonzept
- Notfallvorsorgekonzept
- Datensicherungskonzept

Die Regelungen haben verbindlichen Charakter, so dass Verstöße gegen die

Inhalte der Richtlinien zu arbeitsrechtlichen Konsequenzen führen können.

Die "Sicherheitshinweise für Administratoren" werden im Intranet veröffentlicht.

Zur Verbesserung der Informationssicherheit hat ein Administrator mit dem IT-Sicherheitsbeauftragten zu kooperieren. Darüber hinaus hat er sich regelmäßig über sicherheitsrelevante Patches, Updates oder sonstige Anleitungen zur Behebung von Sicherheitslücken zu informieren. M 2.35

Jeder Administrator hat als Benutzer der IT-Dienste auch die "Sicherheitshinweise für IT-Benutzer" (siehe Musterdokument des BSI) zu beachten.

IT-Benutzer sind bei der Arbeit an IT-Diensten und der Umsetzung von Standard-Sicherheitsmaßnahmen zu unterstützen. M 2.12

Jeder Administrator hat einen Vertreter einzuweisen und laufend zu informieren. Dokumentationen sind so zu gestalten, dass der Vertreter mit ihrer Hilfe seine Aufgaben wahrnehmen kann.

Der Administrator hat bei der Erstellung von Konzepten (z. B. Virenschutz- oder Notfallkonzept) mitzuwirken.

3 Verwaltung der IT-Dienste

3.1 Konfiguration der IT-Dienste

Vor dem Einsatz ist Soft- und Hardware nach Möglichkeit zu testen. M 4.65

Es sind die Test- und Freigabeverfahren zu beachten. M 2.62, M 2.216

Soft- und Hardware sind durch den Administrator möglichst so zu konfigurieren, dass ohne weiteres Zutun des Benutzers optimale Sicherheit erreicht werden kann. Es sind angemessene Sicherheitsprodukte einzusetzen. M 2.87, M 4.30, M 4.79, M 4.41

Default-Einstellungen des Herstellers sind zu prüfen und eventuell zu ändern.

Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist technisch zu unterdrücken. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind durch den Administrator zu deaktivieren. M 4.12, M 4.17

Die Firewall ist so zu konfigurieren und zu administrieren, dass sie unseren Sicherheitsbedürfnissen gerecht wird. Es sind die oben genannten Richtlinien zu beachten. M 2.76

Elektronische Datenträger mit vertraulichen Informationen, die nicht weiter benötigt werden, sind vor der Entsorgung sicher zu löschen. Bei der Aussonderung von IT-Systemen ist ebenfalls darauf zu achten, dass keine vertraulichen Informationen mehr zugänglich sind. M 2.167

3.2 Wartung

Der Administrator ist dafür verantwortlich, dass die Informationsverarbeitung möglichst störungsfrei abläuft. Hard- und Softwarekomponenten sind daher ordnungsgemäß zu warten. Die Wartungs- und Reparaturarbeiten sind, sofern möglich, außerhalb der normalen Bürozeiten durchzuführen, wenn diese zu Beeinträchtigungen des laufenden Betriebs führen können. Die Benutzer sind vorab zu informieren. M 2.4

Die mit Pflege und Wartung verbundenen Maßnahmen sind nach Art, Inhalt und Zeitpunkt zu protokollieren. M 2.4, M 4.106

Bei Arbeiten an Diensten mit sensiblen Informationen, ist nach Möglichkeit das Vier-Augen-Prinzip anzuwenden.

Wird Hardware außer Haus gegeben, sind, sofern möglich, alle sensitiven Informationen, die sich auf Datenträgern befinden, vorher sicher zu löschen. Die Übergabe bzw. Transport ist sicher zu gestalten. M 2.218 M 2.167 M 2.44

4 Revision

Alle Systemeinstellungen und Sicherheitsmaßnahmen sind so zu dokumentieren, dass sie für den Vertreter und andere fachkundige Dritte verständlich sind. M 2.25, M 2.34

Alle Fehler und Probleme, die IT-Dienste betreffen, sind zur Kontrolle vom Administrator zu protokollieren. M 2.215 M 2.64

Es ist eine regelmäßige Kontrolle der Funktionalität der IT-Dienste, der IT-Sicherheit und der Einhaltung der Richtlinien durchzuführen. Zu diesem Zweck sind Protokolle zu erstellen. M 2.182

Bei der Protokollierung sind Datenschutz- und Mitbestimmungsaspekte zu beachten. Bei Auswertungen von Protokollen mit personenbezogenen Daten ist das Vier-Augen-Prinzip anzuwenden. M 2.110

5 Zugangs- und Zugriffskontrolle

5.1 Allgemeines

Die Zugangs- und Zugriffsrechte sind vom Administrator einzurichten, zu dokumentieren und vor Manipulationen zu schützen. M 2.7, M 2.8

Der Administrator hat seiner Rolle angepasste Zugangsrechte zu nutzen (Trennung zwischen Administratoren- und Benutzerrechten).

5.2 Passwort-Regelungen

Voreingestellte Passwörter des Herstellers sind sofort zu ändern. M 2.11

(1) Administratoren-Passwort

Die Passwort-Regeln der IT-Benutzer gelten für den Administrator gleichermaßen (siehe Dokument "Sicherheitshinweise für Benutzer"). Für den Vertretungsfall ist das Administratorpasswort versiegelt aufzubewahren. Die Administrator-Passwörter sind mindestens monatlich zu wechseln. M 2.22

(2) Benutzer-Passwort

Der Administrator hat die Passwort-Regeln der IT-Benutzer (siehe Dokument "Sicherheitshinweise für Benutzer") technisch umzusetzen und deren Einhaltung technisch zu unterstützen. M 2.11

Nach Ablauf der Gültigkeit des Passwortes ist der Nutzer vom System automatisch zu sperren. Gleiches gilt, wenn das Benutzerpasswort dreimal falsch eingegeben wurde. Das Entsperren kann nur vom Administrator durchgeführt werden.

Passwörter sind im System zugriffssicher zu speichern, z. B. mittels Einwegverschlüsselung. M 2.11

Vorläufige Passwörter sind den Benutzern auf sichere Art zu übergeben.

6 Kommunikationsspezifische Regelungen

Zur Verschlüsselung ist dem Benutzer auf Antrag ein Programm zur Verfügung zu stellen. M 2.165

Die am Faxgerät eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit beispielsweise Manipulationsversuche frühzeitig erkannt und verhindert werden können.

Des Weiteren ist die "Sicherheitsrichtlinie für die Internetnutzung" (siehe Musterdokument des BSI) zu beachten.

7 Notfallvorsorge

7.1 Virenschutz

Es ist ein Viren-Schutzprogramm zu installieren. Updates sind regelmäßig durchzuführen und die Viren-Signaturen zu aktualisieren. M 4.3, M 2.159

7.2 Datensicherung

Es sind regelmäßige Datensicherungen durchzuführen. Dies hat anhand eines Datensicherungsplans zu geschehen. M 6.32 M 6.33

8 Verhalten bei eingetretenen Störungen

Der Administrator hat bei Verlust der Netz- oder Systemintegrität schnellstmöglich diese Störungen zu beseitigen. M 6.23, M 6.31, M 6.54

Die Ursachen dieser Störungen sind anhand der erstellten Protokolle mit dem IT-Sicherheitsbeauftragten zu analysieren und Verbesserungen zu erarbeiten. Dies ist zu dokumentieren.