Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitshinweise für IT-Benutzer

- Beispiel -

Stand: Juni 2004

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 IT können Bedrohungen für die Institution entstehen. Neben dem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität persönlicher, 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 dem IT-Grundschutzhandbuch des BSI. In der rechten Spalte befinden sich Verweise zu Hintergrundinformationen und zu Maßnahmenvorschlägen innerhalb des IT-Grundschutzhandbuchs. M x.xx

2 Verantwortung

Jeder Benutzer von IT-Diensten ist verpflichtet, geltende, einschlägige Gesetze und interne Regelungen zu beachten. Folgende Richtlinien sind zu beachten (siehe Musterdokumente des BSI): M 3.2

- IT-Sicherheitsleitlinie
- Sicherheitsrichtlinie zur IT-Nutzung
- Sicherheitsrichtlinie zur Internetnutzung

Diese Sicherheitshinweise werden allen Benutzern bekannt gegeben und im Intranet veröffentlicht.

Die Gesamtheit der enthaltenen Regelungen hat verbindlichen Charakter, so dass Verstöße gegen die Inhalte der Richtlinie zu arbeitsrechtlichen Konsequenzen führen können.

Alle Mitarbeiter sind verpflichtet, an angebotenen Schulungen zu Programmnutzung und Sicherheitsmaßnahmen vor der Nutzung von IT-Diensten teilzunehmen. M 3.4 M 3.5

Bei Fragen zur IT-Nutzung und zur IT-Sicherheit stehen die Administratoren und der IT-Sicherheitsbeauftragte zur Verfügung.

3 Allgemeine Regelungen

Die Nutzung der erlaubten Dienste ist ausschließlich zu dienstlichen Zwecken und im ausdrücklich erlaubten Umfang zur Erledigung der Aufgaben gestattet.

Nur freigegebene Software darf verwendet werden. M 2.9

Die Benutzung privater Hard- und Software zu dienstlichen Zwecken ist ohne Genehmigung ist nicht zulässig. M 2.9

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderungen

an der Konfiguration etc.) sind nur durch den Administrator zulässig.

Informationsträger mit sensitiven Informationen sind in aufgestellte Sammelboxen für vertrauliches Schriftgut zu entsorgen oder in einem Shredder zu vernichten. Nicht mehr benötigte Datenträger (Disketten, CD-ROM etc.) sind sicher zu löschen oder zu vernichten. M 2.13

4 Zutritt und Zugang

Es sind die Zugangsregelungen und die vergebenen Berechtigungen zu beachten. Das Ausprobieren, ob weitere Dienste oder Zugriffsrechte als die Erlaubten genutzt werden können, ist verboten.

4.1 Allgemeine Zutritts- und Zugangsregelungen

Der Arbeitsplatz ist „aufgeräumt“ zu hinterlassen, so dass Unbefugte keinen Zugriff auf Informationen und IT-Anwendungen ermöglicht wird. Hierzu sind Räume – sofern möglich – zu verschließen. IT-Geräte sind zum Schutz von unbefugten Personen mit einem passwortgeschützten Bildschirmschoner ausgestattet. Dieser muss bei Verlassen des Arbeitsplatzrechners oder nach 5 Minuten automatisch aktiviert werden. M 2.37 M 4.2

In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen wird.

Die Weitergabe von eigenen Benutzerkennungen und sonstigen Authentisierungshilfsmitteln an Dritte ist unzulässig.

Wenn der Verdacht besteht, dass die eigenen Zugangs- und Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist das Passwort umgehend zu ändern und der IT-Sicherheitsbeauftragte um Rat zu fragen.

4.2 Passwort-Regeln

Folgende Regeln sind zu beachten: M 2.11

1. Passwörter sind nirgends zu notieren und niemandem mitzuteilen.
2. Das Passwort darf nur dem Benutzer bekannt sein.
3. Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.
4. Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind beispielsweise nicht zur Bildung von Passwörtern geeignet. Es dürfen niemals Trivialpasswörter verwendet werden (z. B. 4711; 12345 oder andere nebeneinanderliegende Tasten).
5. Die Passwörter sind spätestens alle 90 Tage zu wechseln.
6. Sofern Gruppenpasswörter zwingend erforderlich sind, gilt: Gruppenpasswörter sind umgehend zu ändern, wenn die Zusammensetzung der Gruppe sich verändert. Gleiches gilt, wenn Passwörter unautorisierten Personen bekannt geworden sind.
7. Einmal genutzte Passwörter sind nicht wieder zu verwenden.
8. Benutzer haben den Empfang von Initial-Passwörtern immer zu bestätigen und müssen diese sofort wechseln.
9. Alle IT-Systeme sind zum Schutz vor unbefugten Personen mit einem passwortunterstützten Bildschirmschoner ausgestattet, dieser ist auch immer zu benutzen.
10. Passwörter dürfen nicht als Teil eines automatischen Anmeldeprozesses zu verwenden, z. B. in einer Makro- oder Funktionstaste.

5 Kommunikationsspezifische Regelungen

Bei der Nutzung von Internet und E-Mail sind Virenschutzprogramme zu nutzen.

Vom Administrator voreingestellte Konfigurationen dürfen nicht vom IT-Benutzer deaktiviert oder geändert werden.

Eine Weitergabe von vertraulichen Informationen bedarf der Zustimmung des Informationseigentümers. M 2.42

Beim Datenaustausch ist eine geeignete Versandart zu nutzen. Die Vertraulichkeit ist beim Versand zu gewährleisten: M 5.23

- E-Mails mit vertraulichem Inhalt, die extern versendet werden, sind zu verschlüsseln.
- Es sind keine vertraulichen Nachrichten auf Anrufbeantworter zu sprechen.
- Die vom Faxgerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.
- Beim Faxversand schutzbedürftiger Dokumente ist ein Sendezeitpunkt mit der Gegenseite abzustimmen. M 5.26
- Ausdrucke mit vertrauliche Informationen sind umgehend aus dem Drucker zu entfernen.

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

6 Notfallvorsorge

6.1 Datenverfügbarkeit

Zur Sicherstellung der Verfügbarkeit ist folgendes sicherzustellen:

i. Daten sind so aufzubewahren, dass sie problemlos wiedergefunden werden können. M 2.258

ii. Um das Risiko eines Datenverlusts zu reduzieren, sind regelmäßig Datensicherungen durchzuführen. M 6.32

6.2 Verschlüsselung

Grundsätzlich sind sensitive Informationen verschlüsselt zu speichern und zu übertragen. Mobile Datenträger sind sicher aufzubewahren. Das gleiche gilt für mobil genutzte IT-Systeme. M 1.36 M 1.33f

6.3 Virenschutz

Jeder elektronische Datenträger (Diskette, Wechselplatte, USB-Stick usw.) ist vor der Verwendung hinsichtlich schadenstiftender Software (z. B. Computerviren) zu untersuchen. M 2.3

E-Mail-Anhängen sind beim Empfang zu überprüfen.

7 Verhalten bei Sicherheitsvorfällen

Die folgenden Verhaltensregeln sind bei den verschiedenen Sicherheitsvorfällen einzuhalten: M 6.23, M 6.31, M 6.54

Sobald ein Fehler oder ein anderes Problem auftritt, ist umgehend der IT-Sicherheitsbeauftragte bzw. ein Administrator zu benachrichtigen. Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird daher immer positiv gewertet! M 6.60

Die Anweisungen des IT-Sicherheitsbeauftragten und der Administratoren sind zu

befolgen.