

③ **Passwörter**

- Vermeiden Sie triviale Passwörter (Namen, Vornamen, Geburtsdaten, ...).
- Schreiben Sie Passwörter nicht auf, da diese den Zugang zu Ihrer Information ermöglichen.
- Verwenden Sie Passwörter, die mehr als 7 Zeichen umfassen. Achten Sie dabei darauf, dass sowohl in den ersten 7 Zeichen wie auch im Rest Sonderzeichen vorkommen.
- Verwenden Sie nicht das gleiche Passwort in unterschiedlichen Sicherheitsbereichen.
- Wechseln Sie Ihre Passwörter in regelmäßigen Abständen.
- Geben Sie Passwörter nie weiter, auch nicht bei vorgegebenen Systemproblemen.

④ **Viren**

- Stellen Sie sicher, dass Ihr Computer bereits vor dem ersten produktiven Gebrauch einen aktiven Virenschutz besitzt.
- Aktualisieren Sie die Virenschutzdateien regelmäßig und automatisch.
- Schalten Sie den Virenschutz nie ab, auch dann nicht, wenn dies als Fehlerbehebung automatisch vorgeschlagen wird.
- Überprüfen Sie fremde Daten über Speicher und über Internet auf Viren, bevor Sie diese verwenden (Quarantänemechanismen).
- Wenn dennoch ein Virus auftritt, nehmen Sie Ihr Gerät vom Netzwerk, schalten Sie es ab und verständigen Sie Ihren Systembetreuer.

⑤ **Sensible Daten**

- Verwahren Sie sensible Daten immer verschlüsselt.
- Wenn Sie die Daten auf Backupmedien unverschlüsselt halten, stellen Sie die geeignete Verwahrung und den Schutz vor Zugriff sicher.
- Bedenken Sie, dass bei Schlüsselverlust verschlüsselte Daten verloren sind.
- Sorgen Sie für ein vertrauenswürdigen Backup verschlüsselter Daten unter einem anderen Schlüssel.
- Beachten Sie Regeln für den Autostart von Datenträgern.
- Betrachten Sie fremde Datenträger und Daten wie unsichere Informationen aus dem Internet.

⑥ **Intranet / Internet**

- Vergewissern Sie sich bei allen Downloads, dass keine ungewollten Programme ausgeführt werden.
 - Achten Sie auf Dateitypen.
 - Kontrollieren Sie Ihre Einstellungen.
 - Laden Sie Programme nur in kontrollierten Umgebungen.
- Achten Sie auf möglichst restriktive Browsereinstellungen.
- Laden Sie von nicht mit SSL gesicherten und freigegebenen Sites nur passive Daten (.html, .txt, .tiff,...).
- Verschlüsseln Sie vertrauliche Daten vor dem Versand.
- Signieren Sie Ihre Mails, damit die Herkunft nachgewiesen werden kann.

⑦ **Laptops**

- Achten Sie auf unbewusstes / unerkanntes Networking (Infrarot, Bluetooth, WLAN) und deaktivieren Sie nicht benötigte Netzwerkkanäle.
- Vermeiden Sie unbeherrschte Services (File- & Printerservice, etc...).
- Aktivieren Sie immer eine persönliche Firewall.
- Verwenden Sie nur die für Ihre Umgebung / Ihren Arbeitsbereich freigegebenen Programme.
- Betreiben Sie Laptops immer im eingeschränkten Benutzermodus. Ein Administratorkonto soll nur in jenen Fällen verwendet werden, wo es unumgänglich ist.
- Beachten Sie die Gefahren der Synchronisation und Datenübernahme aus PDAs und Handys, da hier ausführbare Elemente transferiert werden können.
- Verwenden Sie ein Startpasswort, um Ihre Festplatte zu schützen.
- Verwahren Sie Ihren Laptop immer in geeigneter Weise.
- Lassen Sie Ihren Laptop in öffentlichen Bereichen (Flughafen, Café, Hotel, ...) nie unbeobachtet.
- Verlassen Sie nie ein angemeldetes Gerät ohne den Zugriff zu sperren, auch nicht zum Holen einer Tasse Kaffee.

⑧ **Dokumentenversand**

- Beim Versand von Dokumenten übernehmen Sie Verantwortung:
 - für die Vertraulichkeit
 - für die Sicherheit und Freiheit von schädigenden Elementen
- Achten Sie auf Virenprüfung vor dem Versand.
- Vergewissern Sie sich, dass Dokumente weitergegeben werden dürfen.
- Beachten Sie Kopiereinschränkungen.
- Passwörter, die in Dokumenten vergeben werden, sind in der Regel kein ausreichender Schutz. Verwenden Sie Verschlüsselung bei vertraulichen Dokumenten.
- Verwenden Sie nach Möglichkeit Formate, die keine Änderungen zulassen (z.B. PDF).
- Signieren Sie im elektronischen Versand, damit der Empfänger das Dokument auch vertrauenswürdig öffnen kann.
- Achten Sie auf zulässige Austauschformate und vermeiden Sie nach Möglichkeit Formate, die ausführbare Elemente erlauben.



9 Zutrittskarten / Schlüssel

- RF-Schlüssel (kontaktlose Karten, elektronische Schlüssel, etc...) können Aufschluss über die Identität und Rollen liefern. Beachten Sie die Aufbewahrungsvorschriften sorgfältig.
- Nehmen Sie Schlüssel und Zutrittskontrolltags nicht in die Freizeit mit. Lassen Sie diese nicht im Auto liegen.

Melden Sie jeden Verlust von Schlüsseln oder Zutrittskarten unverzüglich.

10 Was tun, wenn tatsächlich etwas vorfällt?

- Entscheiden Sie zuerst, wo Gefahr in Verzug ist - nur in diesen Bereichen sind Notmaßnahmen ohne externe Hilfe gerechtfertigt.
- Verständigen Sie unverzüglich alle Zuständigen - Systemadministratoren, Vorgesetzte, Verantwortliche für Warnsysteme, Hausverwaltung, etc.
- Protokollieren Sie den gesamten Hergang.
- Trennen Sie alle betroffenen Geräte vom Netzwerk.
- Achten Sie auf fachgerechte Datensicherung.
- Führen Sie keine Startversuche von betroffenen Geräten durch.

Achten Sie darauf, dass die größeren Schäden oft durch voreiliges Handeln entstehen.



Unterschätzen Sie nicht die Bedrohungen Ihrer Infrastruktur und Ihrer Informationen

- In den allermeisten Fällen führt eigenes, unachtsames Verhalten zu Schäden.
- Viren können großen Schaden oder sogar totalen Datenverlust zur Folge haben.
- Datenträger und Dokumente können gestohlen werden.
- Geknackte und gestohlene Passwörter öffnen Unberechtigten den Zugang zu sensiblen Informationen und Gebäuden.
- Telefonleitungen und Internetverbindungen können angezapft werden.

Die Folgen von Sicherheitsverletzungen können schwerwiegend sein, beachten Sie daher die Regeln genau.

? Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

www.a-sit.at

2007-11



IT-Sicherheit am Arbeitsplatz

10 Grundsätze bei der Verwendung des Computers in der Arbeit

- Ihr Computer
- Peripherie
- Passwörter
- Viren
- Sensible Daten
- Intranet / Internet
- Laptops
- Dokumentenversand
- Zutrittskarten / Schlüssel
- Und wenn etwas passiert?

1 Ihr Computer

- Stellen Sie Ihren PC wenn möglich so auf, dass Unberechtigte keine Einsicht in sensitive Informationen erhalten.
- Aktivieren Sie immer einen Bildschirmschoner. Achten Sie darauf, dass dieser nur mit Passwort entsperrt werden kann.
- Lagern Sie sensitive Informationen auf entfernbaren Datenträgern und versperren Sie diese immer, wenn Sie nicht an Ihrem Arbeitsplatz sind.
- Im Zweifelsfall beenden Sie das System, wenn Sie Ihren Arbeitsplatz verlassen.
- Achten Sie auf geeignete Verwahrung von Daten, deren Verlust Ihnen schaden könnte.

2 Peripherie

- Lassen Sie externe Datenträger (z.B. USB-Sticks) nie unkontrolliert benutzen.
- Verwenden Sie Quarantänemechanismen bevor Sie Datenträger, die mit anderen Rechnern in Kontakt waren, weiter verwenden. Wo immer möglich verwenden Sie „read only“ Modes.
- Aktivieren von Druckern kann exekutierbare Elemente enthalten und soll daher nur in kontrollierten Umgebungen stattfinden.
- Drucken Sie sensitive oder vertrauliche Informationen nur in Ihrer Gegenwart. Entsorgen Sie Fehldrucke und Fehlkopien.
- Verwenden Sie Aktenvernichter selbst, um Missbrauch von Dokumenten zu verhindern.