



5 SICHERHEIT

Die Aufbereitung der Informationen und die Speicherung dieser Daten sind der wesentliche Teil der Datenverarbeitung. Das ist kostspielig und, wenn es sich um sensible Daten handelt – verantwortungsvoll.

Bei komplexen Systemen wie es Computer und Netzwerke sind, ist es unmöglich, alle Risiken völlig auszuschließen. Man kann diese Gefahren jedoch auf ein Minimum reduzieren. Im Bereich der Datenverarbeitung und Datenarchivierung sind 2 wesentliche Faktoren unterscheidbar:

- Sicherheit, dass Daten nicht missbräuchlich abgerufen oder verwendet werden.
- Sicherheit der Information vor Zerstörung bzw Verlust.

Bewusstseinsbildung der Anwender

Ein erster Schritt, Daten vertraulich zu behandeln und fehlerhaftes Hantieren zu vermeiden, ist die Unterweisung und Schulung der Anwender. Nur wenn man sich der Gefahren bewusst ist, wird man die nötige Sorgfalt aufbringen.

5.1 Identität/ Authentifizierung

Zugriffsberechtigung

Jene Bereiche, in denen sich sicherungswürdige Daten befinden, sollen durch entsprechende Sicherheitsmaßnahmen gegen Fremdzugriff gesperrt sein. Personen, die mit den entsprechenden Daten oder mit der Bedienung der Hardware nicht beauftragt sind, wird der Zugriff verwehrt. Das gilt sowohl für den Eintritt in die EDV-Zentrale als auch für den Zugriff auf den Computer und das Öffnen von Dateien.

Einstieg in SoftCard-Rechnungswesen



5.1.1 Wissen, dass aus Sicherheitsgründen eine Benutzeridentifizierung (User-ID) und ein Kennwort erforderlich sind, wenn ein Benutzer auf einen Computer zugreifen möchte

Der Eintritt in verschlossene Räume erfolgt mittels Schloss und dazugehörigem Schlüssel. Der Zugriff auf Daten in einem Computer erfolgt durch die Identifizierung der Person und der Verwendung des Kennwortes dieser Person.

Zugangskontrolle im Betriebssystem

Fast alle Betriebssysteme bieten eine sichere Zugriffskontrolle durch Benutzerregistrierung. Der Administrator legt für jede Person, die in das System einsteigen darf, ein Benutzerkonto an. In diesem wird festgehalten, welche Rechte der jeweilige Benutzer hat und mit welchem Kennwort (Passwort) er sich beim Einstieg identifizieren muss. Ist die Person, die den Computer benutzen will, nicht registriert oder wird ein falsches Passwort verwendet, dann ist kein Computerzugang möglich.

Zugriff auf Daten

In gleicher Weise erfolgt auch die Freigabe von Datenträgern, Ordnern und Dateien. Je nach Betriebssystem und Anwendungsprogramm können für die einzelnen Elemente unterschiedliche Passwörter vergeben werden und die dazu festgelegte Berechtigung kann sich auf das Öffnen, das Kopieren, das Bearbeiten usw. beschränken.



5.1.2 Über gute Kennwort-Strategien Bescheid wissen wie: Kennwort nicht für mehrere Zwecke nutzen, Kennwörter regelmäßig ändern, angemessene Länge der Kennwörter, angemessene Zusammensetzung aus Buchstaben und Ziffern

Kein Sicherheitsmechanismus nützt etwas, wenn sich eine andere (nicht berechnete) Person unter dem Namen der berechtigten Person in das Computersystem einloggt (anmeldet). Daher verlangen Dienstleistungen im Internet fast immer, dass der Benutzer sich authentifiziert. Dies geschieht durch die Eingabe eines Benutzernamens und eines geheim zu haltenden Passworts. Das Passwort besteht aus einer Kombination von Buchstaben und Zeichen, die Sie sich meist selbst aussuchen können - was bedeutet, dass Sie auch ein sehr schlechtes Passwort wählen können. Daher sollten Sie dringend einige Regeln beachten, damit die Schutzfunktion des Passworts auch greift. Je nach



Betriebssystem und Programm können unterschiedliche Schreibweisen von Passwörtern erlaubt sein.

Einige Tipps für Passwörter

- Das Passwort muss einfach genug sein, dass Sie es sich merken können - und zugleich kompliziert genug, dass es niemand erraten kann.
- Bilden Sie Ihre Passwörter aus mindestens sechs Zeichen.
- Kombinieren Sie Buchstaben und Zahlen; unterscheiden Sie Groß- und Kleinschreibung.
- Benutzen Sie keine aufeinanderfolgenden Zeichen wie "abcdefg" oder Wörter, die in einem Lexikon vorkommen können.
- Verwenden Sie auf keinen Fall unverändert den Namen Ihres Lebenspartners, Haustiers, Ihren Wohnort oder ähnliches!
- Benutzen Sie nicht Ihren Benutzernamen (Login) auch als Bestandteil des Passworts.
- Verwenden Sie für verschiedene Konten (für E-Mail, Online-Banking, Terminkalender) verschiedene Passwörter.
- Wechseln Sie das Passwort von Zeit zu Zeit.

Gute und schlechte Passwörter

Mit wenigen kleinen Änderungen machen Sie aus einem schlechten ein gutes Passwort:

schlecht	gut
Theresia (Name der Mutter)	Theres1A
Achterbahn (Begriff aus dem Lexikon)	8-erBahn
Mausilein(häufiger Kosenamen)	M@usiLein
Wolfgang (Ihr Name)	WoGangLf

Wo soll ich Passwörter aufbewahren?

Neben dem Aufbau eines Passwortes ist die richtige Aufbewahrung entscheidend.

- Speichern Sie wichtige Passwörter nicht auf dem Rechner, da sie dort für elektronische Angreifer (Trojaner, Hacker-Angriffe) zugänglich sein könnten.
- Wenn Sie sich Passwörter aufschreiben, verwahren Sie den Notizzettel an einem Ort, der nicht jedem zugänglich ist.
- Geben Sie keine Passwörter an Dritte weiter. Und wenn das unumgänglich war, dann ändern Sie es danach sofort!



5.2 Datensicherheit

Neben dem Risiko, dass Daten von nicht berechtigten Personen abgerufen oder verändert werden, besteht auch die Gefahr, dass Daten zerstört werden oder verloren gehen. Die Gründe sind vielfältig:

Grund	Wirkung
Schadhafte Hardware	Datenträger weist Fehler auf – Daten können nicht mehr gelesen werden. Stromausfall löscht den Arbeitsspeicher.
Virenattacken	Auf dem Rechner setzt sich ein Virus fest, der die Dateien zerstört.
Fehlbedienung durch Anwender	Eine bearbeitete Datei wird nicht gespeichert. Ein leeres Dokument wird mit dem Namen einer bestehenden Datei gespeichert. Ganze Absätze eines Dokuments werden versehentlich gelöscht.

Um Datensicherheit zu gewährleisten, können vorbeugende Maßnahmen ergriffen werden.

Vorbeugung

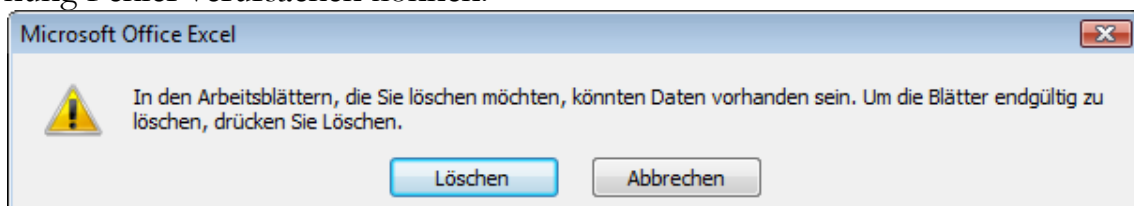
Eine **unterbrechungsfreie Spannungsversorgung (USV)** kann Störungen im Stromnetz ausgleichen und gibt bei totalem Stromausfall durch den integrierten Batteriepuffer noch genügend Zeit, alle Anwendungen ordnungsgemäß zu beenden.



Virenschutzprogramme (**Virens Scanner**) verhindern das Eindringen von Viren durch virusbefallene Dateien, wie sie zB im Anhang von E-Mails sein können.

Eine **Firewall** kann den Zugriff von außen verhindern, wodurch es Hackern nicht möglich ist, auf Daten des Computers zuzugreifen.

Sicherheitsabfragen in den Programmen warnen vor dem Schließen der Datei, diese vorher zu speichern, oder vor Aktionen, die bei irrtümlicher Bedienung Fehler verursachen können.





Datensicherung

Die Daten eines Computers, sowohl Programme als auch die Anwenderdateien, sollen laufend gesichert werden. Sicherung bedeutet, die Dateien werden auf einen anderen Datenträger kopiert (Backup) und bei Bedarf kann mit dieser Kopie der ursprüngliche Datenbestand wieder hergestellt werden (Restore).

Zur Datensicherung eignen sich alle Datenträger, deren Speicherkapazität dem zu sichernden Datenvolumen entspricht.

Im privaten Bereich kann das ein USB-Stick oder eine externe Festplatte sein. Programmdateien (zB die Sicherung des Betriebssystems oder der Office-Programme) können auf eine DVD kopiert werden, die dann auch gleich für die Neuinstallation verwendet werden kann. Beachten Sie dazu jedoch die Lizenzbedingungen des Programmherstellers – siehe Punkt 6.1.3)

Anwender, die ein Netzwerk betreiben, werden ihre Daten auf einen Rechner im Netz überspielen, der von den anderen Computern räumlich getrennt ist - in der Hoffnung, nicht alle Rechner fallen einem Brand zu Opfer. Siehe dazu auch Online-Datenspeicherung Punkt 1.3.3, Seite 25.

5.2.1 Die Bedeutung der Aufbewahrung von Sicherungskopien (Backup) von Dateien an einem anderen Ort kennen

Im Schadensfall von Brand oder Hochwasser sind jedoch auch die Sicherungsdaten gefährdet. Deshalb sollte der Aufbewahrungsort dieser Datenträger gut gewählt werden. Je nach Wichtigkeit der Daten und der Kosten, die durch eine Wiederherstellung anfallen, wird der Lagerort ausgewählt.

Größere Unternehmen und Rechenzentren sollten sich speziell gesicherte Safes oder Räumlichkeiten zur feuersicheren Unterbringung der Sicherungsdatenträger einrichten. Eine zusätzliche Sicherheit ergibt sich aus der Verteilung der Sicherungsdaten auf verschiedene Standorte.

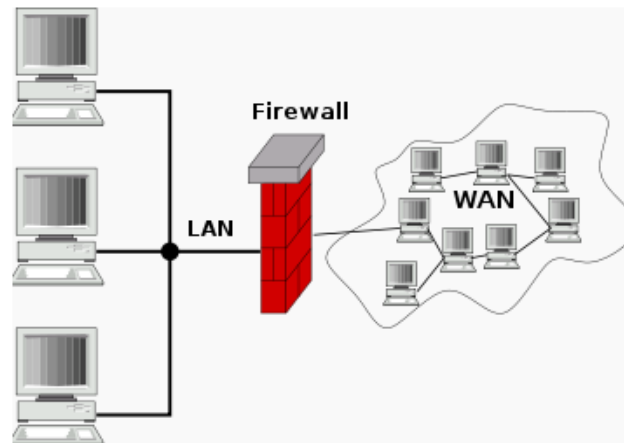
5.2.2 Den Begriff Firewall kennen

Als Firewall bezeichnet man Hardware oder Software, die die aus einem Netzwerk - speziell aus dem Internet - eingehenden Daten überprüft und dann je nach den gewählten Einstellungen blockiert oder zum Computer weiterleitet. Sie kann damit verhindern, dass Hacker Zugriff auf einen Computer erlangen.

Dieser Schutz kann in Form eines eigens konzipierten Servers erfolgen oder als Software am jeweiligen Rechner installiert sein.



In den Betriebssystemen Windows Vista und Windows 7 ist bereits eine Firewall integriert.



5.2.3 Über die Möglichkeiten zur Vermeidung von Datendiebstahl Bescheid wissen wie: eine Benutzeridentifizierung und Kennwort verwenden, Computer und weitere Hardware mit einem Sicherungskabel abschließen

In der heutigen Informationsgesellschaft haben gespeicherte Daten besonderen Wert. Sie zu erfassen, kostet Zeit, Geld und vor allem das nötige Wissen, das in den Daten steckt. Es ist daher oft nicht der Verlust der Hardware (Laptop, PDA oder Mobiltelefon) das wirkliche Übel, sondern die Wiederbeschaffung der Daten sowie der Schaden, der durch die missbräuchliche Verwendung dieser abhanden gekommenen Daten entstehen kann.

Diese Gefahr droht vorrangig durch Verlust bzw. Diebstahl der Hardware samt den darin gespeicherten Daten.

Vorkehrungen

- EDV-Geräte sollen niemals im abgestellten Fahrzeug zurückbleiben – womöglich noch gut sichtbar.
- Laptops können durch ein Sicherungskabel an einem fixen Gegenstand (Tischfuß) angebunden werden.
- Der Zugang (Login und Öffnen von Dateien) ist nur über die Benutzeridentifikation und ein Kennwort möglich.
- Besonders sensible Daten können verschlüsselt gespeichert werden.
- Daten sollen laufend gesichert werden.
- Manche Versicherungsverträge decken auch die Wiederherstellung der Daten.



Schadensfall eingetreten! Was tun wenn

- das Gerät Teil eines Netzwerks ist?
Den Administrator (Internetprovider, Telefonbetreiber) kontaktieren, um den Zugang zu sperren bzw die Zugangsberechtigung neu zu konfigurieren.
- im Gerät Kennwörter gespeichert wurden?
Alle Kennwörter, PIN, TAN sofort ändern oder sperren lassen.

5.3 Viren

Im landläufigen Sinn wird alles, was Schaden verursacht, als Virus bezeichnet. Erst bei genauerer Analyse werden die Unterschiede erkennbar. Allgemein gültig ist jedoch die Vorsicht, mit der der Anwender dem Thema gegenüberstehen soll:

- Anwender sollten niemals unbekannte Dateien oder Programme aus unsicherer Quelle ausführen. Das gilt insbesondere für Dateien, die per E-Mail empfangen wurden. Solche Dateien – auch harmlos erscheinende Dokumente wie Bilder oder PDF-Dokumente – können Schadprogramme aktivieren.
- Durch die Autostartfunktion für CD-ROMs und DVD-ROMs können Programme bereits beim Einlegen eines solchen Datenträgers ausgeführt und damit ein System infiziert werden.
- Alle Dateien, die aus dem Internet heruntergeladen werden, sollten mit einem aktuellen Antivirenprogramm überprüft werden.
- Betriebssystem und Anwendungen sollten regelmäßig aktualisiert werden und die vom Hersteller bereit gestellten Service Packs eingespielt werden.



<http://bauwiki.tugraz.at>



5.3.1 Den Begriff Computer-Virus verstehen

Ein **Computer-Virus** ist ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust. Wenn dieses Programm einmal gestartet wird, kann es Veränderungen am Status der Hardware (zum Beispiel Netzwerkverbindungen), am Betriebssystem (Bootviren) oder an der Software vornehmen (Löschen oder Beschädigen von Dateien). Computerviren können die Computersicherheit beeinträchtigen und zählen zur Malware (schädliche Software).

Bezeichnung	Wirkung
Computerviren	
Virus	Ein einfacher Virus wird durch Aufruf des Programmes, in dem er sich eingenistet hat, aktiv. Er verbreitet sich auch auf andere Dateien und innerhalb des Netzwerkes.
Wurm	Die Wirkung entspricht dem eines einfachen Virus. Er verbreitet sich allerdings selbstständig beispielsweise über das Adressmaterial für E-Mails. Dazu nutzt er die Sicherheitslücken des Betriebssystems.
Trojaner	Programme, die in das Computersystem eingeschleust werden und im Hintergrund ohne Wissen des Anwenders eine andere Funktion, meist zum Schaden des Anwenders, erfüllen. Mit solchen Programmen kann der <i>Hacker</i> Passwörter oder Tastatureingaben herausfinden, um damit einen Zugang in den Computer, aber auch auf Bankkonten des Anwenders zu erlangen.
Sonstige Gefahren im Internet	
Hoax	Wörtlich ein Scherz oder Falschmeldung; Meistens erfolgt eine derartige Scherz- oder eine Falschmeldung mittels E-Mail. Sie gibt bekannt, dass ein Virus unterwegs sei und fordert den Anwender auf, etwas zu tun. Ein Hoax soll meist nur erschrecken.
Phishing	Bei Phishing handelt es sich bereits um Betrug. Der Empfänger der E-Mail wird auffordert, persönliche Daten, Kontonummern, Anmeldedaten für das Onlinebanking, per E-Mail oder über eine gefälschte Website bekannt zu geben. Über E-Mail werden Sie zu strafbaren Handlungen verleitet (Geldwäsche).
Dialer	Programm, das über das Telefonnetz einen Internetzugang öffnet. Schädlich sind diese Programme nur dann, wenn sie ohne Wissen des Anwenders kostenpflichtige Telefonnummern anwählen. Der Schaden entspricht den Kosten, die diese Anrufe verursachen.



5.3.2 Wissen, wie Viren in ein Computersystem eindringen können

Verwenden Sie keinen Computer! Nur damit sind Sie sicher, jemals einen Computervirus einzufangen. Dieser Ratschlag ist hier wohl nicht umsetzbar. Doch man kann die Gefahr minimieren. Dazu ist es wichtig zu erkennen, wie Viren oder andere Malware auf einen Computer kommen.

- Durch Öffnen von (unbekannten) Dateien
- Zugriff auf Internet-Websites
- Download und Installation von Programmen
- Durch Würmer, die sich selbst verbreiten
- Sollte auch nur ein leiser Verdacht aufkommen, dass sich ein Virus eingemischt hat, dann isolieren Sie diesen Rechner
 - Trennen Sie die Verbindung zu anderen Computern (Netzwerk)
 - Trennen Sie die Verbindung zum Internet (Modem)
 - Geben Sie keine Dateien mehr an andere User weiter (USB-Stick, selbst erstellte CDs)

5.3.3 Maßnahmen gegen Viren kennen und wissen, wie wichtig die regelmäßige Aktualisierung der Anti-Viren-Software ist

Um den Computer vor Viren zu schützen, ist es zweckmäßig, ein

- Antivirenprogramm und eine
- Firewall auf dem Rechner einzurichten.

Die *Firewall* meldet den Versuch, dass von außerhalb auf den Computer zugegriffen wird (hilft gegen das Einschleusen von Würmer und Trojaner).

Das *Antiviren-Programm* durchleuchtet (scannt) alle Dateien bevor sie aus dem Internet heruntergeladen und geöffnet werden. Aber: verwenden Sie es auch – selbst dann, wenn der Computerstart und das Öffnen der E-Mail-Anhänge (Attachment) dadurch verlangsamt wird.

Täglich werden weltweit neue Schadprogramme entwickelt. Daher ist es auch erforderlich, dass das installierte Antivirenprogramm laufend aktualisiert wird. Die Hersteller dieser Programme bieten daher über das Internet eine automatische Aktualisierung ihrer Programme an, so dass der Anwender automatisch immer mit der neuesten Version des Programms arbeiten kann.

