

1 2.4.1.2. Datensicherheit im Lehrbetrieb

1.1 Allgemein

Die Datensicherheit bezeichnet Eigenschaften, welche die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicherstellen. Datensicherheit dient dem Schutz vor Gefahren und Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken.

Private und öffentliche Unternehmen sind heute in allen Bereichen ihrer Geschäftstätigkeit auf IT-Systeme angewiesen. Die Datensicherheit stellt einen Baustein des Risikomanagements einer Unternehmung dar.

Folgende Bedrohungen sind vorstellbar:

- Technischer Systemausfall
- Systemmissbrauch
- Sabotage
- Spionage
- Betrug und Diebstahl

1.2 Massnahmen

Um Schäden aus mangelhafter Datensicherheit zu verhindern oder zumindest zu minimieren, können verschiedene Massnahmen ergriffen werden.

1.2.1 Management

Die Datensicherheit ist grundsätzlich Aufgabe der Geschäftsleitung eines Unternehmens, die Sicherheitsrichtlinien aufstellen sollte. Weitere Aufgabe des Managements ist die Installation eines Sicherheits-Managementsystems. Dieses ist für die operative Umsetzung und Kontrolle zuständig, sorgt also dafür, dass die getroffenen Sicherheitsrichtlinien von allen eingehalten werden.

1.2.2 Software aktualisieren

Für viele Programme werden Aktualisierungen angeboten. Diese bieten teilweise nicht nur erweiterte oder verbesserte Funktionen, sondern beheben häufig auch schwere Sicherheitslücken. Besonders betroffen sind Programme, die Daten mit dem Internet austauschen. Die Aktualisierungen sollten so schnell wie möglich auf den entsprechenden Rechnersystemen installiert werden. Viele Programme bieten eine automatische Funktion an, die die Aktualisierung im Hintergrund ohne das Eingreifen des Benutzers vollzieht. Bei grösseren Unternehmen mit Systemadministratoren können diese Updates ohne Einschränkungen des Betriebs über Nacht installiert werden.

1.2.3 Antiviren-Software verwenden

Wenn Daten aus dem Internet oder von Mailservern heruntergeladen oder von Datenträgern kopiert werden, besteht immer die Möglichkeit, dass sich schädliche Dateien darunter befinden. Aus diesem Grund sollte man nur Dateien öffnen, welchen man vertraut und die bereits bekannt sind. Ansonsten sollte unbedingt ein Antiviren-Programm installiert sein, welche die schädlichen Dateien schnell erkennt und entfernen kann. Auch hier ist darauf zu achten, dass die Antiviren-Software auf dem neuesten Stand ist.

1.2.4 Diversifikation der Software

Eine weitere Massnahme zur Reduktion der Gefahren besteht in der Diversifizierung von Software, also darin, Software von verschiedenen, auch nicht marktführenden Anbietern zu

Lernender.ch

verwenden. Die Angriffe zielen oftmals auf Produkte von grossen Anbietern wie zum Beispiel Microsoft, da die Angreifer damit den grössten Erfolg einfahren können.

1.2.5 Firewalls verwenden

Für Angriffe, die ohne eine aktive Handlung des Nutzers drohen, ist es unerlässlich, eine Firewall zu installieren. Viele unerwünschte Zugriffe auf den Computer und unbeabsichtigte Zugriffe vom eigenen Computer, die vom Benutzer meist gar nicht bemerkt werden, können auf diese Weise verhindert werden.

1.2.6 Eingeschränkte Benutzerrechte

Der Systemadministrator kann tiefgehende Änderungen an einem Computer durchführen. Moderne Betriebssysteme verfügen daher über die Möglichkeit, Benutzerrechte einzuschränken, so dass zum Beispiel Systemdateien nicht verändert werden können.

1.2.7 Aktive Inhalte deaktivieren

Bei aktiven Inhalten handelt es sich um Funktionalitäten, die die Bedienung eines Computers vereinfachen sollen. Das automatische Öffnen beziehungsweise Ausführen von heruntergeladenen Dateien birgt jedoch die Gefahr, dass diese den Rechner infizieren. Um dies zu vermeiden sollten aktive Inhalte wie zum Beispiel ActiveX oder JavaScript soweit wie möglich deaktiviert werden.

1.2.8 Sensible Daten verschlüsseln

Daten, die nicht in die Hände Dritter gelangen sollen, müssen durch geeignete Massnahmen verschlüsselt werden. Ein Zugriff auf die Inhalte darf nur dann möglich sein, wenn die Beteiligten über den richtigen Schlüssel verfügen. Besonders gefährdet sind unverschlüsselte, kabellose Netze wie zum Beispiel WLANs, da hierbei Unbefugte unbemerkt Zugriff auf die Daten und sogar die Kontrolle über den ungeschützten Computer erlangen können.

1.2.9 Sicherungskopien erstellen

Von jeder wichtigen Datei sollte mindestens eine Sicherungskopie auf einem getrennten Speichermedium angelegt werden. Hierzu gibt es zum Beispiel Backup-Software, die diese Aufgaben regelmässig und automatisch erledigt.

1.2.10 Protokollierung

Automatisch erstellte Protokolle oder Log-Dateien können dabei helfen, zu einem späteren Zeitpunkt zu ermitteln, wie es zu Schäden an einem Rechnersystem gekommen ist.

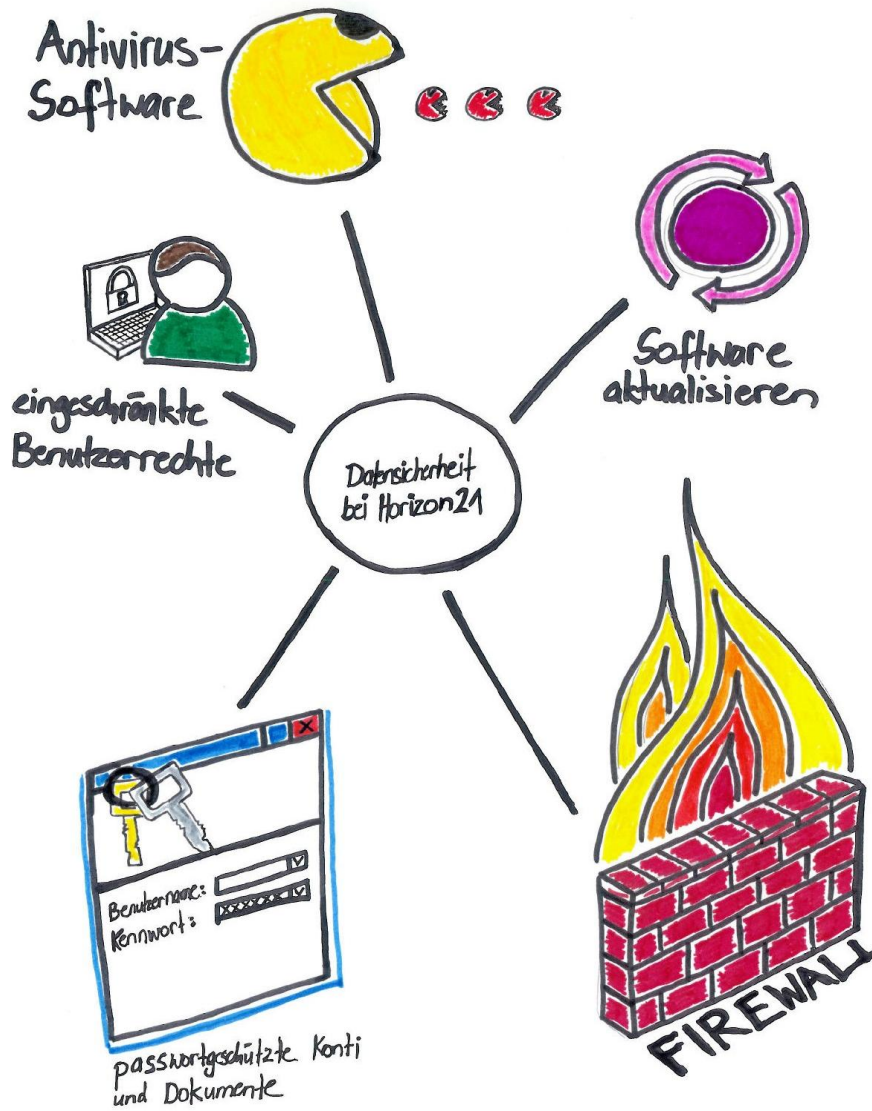
1.2.11 Sensibilisierung und Ausbildung der Mitarbeiter

Ein wichtiger Aspekt in der Umsetzung der Sicherheitsrichtlinien ist die Miteinbeziehung der eigenen Mitarbeiter. Auch die besten Schutzmassnahmen nützen nur begrenzt, wenn die Mitarbeiter selber nicht wissen, wie mit Gefahrensituationen umzugehen ist. Die Mitarbeitersensibilisierung variiert von Unternehmen zu Unternehmen von Veranstaltungen über webbasierte Seminare bis hin zu ganzen Kampagnen in grösseren Betrieben.

1.2.12 Überprüfung der Massnahmen

Um ein gewisses Mass an Datensicherheit zu gewährleisten, ist die regelmässige Überprüfung der getroffenen Massnahmen Pflicht.

1.2.13 Instrumente zum Schutz von Daten vor unberechtigten Zugriffen



Schematische Illustration 1: Schutz vor unberechtigten Zugriffen