Theorie Kapitel 2 Lektion 2
Informationssicherheit

- Daten- und Informationssicherheit
- Sicherungskopien

✓ Wenn die Daten einerseits sicher vor fremden Zugriffen sein sollen, wie wird dann Informationssicherheit im Unternehmen so gewährleistet, dass die Mitarbeiter und Mitarbeiterinnen auf die Daten noch zugreifen können? Das ist Thema dieser Lektion.

Aufgabe

1. Daten- und Informationssicherheit

Was muss sichergestellt werden:

- Der Datenschutz personenbezogene Daten und
- die Informationssicherheit der vertraulich zu behandelnden Firmendaten.

Wie wird die Sicherheit erreicht

- Mitarbeitende sensibilisieren
  Sind sich die Mitarbeitenden darüber im Klaren, was Datenschutz und Informationssicherheit bedeuten? Das Spektrum reicht von Manipulation der Daten, zu späte Verfügbarkeit, unzulässige Verwertung und Fahrlässigkeit bis hin zu Preisgabe von Informationen durch Gutgläubigkeit.

- IT-Sicherheit
  Geeignete Sicherheitstechniken sind Firewalls, Zugriffsschutz durch Passwörter, Verschlüsselung der Daten beim Speichern und eingeschränkte Benutzerrechte. Verwenden Sie Anti-Viren-Programme und senden Sie vertrauliche Daten nur verschlüsselt per E-Mail.

  Firewalls verhindern den Zugriff auf das System von Personen außerhalb. Sie überwachen die Verbindung zwischen zwei Netzen.

  Passwörter haben Sinn, wenn Sie ausreichend lang, nicht leicht zu erraten oder gar von Notizzetteln abzulesen sind. Verwenden Sie also keine Kosenamen oder Geburtsdaten. Sichere Passwörter setzen sich zusammen aus einer Kombination von Buchstaben (Groß- und Kleinschreibung verwenden), Ziffern und sogar einigen Sonderzeichen.

  Passwörter für sensible Daten werden am besten in bestimmten Abständen geändert.

  Passwörter werden schnell von Programmen herausgefunden. Je länger das Passwort, zusammengesetzt aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, je länger dauert und es, das Passwort herauszufinden. Recherchieren Sie beispielsweise unter http://de.wikipedia.org/wiki/Brute-Force-Methode.

Einen Zugang zu hacken hat einer meiner Teilnehmer bei Daten seines Chefs sehr einfach realisiert:

Der Chef hatte alle Passwörter in einer Excel-Datei gespeichert. Die Datei war mit einem Kennwort gesichert, das machte den Teilnehmer stutzig. Als Kennwort gab der reiselustige Chef eines seiner Lieblingsreiseziele ein. Mein Teilnehmer musste nicht einmal ein Programm nutzen, um an die Passwörter zu gelangen.

(Er hat natürlich nichts damit gemacht, sondern den Chef auf sein leicht zu knakkendes Kennwort angesprochen - ethisches Hacking sozusagen.)

Eingeschränkte Benutzerrechte erlauben das Arbeiten mit den Programmen, regeln den Zugriff zu Firmeninformationen und lassen das Recht, tiefgreifende Änderungen am Computer durchzuführen, in der Systemadministration.

Verschlüsseln Sie vertrauliche Daten, zB Identifikationsnummern (PIN) oder Transaktionsnummern (TAN), beim Versenden an einen anderen Computer. Verschlüsseln schützt sensible Daten auch auf einem externen Datenträger.

- **Sicherheitsrichtlinien**
  Halten Sie die Sicherheitsrichtlinien ein und erstellen Sie einen Notplan: Wer soll nach Störungen informiert werden und wie soll weiter gearbeitet werden.
- **Datensicherung mit Sicherungskopien**
  Erstellen Sie von jeder Datei, die wichtig ist, mindestens eine Sicherungskopie. Beschriften Sie die Kopie. Bewahren Sie die Sicherung getrennt vom Original auf, evtl. in einem feuerfesten Safe. Firmendaten werden meist am Ende eines Arbeitstages komplett gesichert. Der Fachbegriff dafür lautet **Backup**.

Beachten Sie bei Notebooks
Flexibles Arbeiten an unterschiedlichen Orten macht Notebooks bzw. Laptops zu unersetzlichen Begleitern. Sensible Unternehmens- und Kundendaten entziehen sich damit jedoch der Zugriffskontrolle durch das Unternehmen. Dabei sind gerade Daten, die von den Mitarbeitenden selber mit mobilen Geräten nach außen getragen werden, besonders leicht zu entwenden oder zu sabotieren.

- Schützen Sie sich vor Diebstahl des Gerätes mit speziellen Sicherheitsschlössern, so genannten *security cables*.
- Vergeben Sie sowohl zum Anmelden am Laptop ein Kennwort als auch zum Einwählen in das firmeninterne Netzwerk.
- Besonders sensible Daten sollten Sie verschlüsseln.

2. Sicherungskopien[1]

Disketten sind Auslaufmodelle. Sie eignen sich für kleinere Dateien. Die Speicherkapazität einer Diskette beträgt 1,44 MB. Sie sind empfindlich gegen Hitze, Strahlung und Feuchtigkeit.

CDs oder **DVDs** eignen sich für größere Datenmengen, wie zum Beispiel Bilder. Die Speicherkapazität einer CD beträgt zwischen 650 und 800 MB. Auf eine DVD brennen Sie sogar Filme. Achten Sie auf eine staubfreie Lagerung in den mitgelieferten Hartplastikhüllen.

Streamer Tapes oder **Magnetbänder** vergleichen Sie mit den „alten" Musik-Kassetten oder Tonbänder. Sie speichern so viel, wie das Band lang ist, zB 200 MB.

Festplatten speichern dzt. bis zu 4 TB (Terabyte). Sie eignen sich für große Datenmengen, dabei werden externe Festplatten schnell an andere Rechner angeschlossen.

In **Netzwerken** von Firmen wird meist ein *Backup* des gesamten Datenbestandes auf eigenen *Servern* erstellt. Die Datenbankadministration kümmert sich darum.

---

[1] *Mehr Informationen zu Speichermedien finden Sie ab Seite 56.*

Im **Internet** lagern Sie Ihre Daten ebenso. Das bringt den Vorteil, dass Sie mit Internetzugang von überall auf der Welt auf Ihre Daten zugreifen.

Ein klassisches Beispiel für eine Strategie zur Datensicherung
In einem Büro erstellen 10 Mitarbeitende umfangreiche Berichte und Kalkulationen. Diese Daten werden laufend am Server gespeichert. Jede Nacht wird ein Backup auf Magnetband erstellt. Es gibt 8 Bänder für Mo, Di, Mi, Do, Fr1, Fr2, Fr3 und Fr4. Die Wochentage werden überspielt, Freitage erst alle 4 Wochen - somit ist der Datenbestand immer greifbar. Wichtige Dateien und Verträge werden zusätzlich auf CDs gebrannt und im Safe aufbewahrt. Sinnvoll ist es wohl, wichtige Daten sofort zu sichern.

Beachten Sie
Es ist leicht, Viren zu programmieren. Recherchieren Sie einmal mit einer Suchmaschine - Sie finden Bausteine zum Downloaden! Das ist gratis und für alle zugänglich. Wenn Sie ein System absolut sicher halten wollen, dürfen Sie den Rechner nie mit einem anderen Computer verbinden oder fremde Daten verwenden. Aber gerade die Vernetzung ist es, aus der wir Erfolge ziehen, ergo wollen wir die Systeme nicht abkapseln. Halten Sie den Aufwand, Ihr System zu infizieren, so groß, dass es sich für kriminelle Personen einfach nicht lohnt. Aktualisieren Sie Ihre Software, so werden Sicherheitslücken geschlossen und verwenden Anti-Viren-Software.

Ein vereinfachter Ablauf sieht so aus:

1. Ein Programmierer erstellt ein kleines Programm.
2. Das Programm wird an den Anfang eines anderen Programms gestellt.
3. Beim Aufrufen wird zuerst das Virenprogramm ausgeführt.
4. Es sucht auf der Festplatte nach noch nicht infizierten Programmen.
5. Bei jedem weiteren infizierten Programm wird zuerst das Virusprogramm aktiv.

Übung

1. Finden Sie ein sicheres Passwort.

Testen Sie Ihr Wissen

1. Wie oft sollte eine Bank Daten sichern?
2. Wozu dienen Kennwörter?
3. Wo und wie sollten Sie Sicherungskopien aufbewahren?

Im Internet beantworten Sie diese und weitere Fragen Online.