

Datensicherheit II

Computertraining4you.eu
© Daniela Wagner

► Datenschutz und
Informationssicherheit

Daten- und Informationssicherheit

Was muss sichergestellt werden

- der Datenschutz personenbezogene Daten
- die Informationssicherheit der vertraulich zu behandelnden Firmendaten

Wie wird die Sicherheit erreicht

- MitarbeiterInnen sensibilisieren

Sind sich die Mitarbeiterinnen und Mitarbeiter 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 simple Gutgläubigkeit.

- IT-Sicherheit

Geeignete Sicherheitstechniken sind Firewalls, Zugriffsschutz durch Passwörter und eingeschränkte Benutzerrechte. Im Internet verwenden Sie Anti-Viren-Programme und senden vertrauliche Daten nur verschlüsselt.

Firewalls verhindern den Zugriff auf das System von Personen außerhalb.

Passwörter haben Sinn, wenn diese nicht leicht erraten oder gar von Notizzetteln abgelesen werden können. Verwenden Sie keine Kosenamen oder Geburtsdaten.

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

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 welchen 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 und bewahren Sie sie sicher auf. Firmendaten werden meist am Ende eines Arbeitstages komplett gesichert. Der Fachbegriff dafür lautet *Backup*. Das reicht bei Banken nicht aus - Auf jeden Fall brauchen Sie einen guten Plan, wie oft gesichert werden soll.

Auf welchen externen Datenträgern Sie sichern

Disketten 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* können Sie mit den „alten“ Musik-Kassetten oder Tonbänder vergleichen. Sie speichern so viel, wie das Band lag ist, zB 200 MB.

Externe Festplatten können mittlerweile bis zu 1 TB (Terabyte) speichern. Sie eignen sich für große Datenmengen und können schnell an andere Rechner angeschlossen werden.

In Firmen wird meist ein *Backup* des gesamten Datenbestandes auf eigenen *Servern* erstellt. Datenbankadministratoren kümmern sich darum.

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

Ein Beispiel

In einem Büro erstellen 10 MitarbeiterInnen 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.

Beachten Sie

Es ist leicht, Viren zu programmieren. Recherchieren Sie mal mit einer Suchmaschine. Sie finden Bausteine zum Downloaden. Das ist frei, 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. Wir können unsere 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. Verwenden Sie die bereits erwähnte 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 der Virus aktiv.

Übrigens: Jedes Verändern, Löschen oder Ausspähen fremder Daten ist strafbar!

Überprüfen Sie Ihr Wissen

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

Antworten

Im Internet können Sie diese und weitere Fragen [Online](#) beantworten und korrekte Lösungen mit Erklärungen anzeigen lassen.