

Theorie Kapitel 2 Sicherheit und Recht

Lektion 1

Datensicherheit

- × Datenverlust
- × Maßnahmen
- ✓ In einer Welt, die von Computern abhängt, ist es ein Desaster, nicht auf die Daten zugreifen zu können. Schützen Sie sich vor Datenverlust!

Aufgabe

1. Datenverlust

Gründe, die zu Datenverlust führen:

- ▶ Stromausfall
- ▶ Fehlbedienung
- ▶ Programmfehler
- ▶ Geräteschaden
- ▶ Umweltkatastrophen
- ▶ Sabotage, Missbrauch und Diebstahl
- ▶ Hacker
- ▶ Viren

2. Maßnahmen

Stromausfall

Bei Stromausfall schützen Sie sich vor Datenverlust durch ein Notstromaggregat.

Fehlbedienung

Gegen Fehlbedienung schützen Sie sich mit Wissen - machen Sie einen Computerkurs.

Programmfehler

Verwenden Sie Originalprogramme. Erstellen Sie von wichtigen Dateien Sicherungskopien. Gehen Daten verloren, greifen Sie darauf zurück.

Geräteschaden

Festplatten gehen auch einmal kaputt. Kümmern Sie sich um aktuelle Sicherungen.

Umweltkatastrophen – „Höhere Gewalt“

Feuer, Blitzschlag, Hochwasser, Stürme, Umweltkatastrophen zerstören unter Umständen Ihre Daten. Bauliche Maßnahmen helfen. Halten Sie die Brandschutztüren geschlossen und installieren Sie den Serverraum nicht im Keller. Hilft das alles nichts, greifen Sie auf Sicherungskopien zurück.

Die Abhängigkeit von der Computertechnologie zeigte sich zum Jahreswechsel 1999 auf 2000, auch bekannt unter dem Namen Y2K-Problem. Durch den Ziffernsprung von 99 auf 00 wurden falsche Berechnungen durch Computer erwartet, Katastrophenszenarien vorhergesagt. Damals wurde geraten, rechtzeitig Geld zu beheben, Sylvester nicht mit Aufzügen zu fahren und Verkäufer/-innen mussten am 1. 1. im Geschäft nachsehen, ob die Kühlvitriolen noch funktionierten.

Datensabotage und Spionage aus den eigenen Reihen verursacht geschätzte 70 % der Sabotage-Schäden

Wir verlassen uns darauf, dass unsere Daten bei Ämtern und Firmen sicher verwahrt bleiben. In Österreich hat im Juli 2011 ein Angriff der Gruppe Anonymous Daten der GIS-Kunden gehackt. (GIS zieht in Österreich die Zwangsgebühren für Radio und TV ein, etwa wie GEZ in Deutschland).

214 000 Datensätze mit 95 954 Kontonummern waren unverschlüsselt auf dem Server gespeichert. Das Verhalten der GIS war unverantwortlich und zeigte, wie sorglos mit persönlichen Daten umgegangen wird. Dass die Daten gehackt wurden, veröffentlichte die GIS auch erst, als Anonymous ein Ultimatum stellte.

Auf Seite 34 erfahren Sie mehr zum Thema Datenschutz.

Sabotage, Missbrauch und Diebstahl

Gegen Sabotage schützen Sie sich mit baulichen Maßnahmen: Sperren Sie Büroräume und Rechenzentrum ab. Eine Zugangskontrolle verhindert, dass sich unberechtigte Personen in den Räumen aufhalten. Wenn doch etwas passiert, verwenden Sie Ihre Sicherungskopien.

Bei der Arbeit auf PCs und Laptops verwenden Sie eine Benutzeridentifizierung (User-ID) und vergeben Sie Kennwörter. Damit gewährleisten Sie auf Firmen-PCs, dass nur berechtigte Personen auf die Daten zugreifen können. Wird ein Laptop gestohlen, hat der Dieb zumindest eine Menge Arbeit, um an die Daten zu kommen. Beugen Sie dem Missbrauch der Daten auch durch spezielle Sicherungskabel für die Hardware vor.

Hacker

Hacker greifen über das Internet auf Ihre Daten zu. Lassen Sie die Firewall aktiviert. Überlegen Sie sich auch, ob alle wichtigen Daten in einem Ordner auf einem Rechner liegen müssen, das erleichtert einem Hacker die Arbeit zusätzlich. Verschlüsseln Sie persönliche oder sensible Daten. Mit Sicherungskopien arbeiten Sie zwar wieder, aber was passiert mit den gestohlenen Daten?¹

Viren

Viren und andere Malware wie Würmer oder Trojaner, bekommen Sie durch Downloads aus dem Internet, durch Anhänge an E-Mails oder durch bereits verseuchte Datenträger. Installieren Sie eine gute Anti-Viren-Software und sorgen Sie für aktuelle Sicherungskopien.

Übung

1. Finden Sie eine Strategie zum Sichern Ihrer wichtigen Daten.

Testen Sie Ihr Wissen

1. Welchen Nachteil haben elektronisch gespeicherte Daten?
2. Welche Maßnahme schützt vor Hackern?
3. Wie gelangen Viren auf Ihren Rechner?

Im Internet beantworten Sie diese und weitere Fragen [Online](#).

¹ Die Quellen zu dem Anonymous-Angriff auf die Kundendaten der GIS sind einerseits die damals aktuellen Berichterstattungen und andererseits ein Artikel in der Presse vom 25. 7. 2011 unter <http://diepresse.com/home/techscience/internet/sicherheit/680532/GIS-beugt-sich-Hackern-und-gesteht-Datenleck-ein>.

Am 17. 1. 2012 findet sich unter <http://diepresse.com/home/techscience/internet/sicherheit/724395/Millionen-Kundendaten-bei-Amazon-Tochter-gestohlen-?from=simarchiv> die Meldung, dass Millionen Kundendaten bei der Amazon-Tochter Zappos gestohlen wurden.

Am 26. 1. 2012 findet sich unter <http://diepresse.com/home/techscience/internet/sicherheit/727164/Hacker-knackte-OnlineShop-von-T-Mobile-und-Telering?from=simarchiv> die Meldung, dass der Online-Shop von T-Mobile Austria und Telering geknackt wurde.

