Übung

Sicherheitsmaßnahmen empfehlen
Lesen Sie die Sachverhalte. Welche Sicherheitsmaßnahmen würden Sie empfehlen?

Sachverhalt	Empfohlene Sicherheitsmaßnahme (Begründung)
Zum Labor eines großen Pharmakonzerns haben nur einzelne Mitarbeiterinnen und Mitarbeiter Zugang. Unbefugten Personen ist der Zugang zum gesamten Gebäude verwehrt.	
In der Datenbank eines großen Sport-artikelherstellers werden alle Artikel, Lieferanten, Kunden und Fakturenpositionen gespeichert. Neue Verkaufsmitarbeiterinnen und -mitarbeiter sollen nur eingeschränkten Lesezugriff auf die Datenbank haben. Sie dürfen keine Datensätze löschen oder bearbeiten.	
Durch ein starkes Unwetter kommt es zu einem Stromausfall.	
Im Sommer steigen die Temperaturen im Serverraum auf weit über 30 Grad. Es kommt zur Überhitzung und zu einem Kabelbrand.	

WissensCheck – „Sicherheitsrisiken und -maßnahmen"

1. Nennen Sie die wichtigsten Sicherheitsrisiken, vor denen Datenverarbeitungssysteme zu schützen sind.
2. Erklären Sie, durch welche Maßnahmen der Objektschutz gewährleistet werden kann.
3. Nennen Sie vier Beispiele für biometrische Daten.
4. Nennen Sie häufige Ursachen für Gefährdungen der Hardware.
5. Erklären Sie, durch welche Maßnahmen der Hardwareschutz gewährleistet werden kann.
6. Nennen und erklären Sie Beispiele für deliktische Handlungen, vor denen Hardware geschützt werden muss.
7. Erklären Sie die Aufgabe des Softwareschutzes.

1.2 Computerschädlinge und Manipulation

Unter Computerschädlingen versteht man nicht nur Schadprogramme, wie Computerviren, Würmer, Trojaner, sondern auch lästige Spams, die Ihren Posteingang füllen. Im folgenden Abschnitt werden Sie noch viele weitere dieser Schädlinge kennenlernen. Mit Sicherheit sind Sie schon einmal auf den einen oder anderen gestoßen.

1.2.1 Computerviren

Computerviren sind schädliche Programme, die durch Wechseldatenträger und über Rechnernetze verbreitet werden und sich selbstständig vervielfältigen (replizieren) können. Hauptsächlich DOS- und WINDOWS-PCs können durch Viren geschädigt werden. In geringerem Maße besteht auch bei APPLE-MACINTOSH- und UNIX-Rechnern die Gefahr des Virenbefalls. Je nach **Funktionsweise** und **Gefährdungspotenzial** unterscheidet man zwischen **verschiedenen Virentypen.**

Viren	Beschreibung
Bootsektor-viren	Beim Starten des Rechners (Booten) von der Festplatte oder von einem Wechseldatenträger wird das Virus aktiviert. Die Original-Bootsektoren werden überschrieben, das Gerät muss neu konfiguriert werden.
Dateiviren	Hängen sich an Programmdateien an und löschen oder manipulieren Daten.
Makro- und Scriptviren	Sind in Makrosprachen von Programmen, z. B. OFFICE, geschrieben und können u. a. Dateien löschen oder manipulieren.
Trojanische Pferde	Sind als harmloses Programm getarnt (z. B. als Bildschirmschoner oder Update), das jedoch versteckt Anweisungen enthält, mit denen sich der Virenautor Zugriff auf die Daten verschaffen kann, die auf dem befallenen Computer gespeichert sind. Aktiviert werden sie, indem Nutzer/innen das infizierte Programm starten.
Backdoors (Hintertüren)	Lassen eine Fernsteuerung des Rechners zu. Damit können Angreifer/innen von außen über das Netzwerk Daten manipulieren oder ausspionieren.
Würmer	Können sich selbst vervielfältigen und verbreiten sich über Netzwerke oder über Wechselmedien wie USB-Sticks. Beispielsweise kann ein Wurm Kopien von sich selbst an alle Kontakte aus dem E-Mail-Adressbuch senden und sich dann wiederum auf alle Kontakte in deren Adressbüchern ausbreiten. Beispiele für Computerwürmer sind: Sasser, Blaster, Conficker.
Exploits	Gelangen unter Ausnutzung von Sicherheitslücken im Betriebssystem oder durch Anwendungsprogramme in den Computer und können ihn teilweise oder ganz lahmlegen.

Folgende Maßnahmen schützen vor Computerviren:

- Regelmäßiges (mindestens wöchentliches) Anfertigen von **Sicherheitskopien** der wichtigsten Daten.
- Installation einer **Antivirensoftware.**
- Keine Attachments öffnen, deren **Ursprung nicht zweifelsfrei seriös** ist.
- **Attachments** von einer Antivirensoftware **prüfen lassen.**
- Durch **Voreinstellungen in WINDOWS und OUTLOOK** lässt sich die Gefahr von Viren ebenfalls stark einschränken.
- Auch Original-CD-ROMs und -datenträger können Viren enthalten.
- Im BIOS-Setup sollten Sie die Boot-Reihenfolge auf „C, A" oder „C only" einstellen, damit nicht versehentlich von einem infizierten Wechselmedium gebootet wird.

Die zentralen **Gefahrenquellen** für einen Virenbefall sind E-Mail-Anhänge, WWW-Downloads, FTP-Downloads, IRC (Internet Relay Chat), Newsgroups sowie OFFICE-Dokumente und Multimedia-Dateien.

Computerviren verursachen mittlerweile jährlich Schäden in Billionenhöhe mit steigender Tendenz.

Zur Erinnerung! Zentrale Gefahrenquellen für einen Virenbefall sind:

- E-Mail-Anhänge
- WWW-Downloads
- FTP-Downloads
- IRC (Internet Relay Chat)
- Newsgroups
- OFFICE-Dokumente
- Multimedia-Dateien

1.2.2 Spams

Bei Spams handelt es sich **nicht** um Viren, weil sich ein Spam nicht selbstständig verbreitet. Spams sind Werbemails, die unverlangt in großen Massen verschickt werden. Sie sind lästig, jedoch nicht schädlich.