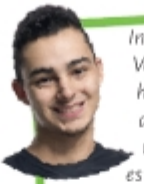
1 Datensicherheit und Datenschutz



In Alis Schule war heute ein IT-Experte zu Besuch und hat einen Vortrag zum Thema „Datensicherheit und Datenschutz" gehalten. Ali hat gelernt, welchen Sicherheitsrisiken und Schädlingen EDV-Systeme ausgesetzt sind und wie Daten sowie Hard- und Software geschützt werden können. Er weiß nun auch, welche Verschlüsselungsverfahren es gibt, und wie diese die Datensicherheit erhöhen können. Endlich weiß Ali, welche Bedrohungen es gibt, und wie er sich davor schützen kann.

Wie schützen Sie Ihren Computer und Ihre Daten vor unerwünschten Zugriffen? Tauschen Sie sich mit Ihren Mitschülerinnen/Mitschülern aus.

KOMPETENZ-ERWERB

Meine Ziele

Nach Bearbeitung dieses Kapitels kann ich

- die Sicherheitsrisiken eines Datenverarbeitungssystems systematisch einordnen;
- Sicherheitsmaßnahmen im Bereich Objektschutz, Hardwareschutz, Softwareschutz und Datenschutz charakterisieren;
- die verschiedenen Computerschädlinge unterscheiden und anhand von Beispielen analysieren;
- Viren hinsichtlich ihrer Funktionsweisen und ihres Gefährdungspotenzials zuordnen sowie mein Computersystem vor Viren und anderen Computerschädlingen schützen.

Datenschutz soll Individuen vor dem Missbrauch ihrer personenbezogenen Daten schützen. Durch Datensicherheit hingegen sollen Hardware, Software und Daten jeder Art vor Beschädigung, Verfälschung, Diebstahl, Verlust und Zerstörung geschützt werden. **Gute Datensicherheit ist somit eine Voraussetzung für effektiven Datenschutz.**

1.1 Sicherheitsrisiken und -maßnahmen

Sichern bedeutet, ein Datenverarbeitungssystem (ein ganzes Informations- oder Kommunikationssystem oder einzelne Teile) vor Gefahren aller Art zu schützen.

Eine aus Unachtsamkeit zu Boden fallende Festplatte ist nur ein Beispiel für **menschliches Versagen.** Der daraus drohende Verlust aller Daten, die auf der Festplatte gespeichert waren, ist ein unwiderruflicher Schaden für das Unternehmen.

Unter **kriminellen Handlungen** versteht man u. a. Datendiebstahl, das Herstellen von Raubkopien, Zeitdiebstahl, Spionage und Vandalismus.

Überschwemmungen, Brände, Explosionen und unvorhersehbare **Naturkatastrophen** verursachen Schäden durch **höhere Gewalt.**

Zum Bereich **mangelhafte Planung und Organisation** zählen u. a. die Abhängigkeit von Spezialisten, fehlerhafte Programme und Systeme sowie eine ungenügende Kontrolle und fehlende Investitionen.

Der Zweck von **Sicherheitsmaßnahmen** ist es, Risiken zu vermeiden, zu beseitigen oder zu vermindern.

Sicherheitsmaßnahmen

Objektschutz	Hardwareschutz	Softwareschutz	Datenschutz
			
Schutz von z. B. Gebäuden und Räumen	Schutz von z. B. Servern und Computern	Schutz von z. B. Anwendungssoftware	Schutz von z. B. personenbezogenen Daten

Diese Sicherheitsmaßnahmen wirken eng zusammen. So sind beispielsweise Hard- und Softwarekomponenten sowie Daten (Hardware-, Software- und Datenschutz) im Rahmen des Objektschutzes mitgesichert.

Bei der Planung von Sicherheitsmaßnahmen ist es wichtig, die einzelnen Schutztechniken so zu verbinden, dass ein wirksames und wirtschaftliches Schutzsystem entsteht. Ein kompletter Schutz ist jedoch nicht möglich.

Übungen

1. **Sicherheitsrisiken erkennen**
   Durch die Einführung von Notebook-Klassen haben immer mehr Schülerinnen und Schüler eigene Notebooks, die sie zu Hause und in der Schule nutzen. Sie schreiben darauf Briefe und Hausübungen, surfen im Internet und benutzen sie für Spiele. Beurteilen Sie, welche Sicherheitsrisiken bei der Verwendung von Notebooks auftreten könnten.

2. **Sicherheitsrisiken beurteilen**
   Eine kleine Frühstückspension hat einen Personal Computer für verschiedene Aufgaben zur Verfügung. Der Besitzer der Pension erledigt seine Buchhaltung, sein Angestellter den Briefverkehr und sein zehnjähriger Sohn benutzt den PC für Computerspiele. Beurteilen Sie, warum diese Lösung problematisch ist.

1.1.1 Objektschutz

Die Aufgabe des Objektschutzes ist es, die Gebäude, in denen sich Rechnerräume befinden, vor dem Eindringen von Unbefugten zu sichern.

Folgende Anforderungen werden an den Objektschutz gestellt:

- Rechnerräume sollten **außerhalb der Betriebszeiten** für alle Personen (auch für Beschäftigte) **unzugänglich** sein.
- Rechnerräume sollten während der Betriebszeiten **nur für Beschäftigte zugänglich** sein.
- **Zugangskontrollen** sollten den Betrieb in den Rechnerräumen so wenig wie möglich beeinträchtigen.
- Eindringversuche sollten einen **Alarm auslösen.**
- **Identifikationsnachweise** (z. B. Ausweise, mit deren Hilfe Personen erkannt werden), die unberechtigt verwendet wurden, sollten gesperrt werden.

Objektschutz erfolgt durch:	Beispiele
Bauliche Maßnahmen	Ein in der Mauer verankerter Tresor
Zugangs- und Abgangskontrollsysteme	Überprüfen der Zugangsberechtigung nach Person, Ort und Zeit sowie Protokollierung aller Vorgänge; Steuerung von Türöffnungsmechanismen und Auslösen eines Alarms
Schutz durch Einbruchmeldeanlagen	Durchbruchmelder (Glasbruchmelder in Panzerglasscheiben), Öffnungsmelder (Magnetschalter), Raumüberwachungsmelder (Bewegungsmelder)

Fingerabdrücke zählen zu den biometrischen Daten, da sie von Mensch zu Mensch unterschiedlich sind und so jeden einzelnen identifizierbar machen.

Zugangs- und Abgangskontrollsysteme mit modernster Technologie verwenden Erkennungssysteme, die mit **biometrischen Daten** (z. B. Muster der Netzhaut, Geometrie der Hand, Fingerabdrücken und Stimmproben) arbeiten.

Die Wahrscheinlichkeit, Erkennungssysteme, die mit biometrischen Daten arbeiten, überlisten zu können, ist äußerst gering. Bei Erkennungssystemen auf Basis des Netzhautmusters beispielsweise beträgt die Übereinstimmungswahrscheinlichkeit 1 : 1 Million. Die Kosten dieser Erkennungssysteme sind jedoch enorm hoch.

1.1.2 Hardwareschutz

Es gibt zahlreiche Ursachen, die den Betrieb der Hardware unterbrechen, zu Schäden an ihr führen oder die Hardware sogar zerstören. Die Schäden können entweder von Menschen bewusst herbeigeführt werden **(deliktische Handlungen)** oder sie ergeben sich aus **Umgebungseinflüssen.**

Deliktische Handlungen können Sabotageakte, Gerätediebstahl und Zeitdiebstahl sein.

Umgebungseinflüsse können z. B. Brand, Luft, Überspannung, Blitz, Stromversorgung oder Wasser sein.

Sabotage = mutwillige Zerstörung von Gegenständen.

Deliktische Handlungen	
Sabotageakte	Es gibt zahlreiche Möglichkeiten, Sabotageakte auf Hardware auszuüben. Am häufigsten bekannt geworden sind bisher Brandanschläge.
Gerätediebstahl	Oft verschwinden in Betrieben sogar tagsüber auf ungeklärte Weise Hardwarekomponenten. Nachts werden von spezialisierten Banden ganze Netzwerke abgebaut. Wirksame Maßnahmen sind gut ausgebaute Einbruchmeldeanlagen, Zugangs- und Abgangskontrollen sowie Stichprobenkontrollen.
Zeitdiebstahl	Beim Zeitdiebstahl wird das Gerät nicht entwendet, sondern widerrechtlich von Mitarbeiterinnen/Mitarbeitern oder Außenstehenden genutzt (eine Mitarbeiterin/ein Mitarbeiter nutzt z. B. den PC im Büro für die Buchführung des Sportvereins).

Unter Zeitdiebstahl fallen auch das Kopieren und Faxen von privaten Unterlagen im Büro.

Maßnahmen zum Schutz vor Umgebungseinflüssen	
Brandschutz	Zur Brandbekämpfung sollten Rechnerräume mit genügend Feuerlöschgeräten ausgestattet sein.
Luftschutz (Klimatisierung)	Hardware stellt je nach Art und Größe bestimmte Anforderungen an das Raumklima. Um sie zu erfüllen, ist eine Klimaanlage erforderlich.
Blitzschutz	Man unterscheidet zwischen direktem und indirektem Blitzeinschlag. Der direkte Blitzschlag erfolgt direkt ins Gebäude. Beim indirekten Blitzeinschlag schlägt der Blitz beispielsweise in eine Stromleitung ein und breitet sich über diese aus. Die dadurch entstehende Überspannung der Stromleitung kann elektrische und elektronische Geräte beschädigen.
Stromversorgungsschutz	Zur Überbrückung von Spannungsschwankungen, Stromnetzeinbrüchen und Stromausfällen kann eine USV verwendet werden.
Wasserschutz	Die Ursachen von Wasserschäden können der Bruch von Wasserleitungen, undichte Heizungsanlagen, ein Rückstau von Abwässern, Hochwasser und Überschwemmungen, das Eindringen von Regenwasser sowie von Löschwasser infolge einer Brandbekämpfung sein. Die wirkungsvollsten Maßnahmen des Wasserschutzes sind bauliche Maßnahmen (z. B. sollte der Boden der Rechnerräume ein Gefälle haben; keine Wasserleitungen in Rechnerräumen).
Befall durch Ungeziefer	Ratten und Mäuse können Kabelisolierungen aus Kunststoff zerstören. Wirksamste Maßnahmen zur Verhinderung ihres Eindringens sind die absolute Sauberkeit sowie die Montage von Gittern an Stellen, wo sie eindringen könnten.
Störeinstrahlungen	Hochfrequente Störeinstrahlungen (z. B. Rundfunk- und Fernsehsender) mit großer Energie können zu Verarbeitungsfehlern führen.

USV = unterbrechungsfreie Stromversorgung, z. B. eine batteriebetriebene Stromversorgung, die an einen Computer oder an Netzwerkkomponenten angeschlossen wird, um das System bei einem Stromausfall oder bei Spannungsschwankungen abzusichern.

Rundfunk- und Fernsehsender können Verarbeitungsfehler verursachen.

1.1.3 Softwareschutz

Aufgabe des Softwareschutzes ist es, Software vor unberechtigter Nutzung, vor Zerstörung (z. B. durch Viren) sowie vor unberechtigtem Kopieren zu schützen.

Softwareschutz	
Zugriffskontrolle	Passwörter sind die gängigste Maßnahme, um die Identität und Zugriffsberechtigung von Benutzerinnen und Benutzern auf ein System festzustellen. Durch die Eingabe einer Kennung und des dazugehörigen Passworts weisen sich Benutzerinnen und Benutzer als berechtigt aus. Das System überprüft, ob die Kennung existiert und ob das Passwort zur Kennung gehört. Danach lässt es die Benutzung zu oder weist sie ab.
Anti-Virus-Software	Mithilfe von Anti-Virus-Software kann gängige Schadsoftware aufgespürt, blockiert und eventuell entfernt werden.
Softwareupdates	Regelmäßige Softwareupdates tragen zur Sicherheit des Systems bei. Durch Updates beseitigen Hersteller u. a. Fehler und allfällige Sicherheitslücken.

Der Schutz durch Passwörter wird verbessert, wenn Sie möglichst **lange, alphanumerische** und **sinnlose** Zeichenfolgen verwenden.