# Datensicherung

## Gefahren für Daten:

* Hardwaredefekt
* Malware
* Softwarefehler
* äußere Gewalteinwirkung
* Benutzerfehler
* Diebstahl
* Stromausfall

## Malware:

Software, die bewusst zu dem Zweck geschrieben wurde,

Schaden anzurichten, Daten auszuspähen, ein System zu manipulieren oder sabotieren.

## Formen von Malware:

* Viren
* Würmer
* Trojaner
* Spyware
* Ransomware
* Adware

## Art der Schäden, die Malware erzeugen kann:

* Daten löschen
* Daten ausspähen (Spyware)
* Daten verschlüsseln (Ransomware)
* System destabilisieren
* Systemzugriff verweigern
* System fernsteuern (Botnetz)
* Hintertüre öffnen
* Spamserver dienen
* Hardware zerstören
* Rechenkapazität stehlen

## Beispiel für Schäden durch Ausspionieren von Daten

* Betriebsspionage:   
  Z.B. Diebstahl von Forschungsergebnissen
* Ausspionieren von Kreditkartendaten u. Passwörtern,  
  um im Namen eines geschädigten z.B. einkaufen zu können
* Erschleichen höherer Rechte für ein System
* Identitätsdiebstahl
* Erpressung mit Veröffentlichung von Daten privat wie beruflich

## Motivationen für Hacker

* kommerzielle Interessen
* blind möglichst großen Schaden anrichten
* politische, religiöse o.ä. fanatische Interessen
* sportliche Disziplin ohne kommerzielle oder andere weitere Interessen

## Ransomware

Software, die Daten verschlüsselt u. den Systemzugang für Benutzer einschränkt

und ein Lösegeld erpresst zur Entschlüsselung der Daten.

## Viren, Würmer u. Trojaner

Nach allgemeinem Sprachgebrauch werden "Viren" synonym für Schadsoftware verwendet.

Im engeren u. ursprünglichen Sinn waren Viren Schadsoftware,

die sich -im Gegensatz zu Würmern- nur auf einem System vervielfältigten.

Würmer waren ursprünglich dafür ausgelegt,

sich möglichst schnell zu verbreiten.

Trojaner: vom "Trojanischen Pferd", in einem scheinbaren Geschenk versteckte Krieger.

Hier: Programm, das nach außen eine positive Wirkung erreicht,

in Wirklichkeit aber einen Schadauftrag ausführt.

## Phishing:

Kunstwort aus "Password fishing": Abgreifen von Passwörtern über einen Vorwand.

## Verbreitungswege von Schadsoftware

* Anhänge von Mails
  + direkt ausführbare Programme
  + "versteckt" durch vorgegebene zweite Extension  
    bei Unterdrückung der Anzeige bekannter Extensions,  
    z.B.: "virus.txt.exe" wird angezeigt als "virus.txt".  
    Textdateien scheinen dem naiven Benutzer ungefährlich
  + "versteckt" in Makrodateien,  
    z.B. Office-Makros
  + "versteckt" in Bildern oder PDF-Dateien
  + WLAN
* Besuch von manipulierten Internetseiten
* Herunterladen von Programmen
* "gefundene" USB-Stick
* getauschte Datenträger
* WLAN

## Sicherheitslücke WLAN

Um auf ein nur verkabelt vernetztes System zuzugreifen,

z.B. eine Firma ohne oder mit genügend gesicherter Internetanbindung,

musste man sich früher lokal am Firmensitz befinden.

Durch WLAN wird der Zugriff drahtlos möglich.

Ein Eindringen kann von außerhalb erfolgen,

z.B. vom Firmenparkplatz aus.

Dies reduziert die Hemmschwelle.

Das WLAN ist i.d.R. verschlüsselt mit WEP (wired equivalent privacy)

oder WPA bzw. WPA-2 (wifi protected access).

Alle diese Verschlüsselungsstandards sind jedoch gehackt.

Es dauert für einen Angreifer nur Minuten,

den Schutz zu umgehen.

Der Nachfolgestandard WPA-3 ist noch nicht weit verbreitet.

Auch "WPS", ein System zum vereinfachten Einrichten des Zugangs,

ist ein Sicherheitsrisiko.

Wichtig ist ein kompliziertes Passwort bunt gemischt aus Klein- u. Großbuchstaben

sowie Ziffern u. ggf. einigen Sonderzeichen.

## Angriffsszenarien:

* Löschen, Ausspähen oder Verändern von Daten
* Rechner "versklaven", um ihn fernzusteuern für weitere Zwecke
* Denial of servce Attacke:  
  Einen Rechner so mit Anfragen überfluten,  
  dass er "in die Knie geht",

also seiner Aufgabe nicht mehr gerecht werden kann.

* Steigerung davon: "Distributed denial of service attack":

Mehrere versklavte Rechner bombardieren gezielt einen Rechner,  
um ihn handlungsunfähig zu machen.

* "Man in the middle-attack":  
  Hacker schaltet sich in Kommunikation ein,

hört mit, fängt Nachrichten ab u. manipuliert.

* Hacker verschlüsseln Daten u. fordern Lösegeld
  + um Daten nicht zu veröffentlichen
  + zum Rückgängigmachen der Verschlüsselung

## Aufbau von Schadsoftware

Die Programme bestehen aus zwei Teilen:

1. Verbreitungsmechanismus
2. Schadteil

Der Verbreitungsteil dient dazu,

die Schadsoftware möglichst schnell, weit u. unbemerkt zu verteilen.

Es können Mechanismen integriert sein,

die die Verbreitung mitzählen u. sich nach einer erfolgreichen Verbreitung selbst löschen,

um den Infektionsverlauf nicht mehr nachvollziehen zu können.

Es können zur Verbreitung die Kontaktdaten des Infizierten benutzt werden

oder nach Algorithmen IP-Adressen generiert werden.

Unabhängig davon ist der Schadteil, die "payload",

die sehr unterschiedlich sein kann, siehe "Art der Schäden" oben.

## Gegenmaßnahmen Maßnahmen

* Kritisches problembewusstes Verhalten
* Zwei Faktor Verifikation:  
  Bestellungen o.ä. müssen über Handy verifiziert werden
* Anti-Viren-Software
* Firewall
* Betriebssystem u. Programme aktuell halten
* Dubiose Internetseiten vermeiden wie z.B. illegale Downloadplattformen,  
  juristische Grenzbereiche
* Eigene Hardware vor fremdem Zugriff schützen
* Kontoeinstellungen

## Anti-Viren-Software, Firewall

Aufgaben sind allgemein, Schadsoftware fern zu halten

und einer mglw. schon erfolgten Infektion entgegen zu treten.

Dafür werden mehrere Handlungsstränge verfolgt:

* Alle Daten zu kontrollieren, die rein- u. rausgehen
* Regelmäßiger Scan des Festplatteninhaltes
* Regelmäßige Aktualisierung der bekannten Schadsoftware
* Verdächtiges Verhalten von Programmen erkennen
  + Zugriff auf geschützte Speicherbereiche
  + Löschen systemrelevanter Dateien
  + Allokieren unverhältnismäßig großer Speicherbereiche
  + Versuch, Abwehrmechanismen zu deaktivieren
* Deaktivieren potenzieller Bedrohungen
  + Quarantäne für Datei
  + Weitergabe zur Analyse durch Hersteller
  + Versuch bekannte Schäden zu reparieren

Geschäftsmodell:

Für einen Zeitraum von typ. einem Jahr kauft man eine Lizenz

für einen oder mehrere Rechner

mit Berechtigung zu Updates der Virensignaturen.

Typische Hersteller:

Microsoft, Sophos, Kaspersky, Symantec, GData, Avira, FSecure, McAfee u.a.