# 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

## 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

## Prophylaktische 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