Seniorenrat Dietikon

# Dig[iT]reff – 13.7.2022

## Sicherheit mit dem PC


 

# • Wer referiert heute?

**Name**: Walter Riedle
Wohnort: Urdorf
In der EDV/IT (Informatik) seit 1972

**Hobbies**:
Spielbühne Urdorf (1980 – 2022)
Computeria-Urdorf (2006 – 2018)
Astrologie

- **Unser heutiges Thema: PC-Sicherheit**

# Um Illusionen vorzubeugen:
# Einen absoluten Schutz gibt es nicht!

**Heutiges Ziel**

- Die Teilnehmenden kennen die Bedrohungs-Möglichkeiten.
- Sie wissen, wie sie sich davor optimal schützen.
- Sie bekommen einige Tipps und Hinweise.

# "Hausgemachte" Bedrohungen

- **Löschung** (durch Unachtsamkeit)
- **Diebstahl** (Einbruch)
- **Vernichtung** (HW-Defekt, Feuer)

Wie begegnen wir diesen Bedrohungen?

# Unsere Vorkehrungen

*(gegen Löschung, Diebstahl und Vernichtung)*

- Permanent Sicherungskopien der Daten erstellen.
  (Cloud, Externe Harddisk, USB-Stick, etc.)
- Sicherungskopien der Daten sicher auslagern.
  (nicht beim PC aufbewahren)
- Zugriff auf den PC nur mit Identifikation.
  (Passwort, Fingerprint usw.)
- Passwort/Passwörter nicht beim PC aufschreiben.

# Bedrohungen aus dem "Netz"

## Malware (= Schadprogramme) *(engl. malicious software)*

- **Viren** **17%**
  Programmcode, der sich in einem bestehenden Programm einnisten und sich selbst reproduzieren kann.
- **Würmer** **8%**
  Sind selbstständige Programme und können sich selbst reproduzieren.
- **Trojaner** **70%**
  Sind selbstständige Programme, die sich jedoch nicht reproduzieren können.

Die Übergänge zwischen den einzelnen Malware-Typen sind fliessend und teilweise auch sich überschneidend.

# Viren

**Programmcode, der sich in bestehende Programme einschleust und sich dort unkontrolliert vermehrt.**
**Viren brauchen immer ein Wirte-Programm**

- Es gibt Millionen bekannte Viren
- Erste Vireninfektion 1986 an der FU Berlin
- Verbreitung einst durch Disketten, heute via Internet
- Anfällig sind Programme, Skripts, Makros, Bootsektoren

Abhilfe: Verwenden eines Anti-Viren-Programms.
Dieses muss immer aktualisiert werden können.
Bei einem guten AV-Programm gibt es täglich etwa 2 - 3 Updates der Virensignaturen.

## • Würmer

**Programm, das sich im Computersystem einnistet und dort sich aktiviert. Würmer sind selbständige Programme und brauchen kein Wirte-Programm.**

- Meist verbreitet über E-Mails und Internet
- Schnellere Verbreitung als bei Viren möglich, da aktiv
- Werden oft als getarnte E-Mail-Anhänge verbreitet

Abhilfe: Verwenden eines Anti-Viren-Programms.
Vorsicht beim Öffnen von E-Mail-Anhängen.

# • Trojaner

**Programm, das vorgibt eine interessante Funktion zu bieten jedoch ein unerwünschtes Programm einschleust.**

- Öffnen von Backdoors für Zugriff auf den PC.
- Überwachen von Datenverkehr und Benutzeraktivitäten.
- Installation von Dialer-Programmen auf Mehrwertnummern.
- Versenden von E-Mails unter falschem Absender.

Abhilfe: Skepsis gegenüber Unbekanntem.
Verwenden einer Firewall, die den Zugriff von aussen auf den PC verhindert.

# • Spyware

**Software, die Daten ohne Wissen des Benutzers an den Spyware-Hersteller sendet.**

- Das Surfverhalten wird für kommerzielle Zwecke analysiert.
- Einblenden von Werbefenstern.
- Ausspähen sensibler Daten (Passwörter, Kreditkartennr.)
- Keylogger kontrollieren Tastatureingaben (Passwörter)

Abhilfe: Verwenden einer Firewall und einer aktuellen Anti-Viren-Software.

# • Spam

**Automatisch versendete elektronische Mitteilungen an Empfänger ohne deren Einwilligung.**

In der Schweiz verbietet das BG gegen den unlauteren Wettbewerb seit 1. April 2007 den Versand von solchen unerwünschten Meldungen.

*Ausnahme*: Ein Verkäufer darf seinem Kunden Werbematerial für ähnliche Waren, Werke oder Dienstleistungen zustellen, muss diesen aber auf die kostenlose Ablehnungsmöglichkeit aufmerksam machen!

Abhilfe: Verwenden eines Spam-Filters des Providers
(Der Provider darf den Spam nicht von sich aus löschen!)
Beim Provider reklamieren.
Und wenn es nicht nützt vor Gericht klagen.

# • HOAX

**Falschmeldung, die den Adressaten auffordert eine bestimmte Aktion zu ergreifen.**

- Weiterleiten einer E-Mail an alle Freunde und Bekannten
  - Angst machende Information (gefährliche Telefonnummer)
  - Mitleid erregende Information (krebskrankes Kind)
- Löschen „gefährlicher“ Programme auf dem PC
- Bekanntgabe von User-Id und Passwort via E-Mail

Abhilfe: Vor einer „unbedachten“ Aktion kontrollieren, ob es sich um einen Hoax handelt unter https://hoax-info.tubit.tu-berlin.de/hoax/

# • Sicherheitsvorkehrungen

- Betriebssystem auf dem aktuellsten Stand halten.
- Verwenden einer aktuellen Anti-Viren-Software.
- Nur Programme installieren, die benötigt werden.
- Nur Programme aus sicheren Quellen installieren.
- Anwenderprogramme auf dem aktuellen Stand halten.
- Verwenden einer aktiven Firewall.
- Überlegt handeln, aber keine Angst haben.
- Skeptisch sein gegenüber unbekannten Absendern.
- Skeptisch sein gegenüber Mail-Anhängen auch von Freunden.

# • Wie aktualisiere ich das Betriebssystem?

- Das Betriebssystem ist Windows 10 oder 11:
  Kontrolle: Einstellungen/Systemsteuerung ⇨ System ⇨ Info
- Prüfen auf Updates:
  Einstellungen/Systemsteuerung ⇨ System ⇨ Windows Update
- Falls oben steht «Herunterladen und installieren»:
  PC am Ladegerät anschliessen und Meldung anklicken.
- PC laufen lassen bis der Anmeldebildschirm wieder erscheint.

Je nach Update kann dieser bis zu
einer Stunde oder länger dauern!

# • Wie erstelle ich ein sicheres Passwort?

**Ein gutes Passwort sollte …**

- aus Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen
- aus mindestens 10 Zeichen bestehen
- keine Verbindung zum Benutzer enthalten
- keine Wörter aus Wörterbüchern enthalten
- für jeden Zugriff unterschiedlich sein

Folgende Möglichkeiten haben sich bewährt:

- Verwenden eines Merksatzes
- Einsatz eines Passwort-Managers

# • Passwort aus einem Merksatz

- Erstelle einen Merksatz aus Buchstaben, Ziffern und Sonderzeichen.
- Nimm die Anfangsbuchstaben, die Ziffern und die Sonderzeichen.

Beispiel:
Mein 1. Haustier war eine griechische Landschildkröte namens Bobo!

**M**ein **1.** **H**austier **w**ar **e**ine **g**riechische **L**andschildkröte **n**amens **B**obo**!**

**M1.HwegLnB!** oder **M1.HtwegLsnB!**

Wie stark ein Passwort ist, lässt sich über folgenden Link prüfen:
https://www.passwortcheck.ch/

# Die am häufigsten verwendeten Passwörter

2019 hat das Hasso-Plattner-Institut der Universität Potsdam Millionen gestohlene Identifikationen untersucht und damit eine Rangliste der in Deutschland am häufigsten verwendeten Passwörter erstellt:

| *Rang* | *Passwort* | *Anzahl* |
|---|---|---|
| 10. | 00000 | 777'576 |
| 9. | abc123 | 782'643 |
| 8. | 111111 | 800'595 |
| 7. | 1234567890 | 803'771 |
| 6. | 123123drink | 806'419 |
| 5. | 1234567 | 837'534 |
| 4. | Passwort | 858'534 |
| 3. | 12345678 | 953'688 |
| 2. | 123456789 | 1'242'790 |
| 1. | 123456 | 2'068'643 |

# • Einsatz eines Passwort-Managers

Der Passwort-Manager (ein Anwenderprogramm)
speichert verschlüsselt

- URL
- Benutzer-Identifikation
- Passwort

für einen einfachen Zugriff mit komplexen Passwörtern.

Es gibt sie in kostenlosen und käuflichen Versionen.

# • Zwei-Faktor-Authentisierung (2FA)

Prüfen der Berechtigung durch Abfragen auf zwei verschiedenen, getrennten Kommunikationswegen.
Es ist eine zusätzliche Sichheitsstufe.

Funktionsweise:

- Einloggen über Internet-PC mit Benutzer-ID und Passwort.
- Der Empfänger sendet einen Code aufs Handy.
  (Der Code ist nur eine kurze Zeit gültig, z.B. 5 Minuten)
- Dieser Code muss am PC eingegeben werden.

# • Ist E-Banking wirklich gefährlich?

**Grundsätzlich nein, sofern alle genannten Sicherheits-Vorkehrungen eingehalten werden:**

- Starkes Passwort
- Aktuelles Virenprogramm und aktive Firewall
- Alle Programme (inkl. Betriebssystem) auf neustem Stand
- Verbindung nur über sicheres WLAN (oder Kabel)
- Wenn möglich Banken-App verwenden anstatt Browser
- Aufmerksam und vorsichtig sein

E-Banking über den PC dürfte weniger gefährlich sein, als zur Bank zu fahren, Geld abzuheben und auf der Post einzuzahlen!

# • "Update" oder "Upgrade"?

Ein **Update** dient der Sicherheit. Damit werden vorhandene Programmfehler korrigiert resp. eliminiert.
Mit Ausnahme von kleinen Anpassungen oder Erweiterungen werden beim Update keine Änderungen am Programm vorgenommen.

Bei einem **Upgrade** werden insbesondere neue Funktionen in ein Programm eingebaut und auch das ganze Erscheinungsbild kann ändern.

Achtung: Ein Upgrade ist oftmals mit Kostenpflicht verbunden!

- **Ein Wort zu «Dark Patterns»**

Sie versuchen die Entscheidung des Anwenders so zu beeinflussen, dass er zum Vorteil des Anbieters die gewünschte Taste automatisch drückt.

**Sie sind nicht gefährlich, aber lästig!**

**Beispiel** (eines Entwicklungsschritts):

- ☐ Bitte senden Sie mir künftig den Newsletter
- ☑ Bitte senden Sie mir künftig den Newsletter
- ☐ Bitte senden Sie mir künftig keinen Newsletter

# Danke für Ihre Geduld und Aufmerksamkeit


 

# Abschluss

## Kurzes Feedback:

- Wie hat es Ihnen heute gefallen? 1-6 (1=☹ 6=😊)
- Welche drei Ideen/Tricks/Tipps/Themen nehmen Sie heute mit

## Ein freiwilliger Unkostenbeitrag würde uns freuen

## Danke für Ihr Interesse und Aufmerksamkeit!