Vortrag über IT Sicherheit

beim Seniorenbund Donaustadt
am 14.Oktober 2015

von
Dipl. Ing. Anton Staud

Was sichern?

- **Ihre persönlichen Dateien**
  - Fotos, Filme, Eigene Werke, Dokumente, Kontaktdaten
- **Ihre Geräte** (Computer, Tablet, Handy)
- **Das System** (Windows, Android)
- **Ihr WLAN** daheim

Wovor sichern?

- Virtuelle Angriffe aus dem **Internet**
  - Viren, Trojaner, Lösegeld-Programme, etc.
  - Anhänge und Links in unerwünschten (= SPAM/JUNK) E-Mails
  - Unerwünschte (= unbeabsichtigte) Downloads
- Übertragung durch externe Geräte (z.B. USB-Sticks)
- Geräteschaden (z.B. Wasser, Sturz, Ermüdung)
- Diebstahl, Raub

Wie sichern? (1)

- **Ihre persönlichen Dateien sichern Sie am besten auf sogenannten externen Datenträger, z.B.**
  - Externe Festplatten (vorzugsweise 2,5 Zoll)
  - USB Sticks (vorzugsweise 16 GB oder 32 GB)
  - CDs / DVDs (wird immer weniger als Datenspeicher verwendet)
  - In der „Cloud“: (meist Tablet und Smartphone Daten wie Kontakte und Bilder)

-> Ihre persönlichen Daten sollten Sie immer an zwei verschiedenen Stellen speichern!

Wie sichern? (2)

- **Ihren Computer**
  - Mit einer Firewall (in Windows bereits vorhanden)
  - Mit einem Virenscanner, z.B. Kaufprogramme wie Norton oder Kaspersky oder kostenlose Programme wie AVG oder Avast
  - Prüfen Sie immer die Symbole auf Ihrer PC Symbolliste („System-Meldungen“ , Virenscanner Meldungen)
  - Sichern Sie regelmäßig Ihr Gesamt-System auf eine externe Festplatte
  - Prüfen Sie von Zeit zu Zeit Ihre Festplatte auf Materialermüdung (z.B. mit dem Programm Crystaldisk)
- **Ihr Tablet / Smartphone:**
  - Mit einem Virenscanner (auch hier gibt es Kaufprogramme und kostenlose Programme
  - Übertragen Sie regelmäßig Ihre persönlichen Dateien (Kontakte, Fotos, etc) auf Ihren PC oder in die Cloud
- **Ihr WLAN daheim:** mit einem Passwort (WPA oder WPA2)

Passwörter (1)

- **Es sollten die folgenden Anforderungen abgedeckt sein!**

  Passwörter sollten enthalten:

  - Groß- und Kleinbuchstaben,
  - Sonderzeichen und Ziffern
  - Mindestens 8 Zeichen

- **Brauchen Sie für jede verschiedene Internet Anmeldung ein eigenes Passwort?**

  - Meine Antwort ist NEIN

- **Sollten Sie Passwörter periodisch ändern?**

  - JA, aber in längeren Abständen, z.B. einmal pro Jahr

Passwörter (2)

- **Gibt es Anleitungen zur Erstellung eines Passwortes?**
  - z.B: Teilen in einen **Fixen Teil + variablen Teil** (z.B. -> 2919Werk111) mit 111 als variabler Teil
  - „**Passwortsätze**“, z.B. *Wir essen täglich 2 oder 3 Birnen!* -> wird zum Passwort: **Wet2o3B!**
- **Wie speichere ich Passwörter?**
  - Meine Antwort ist: Schreiben Sie sie auf, aber nicht auf einen Zettel, sondern in zwei(!) „kleinen Notizbüchern“, die Sie getrennt aufheben
  - Weitere Möglichkeiten: In einem Programm (Passwort Safe), im PC speichern, sich die Passwörter merken

E-Mails

- **E-Mails sind „unsicher“**
  - Sie werden normalerweise unverschlüsselt gesendet und sind daher (relativ) leicht mitlesbar
  - Eine Absendebestätigung gilt nicht als Beweis (z.B. vor Gericht)

E-Mails von unbekannten Absendern sollten Sie sorgfältig prüfen

- Ist der Absender eine „**seriöse**“ Firma oder Institution?
- Im Zweifelsfall keine E-Mail Anhänge in solchen E-Mails öffnen
- Im Zweifelsfall in diesen E-Mails keine mitgeschickten Internet Links anklicken

Kreditkarten / Telebanking

- In „fremden“ WLANS („**Hotspots**“) sollten Sie **NICHT** mit Kreditkarte einkaufen und auch Telebanking **NICH**T verwenden

- Wenn Sie Bedenken bezüglich der Verwendung von Kreditkarten im Internet haben, holen Sie sich eine „Prepaid“ Kreditkarte von Ihrer Bank

- Für Telebanking sollten Sie immer die von Ihrer Bank empfohlene Methode verwenden - meist zweistufige Sicherheit (TANs oder eTANs)

- Telebanking sollten Sie möglichst nur vom **eigenen PC aus** (und nicht vom Smartphone oder Tablet) und nur im **eigenen WLAN** verwenden

(Unerwünschte) Werbung

- **JUNK/SPAM E-Mails**
  - Leider in vielen Fällen nicht vermeidbar
  - Verwenden Sie für Registrierungen im Internet eine zweite (kostenlose) E-Mail Adresse (z.B. von GMX, Google oder Microsoft)
- **In Internet Seiten**
  - Ebenfalls oft nicht vermeidbar
  - Manchmal mit der Browser Funktion „Popups blocken“ reduzierbar
- **„Cookies“**
  - Können Sie regelmäßig löschen oder generell blockieren
- **Agressive Werbe-Programme („Browser Hijacking“)**
  - Können Sie mit speziellen Programmen wie z.B. ADWCleaner blockieren oder entfernen

Schlusswort

- Dieser Vortrag orientiert sich an meiner eigenen (40-jährigen) Praxis-Erfahrung.
- Die Inhalte beziehen sich grossteils auf
  - **Windows** Computer (mehr als 80% Marktanteil) und
  - **Android** Tablets und Smartphones (ebenfalls mehr als 80% Marktanteil
- Gehen Sie mit **Sorgfalt und Hausverstand** an das Thema „Sicherheit“ heran
- Es ist aber nicht notwendig, „übervorsichtig“ zu sein.