(UN-) Sicherheit zum Anfassen – Schutzmaßnahmen

Thomas Haase – tel: 0175 588 4475 – mail: schutzschild@mailbox.org

Neuigkeiten betreffs aktueller Bedrohungen: https://www.digiwahn.de

Sehr geehrte Damen und Herren, nachfolgend habe ich Ihnen die wichtigsten Tipps; Werkzeuge und Links noch einmal zusammengefasst. Sollten Sie Fragen oder Probleme haben, kommen Sie bitte gern jederzeit auf mich zu. Viele Grüße, ihr Thomas Haase

1. Grundabsicherung Ihres Computers

Maßnahmen Absicherung von Computer / PC

1.1. Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte **Sicherheitsupdates** für Ihr Betriebssystem und die von Ihnen installierten Programme (zum Beispiel Internet-Browser, Office, Flash Player, Adobe Reader) – idealerweise über die Funktion "Automatische Updates".

1.2. Setzen Sie ein **Virenschutzprogramm** ein und aktualisieren Sie dieses regelmäßig.

1.3. Verwenden Sie eine **Firewall**. Diese ist in den meisten modernen Betriebssystemen bereits integriert und soll Ihren Rechner vor Angriffen von außen schützen.

Programme und Werkzeuge

Anti Virenprogramme (Beispiele):

https://www.avira.com/de/index

https://www.eset.com/de/

bei Virenbefall:

https://www.heise.de/download/product/desinfect-71642

https://www.sicherheitstest.bsi.de/avira

2. Grundabsicherung Ihres Smartphones

Maßnahmen Absicherung ihres Smartphones

2.1. Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte **Sicherheitsupdates** für Ihr Betriebssystem und wechseln Sie nach Ablauf der Unterstützung auf ein neues Gerät.

2.2. Installieren Sie Apps nur aus **vertrauenswürdigen Quellen** und prüfen Sie die Zugriffs-berechtigungen.

2.3. Nutzen Sie Sperrcodes und Passwörter mit **ausreichender Länge** und **möglichst komplex**.

2.4. Sperren Sie ihr Smartphone und lassen Sie es **niemals unbeaufsichtigt**.

Programme und Werkzeuge

Anti Virenprogramme (Beispiele):

https://www.avira.com/de/free-antivirus-ios

https://www.avira.com/de/free-antivirus-android

https://www.av-test.org/de/antivirus/mobilgeraete/

Schutzprogramme Hotspot, Funkzellen:

https://prism-break.org/

https://opensource.srlabs.de/projects/snoopsnitch

https://www.telekom.de/unterwegs/apps-und-dienste/sicherheit/protect-mobile

Weitere Informationen:

http://www.schutzschild.org/schulung/ios.pdf

http://www.schutzschild.org/schulung/android.pdf

3. Grundabsicherung Ihres Smart Home

Maßnahmen Absicherung ihres Smart Home

3.1. Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte **Sicherheitsupdates** für Ihren Router und ihre verwendeten Geräte.

3.2. Ändern Sie **alle voreingestellten Passwörter** und wählen diese ausreichend lang und komplex.

3.3. Achten Sie beim Kauf neuer Geräte darauf, dass diese **längerfristig noch gepflegt** und **unterstützt** werden (neue Updates).

Programme und Werkzeuge

Wireless Network Watcher:

https://www.nirsoft.net/utils/wireless_network_watcher.html

Fing Netzwerkscanner:

https://www.fing.io/download-free-ip-scanner-desktop-linux-windows-osx/

Weitere Informationen:

https://www.kuketz-blog.de/wlan-absichern-die-illusion-vom-sicheren-wlan/

https://www.pcwelt.de/ratgeber/10-raffinierte-WLAN-Tools-fuer-Ihr-Netzwerk-Software-9593771.html

4. Grundlegende Regeln

Grundlegende Verhaltensregeln

- Sein Sie skeptisch!
- Trennen Sie private und geschäftliche Daten.
- Verwenden Sie starke Passwörter.
- Verwenden Sie unterschiedliche Passwörter.
- Trennen sie private und geschäftliche Passwörter.
- Sichern Sie Ihre mobilen Geräte.
- Sichern Sie Ihre Daten.
- Halten Sie Ihre Software und Firmware aktuell.

Typische Fehler

- Verwendung unbekannter oder nicht vertrauenswürdiger Dienste mit gleichen Zugangsdaten.
- Schwache Passwörter (start123, admin, Passwort, 123456, usw.).
- Schlechte Zugangsdatenablage (aufgeschrieben auf Zettel, in einer Textdatei, etc.).
- Updates und Sicherheitspatches werden nicht eingespielt.
- Keine Trennung vom Betrieblichen und Privaten.
- Verwendung von Standard-(Router) Passwörtern.
- Keine Handy Zugangssicherung.
- Kein Backup von Daten und Konfigurationen.