IT-Sicherheitskurs – Tag 1

VORTRAGENDER:
GR Thomas Rupprecht, B.Sc

Über mich

- Thomas Rupprecht, B.Sc
- 27 Jahre
- Gemeinderat seit 2015
- Schule: HTL Mödling → FH Wr. Neustadt
- Beruf: Webentwickler (Programmierer)
- Hobbies: Programmieren, Feuerwehr, Tanzen, Politik
- Großes Interesse für IT-Security

Agenda – Tag 1 (heute)

- Passwörter
- Updates
- Firewall
- Virus vs. Anti-Virus
- „Brain.exe“
- Backup
- Betriebssysteme
- Smartphones
- WLAN
- SmartHome/IoT

Agenda – Tag 2

- Privatsphäre
- Datenschutz / DSGVO
- Überwachung
- Darknet
- DDoS
- Kinderschutz
- sichere Kommunikation
- sicheres Surfen
- Phishing

Disclaimer

Nicht alles ist bzw funktioniert genauso wie erklärt. So wird es aber einfacher und verständlicher.

Sicherheitsgefühl

- Wer glaubt genug über IT-Sicherheit zu wissen um sicher im Netz zu sein?
- Wer hatte schon einmal einen Virus?
- Wer hatte schon einmal Datenverlust?
- Wer hat schon mal Geld verloren?
- Wer installiert alle Updates?
- Wer hat ein Anti-Viren Programm?
- Wer glaubt ein gutes Passwort zu haben?

Passwörter

Sicheres Passwort?

- 123456
- hernstein2560
- thomas90
- NiCkY123456
- 22032017maxmustermann2560
- 147896325
-]\pEDr9|.w\XM?8#0l<~

Sicheres Passwort!

- Mindestens 12 Zeichen
- Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen
- Keine Namen, Orte, Geburtsdaten, ...
- Aber: Länge ist wichtiger als Komplexität
- Unterschiedliche Passwörter
- Alle 1-3 Jahre ändern

Sicheres Passwort

- Merksatz
- Wörter kombinieren
  - Password Strength - xkcd
- LeetSpeak (ähnliche Zeichen)
- Passwort Generator
- Kombinationen: Mögliche Zeichen ^ Anzahl Zeichen
  - Bsp. 1: 62^6 = 56.800.235.584
  - Bsp. 2: 26^10=141.167.095.653.XXX

Passwort Tests

- zxcvbn
- How Secure Is My Password?
- Password Meter

Passwort Zusatzinfos 1

- Unterschiedliche Passwörter
  - Wichtig: Bank, Email (Passwort zurücksetzen)
  - Mittel: Shops, alles mit Bezahlung
  - Unwichtig: Social Media, Foren, ...
- Datenleaks: Emails, Passwörter, ...
  - have i been pwned?
  - Passwörter sollten/werden gehasht am Server gespeichert → Kein Zugriff
- Passwort Safes (KeePass)

Passwort Zusatzinfos 2

- Nicht öffentlich herumliegen lassen
  - Wenn dann verschleiert (Rechnung, ...)
- NIEMAND fragt nach deinem Passwort!!!
- Backup Kopie im Safe (USB-Stick/Zettel)
- Nicht alle Zeichen/Länge überall möglich
-
- Biometrie
  - Handys knacken mit Sekundenkleber und Kon taktlinsen

Verteidigungslinien

Verteidigungslinien

- Was ist (am) wichtig(sten)?
  - Anti-Virus
  - Backups
  - „Brain.exe“
  - Firewall
  - Updates
- Laien vs. Experten – Online Sicherheit
- Router → System → Anti-Virus → Brain.exe

Analogien im Reallife

- Haus/Diskothek = PC/Notebook/Smartphone
- Durchgänge/Öffnungen = Ports, USB, ...
- Fenster/Türen = Firewall
- Türsteher = Anti-Viren Programm
- Schlägertyp/Drogendealer = Virus
- Ausweiskontrolle = Dateicheck
- Kontrollgang = Systemcheck
- Sicherheitstür statt normaler Tür = Updates
- Logischer Menschenverstand = „Brain.exe“

Updates

Warum Updates?

- Neue Funktionen
- Schneller (Code optimiert)
- Stabiler (gefundene Fehler)
- Kompatibilität (mit anderen Programmen)
- Sicherer (Sicherheitslücken geschlossen)

Was Updaten?

- ALLES!!!
  - PC/Notebook
    - Betriebssystem, BIOS/UEFI, Anti-Virus, Office, Browser, Java, Flash, Spiele, Add-ons, ...
  - Smartphone
    - Betriebssystem, Apps
  - Router
  - Smart TV
  - SmartHome/IoT
    - Glühbirne, Steckdose, Türschloss, ...

Firewall

Feuerwand?

- Wo: Router, Betriebssystem
- Analogie: Fenster/Türe
- Filtert/Regelt die externen Verbindungen
- Standard: alle Fenster/Türen geschlossen
- Nur von innen zu öffnen
- Bleiben offen bis Verbindung beendet

Virus vs. Anti-Virus

Virus? Trojaner?

- Arten von Malware (Schadprogramm)
  - Viren: Allgemeine Bezeichnung
  - Würmer: selbstständige Vervielfältigung
  - Trojaner/Rootkit: Arbeitet versteckt
  - Backdoor: Öffnet Hintereingang in Systeme
  - Adware: Nervende Werbung
  - Spyware: Versendet private Informationen
  - Ransomware: Erpressung/Verschlüsselung
  - Rogueware: Fake-Anti-Viren Programm

Anti-Viren Programm? Check!

- Hab ich. Also alles sicher? → Nein!
- Warnung von Experten
- AV-Test Vergleich
- Analogie: Türsteher/Kontrolleur

Anti-Viren Programme 1

- Aufgaben:
  - Eigene Firewall
  - Livescan
  - Systemscan
  - Cloudscan (VirusTotal)
  - Verhaltensanalyse
  - Kinderschutz

Anti-Viren Programme 2

- Probleme
  - neue Viren
  - False-Positives
  - eigene Lücken
    - Admin/Root Rechte
  - verschlüsselte Daten
    - MitM → HTTPS Warnungen
    - badssl

“Brain.exe”

“Brain.exe” ???

- Schalte dein Hirn ein!!!
- Denken → dann handeln
- Niemand schenkt dir Geld
- Niemand fragt nach deinem Passwort
- Hab doch dort kein Bankkonto → Betrug
- Keine Rechnung, Bewerbung, ... braucht Makros

Backup

Warum Backup?

- Nichts ist 100% sicher
  - Hacker Angriff, Feuer, Diebstahl, Verlust
- Wie?
  - Externe Festplatte, USB-Stick, DVD
  - Ausdruck (Passwortliste)
  - Verschlüsselung?
- Wo?
  - Geschützter Ort vor Hitze/Kälte/Feuchtigkeit
  - Safe (Bank?)

Betriebssysteme (Desktop)

Windows oder Linux?

- Windows
  - Autom. Updates nur von Microsoft Produkten
    - Nur monatlich
  - Standard: Sendet viele Daten an Microsoft
  - Beliebtes Angriffsziel
- Linux
  - Automatische Updates für jede Software
    - Schnelle (sofort) Updates
  - Geringe Verbreitung → Angriffe unattraktiv
  - Kostenlos

Windows

- Updates!
- Anti-Viren Programm installieren
- Java/Flash nur wenn benötigt
- Dateierweiterungen anzeigen
  - liebes_bild.jpg.exe
- Office: Makros deaktivieren (Standard)
- Benutzerkontensteuerung beachten

Smartphones

Apps

- Apps aus vertraueneswürdigen Quellen
  - PlayStore, AppStore, F-Droid, …
- Angeforderte Rechte überprüfen
  - → Taschenlampe App braucht kein Internet
- Auf Bewertungen achten

Diverses

- Wie immer: Updates!
  - Betriebssystem + Apps
- Android: Custom Roms wenn keine Update mehr angeboten werden
  - LineageOS (früher CyanogenMod)
- Banking keine 2-Faktor Authentifizierung
- System Verschlüsselung

WLAN

WLAN offen/privat?

- WLAN → Funk → Abhörbar
- Offenes WLAN (Gastronomie, ...)
  - Rechtliche Fragen
- Verschlüsseltes WLAN (Privat, Firma)
  - WEP (unsicher)
  - WPA/WPA2 (sicher)

WLAN

- Absichern:
  - Verschlüsselung: WPA2
  - Sicheres WLAN Passwort
  - Standard Admin Login Passwort ändern
- Sinnlos: MAC-Adressen Filter
- Zusätzlich: Port Weiterleitungen

SmartHome
Internet of Things

oder Internet of Shit?

- Praktisch aber auch sicher?
- Vorteile:
  - Automatisierung
  - Strom sparen
- Nachteile:
  - Noch mehr Updates…
  - Mehr vom Hersteller abhängig
  - Noch mehr Einfallstore

Schöne oder Horror Zukunft?

- Hacker Angriffe
  - DDoS-Attacke auf Heizungssteuerung
  - ZigBee-Wurm befällt smarte Glühbirnen
  - Hacker übernehmen Kontrolle über Thermostat
- Mögliche Szenarien
  - Große Blackouts durch SmartMeter Hacks
  - Massenüberwachung bis ins Schlafzimmer
  - Rießige DDoS-Angriffe durch IoT

Empfehlung

- Abwarten
- Nur unkritische Dinge automatisieren
- Muss alles ins Internet?
- Update Garantie wenn möglich
- Nicht am falschen Ende sparen

Zusammenfassung

- Nutzt sichere Passwörter
- Installiert ALLE Updates!!!
- Nachdenken bevor man wo draufklickt
- Ein Anti-Viren Programm reicht nicht
- WLAN → WPA2 Verschlüsselung
- SmartHome/IoT → Zukunft wird lustig bzw der Horror

Ernsthaft!!!

- Nochmals:
- Macht eure Updates!!!
- Damit sind >90% aller Sicherheits-Probleme behoben

Fühlst du dich jetzt sicherer?

KONTAKT:
rupprecht.thomas@gmail.com