LmM Präsentation

"Wie schütze ich mich gegen Bedrohungen?"

- Computer Basics

- Ein paar Begriffe zum Aufwärmen

- Spam: Unerwünschte Mail
- Virus: Schadsoftware die sich selbst repliziert über mehrere Systeme übertragen kann
    - Pop-Ups, Performance, beschädigte/fehlende Dateien
- Malware: Invasive Schadsoftware die sich meist durch Störungen/Schäden bemerkbar macht
    - Performance, Speicherplatz, Programmänderungen/Pop-Ups
- Spyware: Beschaffung persönlicher Informationen
    - Änderung der genutzten Suchmaschine, Weiterleitung zu falschen Websites, Performance
- Spoofing & Phishing: Vortäuschung/Nutzung vermeintlich echter Websites & Absender

- Verständnis für Updates (System & Applikationen)

- Windows System Updates
- AV Programm
    - Erkennung/Prävention bei bekannter oder vermeintlicher Schadsoftware
    - Bezahlen oder nicht?
- Aktualisierung anderer Programme & Automatisierung von Updateprozessen

- Wie kommt es zu einem Angriff?

- Übertragung von infizierten Dateien
    - .exe; .zip; .doc; .pdf; etc.
    - USB- Stick
- Aufruf von falschen Websites

- E-Mail Sicherheit

- Email Spoofing & Phishing

- Ziel: Anmeldeinformationen gewinnen oder Schadsoftware einspielen
- Durchführung: Benutzer öffnet Anhang oder nutzt einen vermeintlich legitimen Link
    - Anhänge sind meist .pdf oder .zip Dateien
- Erkennung anhand von Beispielen
- Was tun bei eingegebenen Benutzerdaten / getätigten Downloads?
    - Passwort beachten, vom Netz trennen, Computer checken/lassen, Backup nach Entfernung, Meldung
- Prävention von zukünftigen Versuchen

- Passwörter

- Best Practice

- “Starke Passwörter” (min. 8 char - letters, numbers, symbols - changed frequently)
- Verwendung personenbezogener Daten & allgemein bekannter Wörter
- Teilen von Passwörtern
- Verwendung von Passwörtern für mehrere Dienste
    - Warum? Angreifer sind nicht dämlich
- Beispiele für schwache/starke Passwörter