FACHHOCHSCHULE
WIENER NEUSTADT
Austrian Network for Higher Education

IT-Sicherheit

Technische Policy

Eingereicht von: **Christy Kariyampalli**

Matrikelnummer: **52010080**

am **Fachhochschul-Bachelorstudiengang Informatik**

Informatik

Begutachter: **Bleier Thomas und Marcel Turobin-Ort**

Wiener Neustadt, 19. Mai 2023

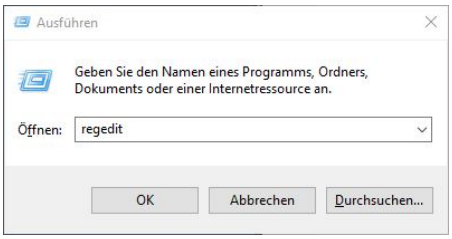
Inhaltsverzeichnis

1 System, Updates, Richtlinien

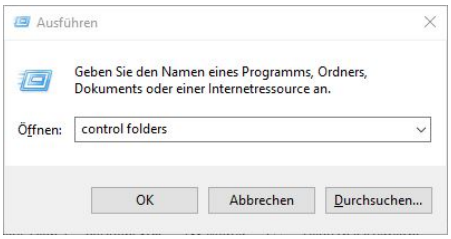
- Regelmäßige Updates (OS, Antivirus, usw.), am besten automatische Aktualiesierung einschalten
- PowerShell Richtlinien überprüfen, um das Ausführen von bestimmten Skripts usw. zu vermeiden (Policies)
- Skripts und sonstige Befehle über Command Line oder PowerShell müssen mit bedacht ausgeführt werden, am besten mit jemanden abgesprochen werden
- Schlüsseln und Verschlüsselungsmethoden verwenden, wenn es benötigt wird
- Bei einer möglichen „Infektion“ oder bei merkwürdigen Ereignissen das Netzwerk trennen und dementsprechende Sicherheitsmaßnahmen leiten
- Nur an vertrauenswürdige Netzwerke verbinden
- Firewall aktivieren und passende Einstellungen verwenden
- Abgeschottete Umgebungen verwenden (Virutalboxen)

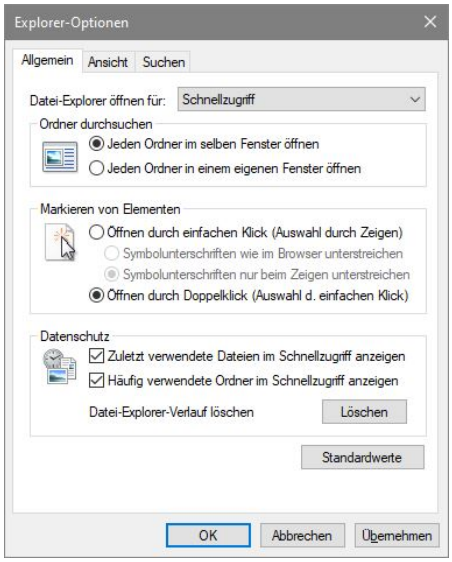
2 Dateien und Software

- Dateien vor dem öffnen über eine dritt-partie Software analysieren
- Deaktivierung von Makros und OLE-Objekten in MS-Office:
  Irgendein MS-Office Produkt öffnen (z.B. PowerPoint) - Datei - Optionen - Trust Center
- Einschränkung bzw. Deaktivierung des Windows Script Hosts (WSH):



  1-Aktivieren und 0-Deaktivieren (Dateienundung mit vbs werden unterdrückt).
- Einsatz von Application-Whitelisting, z. B. mittels Microsoft AppLocker (Wird auch nicht gemacht, weil nur ein Rechner verwendet wird)
- Dateien/Explorer Optionen Konfigurieren





- Nicht bekannte Dateien und Software nicht öffnen/starten

3 Emails und Accounts

3.1 Account/Sicherheit

- Starke (Guidlines) und verschiedene Passwörter verwenden (Accounts sollen auch bestmöglich variieren)
- 2-Faktor-Authentifizierung für alle möglichen Accounts einschalten
- Rollenbasiertes User Management. Bestimmte User können nur bestimmte Aktionen ausführen, bei Fehlverhalten wird der jeweilige User ausgeschlossen (Active Directory usw., wird nicht gemacht, weil nur ein Rechner verwendet wird).
- Passwörte sicher aufbewahren (KeePass oder sinstige Tools) und nicht am Platz liegen lassen oder wegschmeißen (Notizen mit Passwörtern)

3.2 Emails und Bedrohungen

- Empfangene Emails überprüfen und verifikationen Methoden einstellen
- Adressen der empfangenen Email überprüfen (Links, Emailadresse, URL's usw.)
- Dateien und sonstige Links nicht öffnen, außer von seriösen Quellen
- Geöffenete Dateien und Links sicher öffnen durch dritt-Parie Anwendungen, in einer Sandbox und mit Virenscanner laufen lassen