Windows Defender Exploit Guard - Deployment Handbuch

Dieses Handbuch beschreibt die Schritte zur Aktivierung von Windows Defender Exploit Guard-Komponenten, inklusive ASR-Regeln, kontrolliertem Ordnerzugriff, Netzwerkschutz und der Deaktivierung netzwerkbezogener Windows-Dienste.

1. PowerShell-Skript: ExploitGuard_Setup.ps1

Dieses Skript aktiviert:

- Network Protection
- Kontrollierten Ordnerzugriff
- Attack Surface Reduction (ASR) mit den folgenden Regeln:

  - D4F940AB-401B-4EFC-AADC-AD5F3C50688A
    (Office-Makros aus dem Internet blockieren)
  - 3B576869-A4EC-4529-8536-B80A7769E899
    (Skriptausführung durch Office-Anwendungen blockieren)
  - 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
    (Ausführen nicht signierter EXEs aus dem Download-Ordner blockieren)
  - 26190899-1602-49E8-8B27-EB1D0A1CE869
    (Credential-Stealing blockieren)

Ausführung: Als Administrator starten

2. Registry-Datei: Disable_NetworkDiscovery_Services.reg

Diese Datei deaktiviert folgende Dienste:

- SSDP Discovery (SSDPSRV)
- UPnP Device Host (upnphost)
- Function Discovery Resource Publication (FDResPub)

Diese Änderung verhindert Netzwerkkennung und WS-Discovery-basierte Kommunikation.

3. Gruppenrichtlinien (GPO)

Manuelle Konfiguration:

a) ASR-Regeln:

Pfad:

Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows Defender Antivirus > Windows Defender Exploit Guard > Angriffsschutzflächenreduktion

Richtlinie:

"Regeln für Angriffsschutzflächenreduktion konfigurieren"

Werte:

D4F940AB-401B-4EFC-AADC-AD5F3C50688A|1

3B576869-A4EC-4529-8536-B80A7769E899|1

75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84|1

26190899-1602-49E8-8B27-EB1D0A1CE869|1

b) Network Protection:

Pfad:

Windows Defender Antivirus > Netzwerkschutz

Richtlinie:

"Netzwerkschutz aktivieren" -> Aktiviert

c) Kontrollierter Ordnerzugriff:

Pfad:

Windows Defender Exploit Guard > Kontrollierter Ordnerzugriff

Richtlinie:

"Kontrollierten Ordnerzugriff konfigurieren" -> Aktiviert

Dieses Handbuch ist Teil des Deployment-Pakets "ExploitGuard_Deployment.zip".