Praxistipps für den Windows Defender

Einleitung Rolf Gutzwiller mit Praxisbeispiel NZZ

Microsoft Defender ist eine in Windows integrierte Sicherheitsanwendung, die den PC vor Malware, Viren, Ransomware und anderen Bedrohungen schützt. Früher war der Windows Defender, der heute zu Microsoft gehört, tatsächlich kein gutes Schutz-Tool für Windows. Heute wird der kostenlose Schutz von vielen sehr geschätzt, wobei der Defender das Windows-System unnötig langsam macht. Denn er nimmt standardmässig beim Scannen 50 Prozent der Prozessorleistung in Anspruch. Wie Sie den Defender beschleunigen und gleichzeitig die Sicherheit garantieren, wird hier gezeigt.

a. **Virenschutz, Sicherheit**

Sicherheitsprofile
Ransomware: auch oneDrive schützen!

b. **Geräteintegrität**

Geschützte Ordner des Systems/ oder eigenes Profil
Spezialprüfung der Ordner

c. **Firewall**

Firewall ist ein integrierter Bestandteil von Windows, der dazu dient, eingehenden und ausgehenden Netzwerkverkehr zu kontrollieren und zu schützen, indem sie den Netzwerkdatenverkehr filtert und nicht autorisierten Zugriff blockiert. Es verringert das Risiko von Netzwerksicherheitsbedrohungen, indem der Datenverkehr basierend auf verschiedenen Eigenschaften wie IP-Adressen, Ports oder Programmpfaden eingeschränkt oder zugelassen wird
Man kann auf erweiterte Einstellungen für verschiedene Netzwerktypen zugreifen, einschließlich Domänen (Arbeitsplatz), private (vertrauenswürdige) und öffentliche (nicht vertrauenswürdige) Netzwerke.

Konfigurieren der Windows-Firewall, Windows-Sicherheit

d. **Integriertes Phishing-Modul in Edge: Konkurrenzbrowser werden ausgeschlossen**

Möchte man auch andere Browser als Edge verwenden, muss man Defender deinstallieren und andere Schutzprogramme installieren.

Tabelle: Liste guter Schutzprogramme und deren Eigenschaften

Praxis: Vorstellung von Defender: Einstellungen bearbeiten

Virenscan: automatische Scanhäufigkeit ändern
Updates beschleunigen
Smartscreen eistellen
Smart App Control einstellen

Schluss: Quizz, Rolf Gutzwiller