

Windows-Sicherheit (Enterprise)

Fefe / Windows-Boardmittel-Sicherheit

<https://blog.fefe.de/?ts=9c40177c?css=fefe.css>

Ich halte das hier mal fest, geht um [diese Präsentation](#).

Meine Vermutung ist, dass es sich dabei noch um OnPrem-Umgebungen handelt.

1. Software Restriction Policies
2. Office Makros ganz weg (Inklusive Plugins und Software die noch darauf beruht)
3. Zitat: "NTLM Auth weg, Credential Caching für Admins und generell Server abschalten, Debugging Rechte global abschalten und nur im Einzelfall erlauben. LAPS benutzen, auch für Server."
4. [ESAE](#)
5. Hardwarekeys bzw. Smartcards für Admins (damit es keine Keylogger Passwörter gibt)
6. Exchange Split Permissions
7. Backup ohne Domänenmitgliedschaft, Firewall so dass Nur Backup zum Server kann aber nicht andersrum

Grundkonzept

Das unsicherste ist für den Anwender das bequemste, und demnach auch das vom Anwender bevorzugte.

Alle Sicherungsmaßnahmen machen den eigentlichen Umgang mit dem System unbequemer. Daher ist die ideale Sicherheit ein Kompromiss aus Sicherung und Bequemlichkeit.

Domänenabsicherung

1. Fullcloud-Entra / Exchange Online ohne Hybridbetrieb erreichen.
2. Zentrales User-Management via Microsoft Entra
3. Single-Sign-On aus Entra-Daten (weil: Psychologie: Müssen viele Accounts gepflegt werden, wird das gleiche Passwort überall verwendet)

4. Multifaktor-Authentifizierung mit Hardwarekeys (idealerweise via Biometrie) für alle Microsoft Entra Accounts.
 - Alternativ: Multifaktor mit Windows 11 & TPM-Chip der Mainboards.

Danach kommen Dinge wie Patchmanagement etc.

Der Angreifer ist der, der beim unbedarften Anwender anruft, weil er einen Schriftverkehr dazu aus der vorne an der Straße stehenden Papiertonne gefischt hat.

Version #16

Erstellt: 2022-07-08 07:24:50 UTC von Konstantin

Zuletzt aktualisiert: 2023-11-24 12:36:06 UTC von Konstantin