michael wessel
it performance

Materialliste zum heise-Webinar „Windows 10 sicher im Unternehmen“

Webinar vom 29. April 2020, Aufzeichnung: https://www.heise-events.de/webinare/windows_10

- **Kontaktinformation Nils Kaczenski**
  - nka@michael-wessel.de
  - Blog: https://www.michael-wessel.de/blog/
  - Community-Blog: https://www.faq-o-matic.net/
- **Standards und Richtlinien**
  - Windows 10 und Telemetrie - neue Erkenntnisse
    - https://www.lda.bayern.de/media/baylda_report_09.pdf
  - BSI-Empfehlungen zu Windows 10
    - SiSyPHuS Win 10 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html
    - Grundschutz-Kompendium https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6
  - c't: Checkliste Datenschutz
    - https://www.heise.de/select/ct/2019/26/1576522305110949
  - gp-pack (kommerziell; gruppenrichtlinien.de)
    - https://www.gp-pack.com/
  - Security Compliance Toolkit
    - https://docs.microsoft.com/de-de/windows/security/threat-protection/security-compliance-toolkit-10
- **Admin-Prozesse**
  - Rollout, Upgrades, Updates
    - Mark Heitbrink - Wer hat Angst vorm SAC Update? - cim lingen 2019
  - Editionen und ihre Eignung
    - Feature-Vergleich: https://www.microsoft.com/en-us/WindowsForBusiness/Compare
    - Vollständig: https://go.microsoft.com/fwlink/p/?linkid=2089903

- **Sicherheits-Funktionen**
  - Überblick
    - https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-enable-security-features
    - https://docs.microsoft.com/en-us/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10
  - Bitlocker
    - AD-Integration: https://www.gruppenrichtlinien.de/artikel/bitlocker-mit-tpm-einrichten-speicherung-des-wiederherstellungsschluessel-im-active-directory/
    - Utilman-Angriff
      - https://www.faq-o-matic.net/2011/02/03/admin-kennwort-ganz-einfach-zurcksetzen/
  - DeviceGuard
    - https://techcommunity.microsoft.com/t5/iis-support-blog/windows-10-device-guard-and-credential-guard-demystified/ba-p/376419
    - https://www.gruppenrichtlinien.de/artikel/device-guard-windows-defender-application-control/
  - CredentialGuard
    - https://www.gruppenrichtlinien.de/artikel/credential-guard-schutz-vor-pass-the-hash/
  - Remote CredentialGuard
    - https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard
  - Windows Hello for Business
    - https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview
  - Windows Defender Antivirus
    - Management: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/deploy-manage-report-windows-defender-antivirus
    - AMSI-Testskript: http://www.pastebin.com/raw.php?i=JHhnFV8m
  - UAC Best Practices
    - https://www.faq-o-matic.net/2008/02/22/benutzerkontensteuerung-uac-richtig-einsetzen/
    - https://www.faq-o-matic.net/2015/12/23/windows-berechtigungen-mit-uac-verwalten/

- AppLocker
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
  - Probleme von Pfad-Regeln: https://www.gruppenrichtlinien.de/artikel/applocker-oder-software-restriction-policies-loecher-im-sicherheitszaun/
  - Ordner in %systemroot%, auf die ein normaler Benutzer Schreibrechte hat:

    C:\Windows\Registration\CRMLog
    C:\Windows\System32\FxsTmp
    C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys
    C:\Windows\System32\spool\drivers\color
    C:\Windows\SysWOW64\FxsTmp
    C:\Windows\Tasks
    C:\Windows\tracing
- Exploit Protection
  - https://docs.microsoft.com/de-de/windows/security/threat-protection/microsoft-defender-atp/exploit-protection
  - https://www.gruppenrichtlinien.de/artikel/ransomware-schutz-attack-surface-reduction-asr-windows-defender-exploit-guard/
  - https://www.gruppenrichtlinien.de/artikel/exploit-guard-exploit-protection-emet-lebt/
  - Demo-Webseite Network Protection: https://demo.wd.microsoft.com/Page/NP
  - Testskripte für Protection-Regeln: https://demo.wd.microsoft.com/
  - Der Grund, warum die Demo mit dem Ransomware-Trojaner im Webinar fehlschlug: Ich hatte das Skript, das die Regeln aktiviert, vorher manipuliert, sodass es unwirksam war. Im Webinar habe ich dann versehentlich diese falsche Version aufgerufen.

- **Security Worst Practice**
  - Typische Netzwerke übernehmen
    https://www.youtube.com/watch?v=qk9GW4E94R8
  - DOS-Angriff für jedermann, Ursache: Kontensperrung bei falscher Kennworteingabe
    https://www.faq-o-matic.net/2013/08/07/dos-angriff-fr-jedermann-ad-konten-sperren/
  - Kennwortfilter für Active Directory
    - Achtung: Es gibt einen Grund, warum es so wenige Produkte für diesen Zweck gibt. Kennwortfilter laufen innerhalb des LSASS-Prozesses auf Domänencontrollern, man muss ihnen also voll vertrauen können. Jeder Programmfehler kann fatale Auswirkungen auf die Unternehmenssicherheit haben.
    - https://www.qwant.com/?q=windows+password+filter+active+directory&client=opensearch
    - https://github.com/raandree/ManagedPasswordFilter
- **Windows-Sicherheit heute**
  - ESAE und Administrative Tiering
    - Überblick zum Thema:
      https://www.michael-wessel.de/blog/2018/05/17/cdc-germany-in-roten-und-goldenen-wldern/
    - Referenzdesign von Microsoft:
      https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material