IT-PRO-BERLIN.DE

Frühlingserwachen

2021 edition

Microsoft® MVP Most Valuable Professional

Get-SpeakerInfo -Brief

- **Name:** Evgenij Smirnov
- **YearOfBirth:** 1972
- **JobTitle:** { Consultant, Solutions Architect }
- **TwitterID:** @cj_berlin
- **Employer:** SVA System Vertrieb Alexander GmbH
- **MVP:** { 2020 }
- **Certifications:** { MCSE, MCSA, VCP:2, VCAP, VCIX, CCA, QCIC }
- **UserGroups:** { WSUG-B, EXUSG, PSUGB, BerlinVMUG }

ICH HASSE IT-SECURITY

- **Ein Fass ohne Boden**

ICH HASSE IT-SECURITY

- **Ein Fass ohne Boden**
- **Den Angreifern ist es egal,**
  - wie fleißig die Security-Admins die ganze Zeit gewesen sind
  - dass man dieses System in der Frozen Zone nicht patchen darf
  - dass es nur ein Testsystem ist
  - dass es nur für eine Übergangszeit gedacht ist
  - dass es demnächst abgelöst werden soll
  - dass es nur von intern erreichbar ist
  - dass es von Drittfirma betreut wird
  - dass es letzte Woche einen Pentest gab ;-)

IMMER OPTIMISTISCH BLEIBEN!

- **Jeder Angriff ist ein *(kleines)* Geschenk an die Verteidigung.**
- **Von Opfern lernen heißt nicht Verlieren lernen.**
- **SoloriGate zeigt:**
  - DevOps-Toolchain ist der beste Angriffspunkt…
  - …like, **ever**
- **Baron Samedit zeigt:**
  - nur weil etwas schon immer da war… ;-)
- **#shitrix und BlueKeep zeigen**
  - der Perimeter lebt!
- **EWS Subscription-Lücke zeigt:**
  - Remote war auch vor der Pandemie wichtig
  - Split Permissions tun nicht (wirklich) weh

GESTERN WAR DIE ANTWORT: CLOUD

- **Heute ist die Antwort: Zero Trust. Auch in der Cloud. Und morgen?**
- **Das heutige Konzept greift auch noch zu kurz, aber es gibt heute halt nichts Besseres.**
- **Zero Trust → Mikrosegmentierung**
  - Einfachste Regel: Client Isolation. Kann jedes Hotel-WLAN.
  - „KI-basierte“ Lösungen setzen einen „known good“ bzw. „known clean“ Zustand voraus.
- **Mikrosegmentierung mit der Windows Defender Firewall?**
  - Ja, schon, aber man muss seine Netze kennen ;-)
  - Ja, fummelig, aber per Group Policy durchaus beherrschbar
  - Die Verwaltung dieser GPOs muss sehr präzise delegiert werden

PATCH!

- **PATCH!!**
- **PATCH!!!!**
- **PATCH!!!!!!!!**
- **Nicht nur Windows!**
  - siehe HeartBleed…
  - …oder Baron Samedit
- **Es wird immer schwieriger, konkrete Microsoft-Patches konkreten Schwachstellen zuzuordnern**
  - und durch CU Servicing wird das auch immer unmöglicher ;-)
- **Um so wichtiger ist eine Test-Strategie!**

IS PASS-THE-HASH OVER YET?..

- **Moderne Betriebssysteme → Credential Guard**
  - Nur mit Device Guard (VBS) wirklich wirkungsvoll!
  - Schützt nur die native Windows-Anmeldung
- **Go f***ing passwordless!**
  - ~~*oft*~~ meistens leichter gesagt als getan ;-)
  - das letzte verbliebene System ist für Interessierte gut genug
- **Und was ist mit meinen Service-Accounts?**
  - mit Computer-Identität und CBA arbeiten
  - gMSA, wo möglich und sinnvoll (schützt nicht per se)
  - nicht im Gott-Modus betreiben!

IS EMET DEAD?

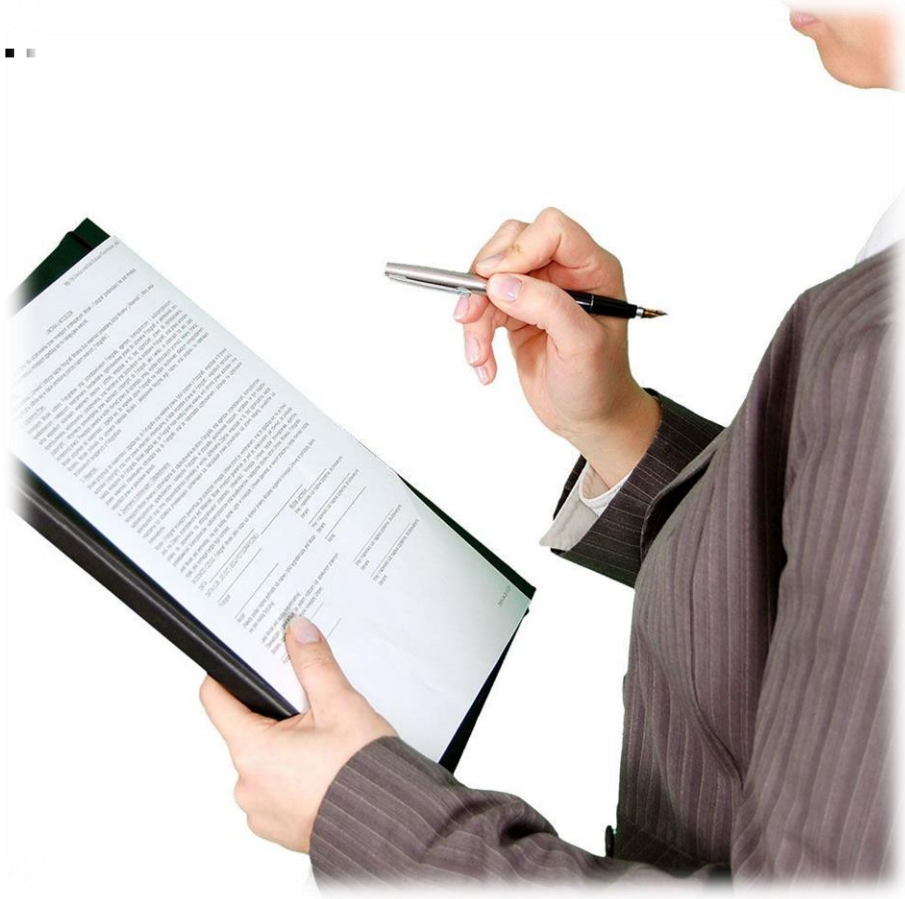
- **(sort of) wiedergeboren als ASR**
- **https://docs.microsoft.com/de-de/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction**
- **Wer einen M365-Vertrag hat, kann richtig profitieren, besonders mit E5**
- **Alle anderen: Selbst ist der Mann!**
  - GPO ist im Standard enthalten (Ab 1709, ab Pro)
  - oder **`Add-/Set-MpPreference`**
  - Audit Mode ist möglich
  - Einrichtung ist fummelig
  - Event Logs müssen eingesammelt und/oder überwacht werden

IS APP ~~WHITE~~ALLOWLISTING DEAD?

- **Keineswegs! Mit Defender Application Control mächtiger als je zuvor ☺**
  - Königsklasse: Kernel Driver!
  - Beste Combo: ~~White~~Allowlisting mit WDAC und Black Denylisting mit AppLocker
- **Default-Rules von AppLocker tun (meistens) nicht weh und helfen etwas**
  - es gibt auch heute noch ein Paar Pfade, die schreibbar sind!
- **Goldene Regeln der Dateiausführung sind eine sinnvolle Ergänzung**
  - besonders, wenn man erst am Anfang des ~~White~~Allowlistings steht…
  - …und schließlich ist Linux damit bisher um ~~White~~Allowlisting herumgekommen ;-)

AUDIT UNTIL YOU DROP

- **Konfigurationsanalysen → CIS, SCT, PingCastle…**
  - Baseline entwickeln
  - Einmal 100% erreichen
  - Ab dann ist es leichter
- **Zugriffsrechte**
  - Lokal, speziell auf Dev-Clients (Solorigate!)
  - AD (Bloodhound, GoldFinger, DIY…)
- **Event Logs**
  - Irgend‘ne Art SIEM braucht heutzutage jeder
  - Im Zweifel… 42
- **Vulnerability scans**
  - Nessus, Rapid7, …



GOOD HUNTING!

Ihr habt ja sonst nichts zu tun…