Herzlich Willkommen!!!

Frühjahrsputz: So bereinigen Sie Ihr Active Directory (Active Directory Härtung mit einfachen Mitteln)

ACP

IT for innovators.

Markus Greiner

Senior Consultant

markus.greiner@acp.de

+49 8586 9604185

+49 173 5894741

IT for innovators.

Agenda:

- Allgemeine Informationen zur aktuellen Bedrohungslage
- Rechtliche Informationen
- Wie funktioniert ein Großteil der Angriffe?
- Welche Schwachstellen werden ausgenutzt?
- Wie identifiziert man alte Objekte im AD?
- Welche Tools können dabei helfen?
- Ein erster Schritt wurde unternommen, welche folgen noch?
- Unser Geschenk an Sie
- Q&A

IT for innovators.

Allgemeine Bedrohungslage

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund **116,6 Millionen** zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

nach Angriff auf Satellitenkommunikation

20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

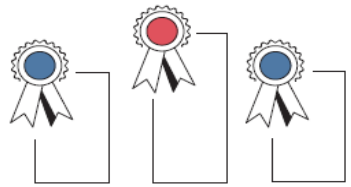
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.



BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.

4.400 (2020) → **5.100** (2021)

Zehn Jahre Allianz für Cyber-Sicherheit: 2022 sind wir bereits **6.220 Mitglieder.**

Bundesamt für Sicherheit in der Informationstechnik

Deutschland **Digital•Sicher•BSI•**

- Die Bedrohungslage ist so hoch wie nie
- Es ist keine Frage, ob man angegriffen wird, sondern wann!!
- Der Großteil der Angriffe ist automatisiert
- 50% der Opfer kommen aus dem Mittelstand (SMB)
- 60% der Opfer bezahlen
- Die weltpolitische Lage ist schwierig

Rechtliche Einschätzung:

Cyberattacken rücken das Verhältnis von IT-Sicherheit und Strafrecht in den Blickpunkt

Artikel unter: https://www.unternehmensstrafrecht.de/cyberattacken-ruecken-verhaeltnis-von-it-sicherheit-und-strafrecht-in-den-blickpunkt/?fbclid=IwAR22rVq4%E2%80%A6

Fazit

Die Cyberattacke auf das Uniklinikum in Düsseldorf ist ein aktuelles Beispiel, das unterstreicht, wie wichtig es für jedes Unternehmen ist, sich mit den Bausteinen einer wirksamen IT-Compliance auseinanderzusetzen. Bislang konzentrierten sich die Staatsanwaltschaften bei Ransomware-Attacken auf die Angreifer. Es nicht auszuschließen, dass sie in Zukunft die strafrechtlichen Ermittlungen auch auf das Innenleben des angegriffenen Unternehmens ausweiten.

Sollten dabei eklatante Mängel bei der Compliance und IT-Sicherheit aufgedeckt werden, ist es wahrscheinlich, dass sich Strafverfahren künftig auch gegen Verantwortliche des Unternehmens richten. Das bedeutet, dass es beim Umgang mit der IT-Sicherheit in Zukunft möglicherweise nicht mehr nur um die Vermeidung von Geldbußen etwa nach der DSGVO gehen wird. Sondern dass es gilt, echte Strafen zu vermeiden.

Wie funktioniert der Großteil der Angriffe?

stark vereinfacht am Beispiel des Bundestagshacks 2015

I. Auf mehreren Rechnern werden durch das einschleusen eines Trojaners lokale Admin Rechte erlangt (~Dezember 2014)
II. Durch die lokalen Admin Rechte konnte mit Tools wie Mimikatz gearbeitet werden
III. Abwarten bis sich jemand mit Domain Admin Rechten auf den Rechner verbindet (ab hier ist die Domäne verloren).
IV. Pass the hash mit Mimikatz

    mimikatz.exe ausführen (alternativ mimidogz)

    privilege::debug

    sekurlsa::logonpasswords

    NTLM Hash * NTLM   : 494cafd53a5d741516003ee021b80d81

V. Ausführung von Powershell mit Domain Admin Rechten

    sekurlsa::pth /user:lab-admin /domain:sws-lab /ntlm:494cafd53a5d741516003ee021b80d81 /run:powershell.exe

VI. Partytime!!!

Was macht einen Angriff einfach?

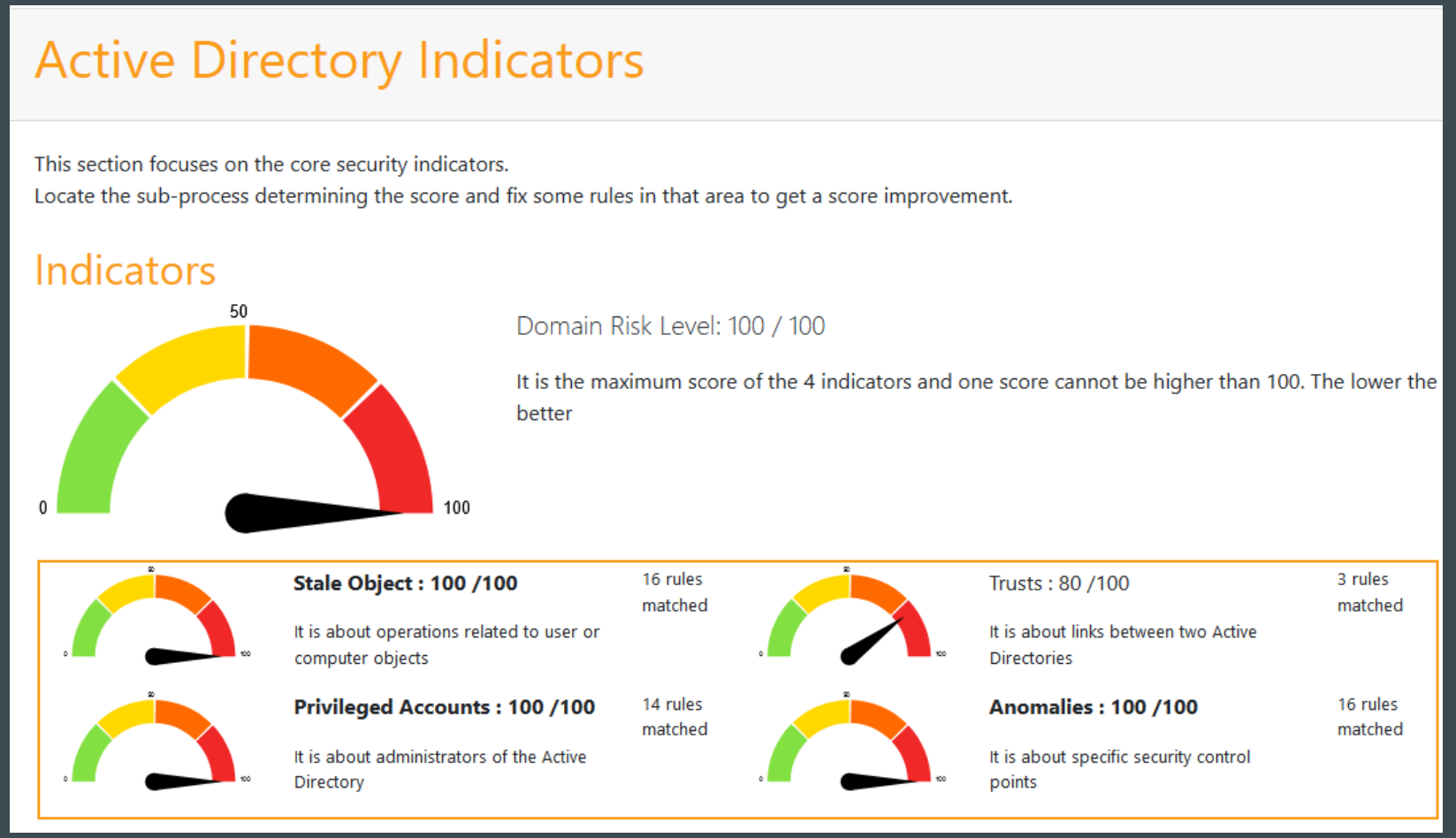
- Unzureichende Planung der Sicherheitsgrenzen
- Zu viele oder nachlässige Vertrauensbeziehungen
- Fehlende Sicherheitsfunktionen durch ältere Betriebssysteme und Domänen- und Gesamtstruktur-Funktionsebenen
- Betrieb weiterer Rollen und Dienste auf Domänencontrollern
- Unzureichende Überwachung und Dokumentation von delegierten Rechten
- Unsichere Authentifizierung
- Zu mächtige oder schwach gesicherte Konten
- Nutzung desselben lokalen Administrierenden-Passworts auf mehreren IT-Systemen
- Unsichere Speicherung von Passwörtern

  https://www.sans.org/blog/protecting-privileged-domain-accounts-lm-hashes-the-good-the-bad-and-the-ugly/
- Unzureichende Absicherung von Domänencontrollern
- Hinterlassen von hochprivilegierten Anmeldeinformationen auf Domänenmitgliedsservern und –clients

  https://www.gruppenrichtlinien.de/artikel/cached-credentials-entmystifiziert-kein-pth-moeglich
- Hinzufügen nicht vertrauenswürdiger IT-Systemen zur Windows-Domäne
- Vermaschung von administrativen Privilegien durch Integration von weiteren Anwendungen

Was können wir dagegen tun?

- Einführung einer Audit Software mit Secure Score und umsetzen der Best Practices und bereinigen der Active Directory



Stale Objects rule details [16 rules matched on a total of 36]

Presence of Windows 2003 = 7	+ 25 Point(s)
Number of accounts which can have an empty password (can be overridden by GPO): 1978	+ 15 Point(s)
1 domain(s) used in SIDHistory	+ 15 Point(s)
Number of computer without password change for at least 3 months: 92	+ 15 Point(s)
Presence of wrong primary group for users: 18	+ 15 Point(s)
Presence of Windows 2008 = 42	+ 15 Point(s)
Presence of non supported Windows 10 = 7	+ 10 Point(s)
Relatively high number of inactive computer accounts: 22% (more than 20% of all computers)	+ 10 Point(s)
SMB v1 activated on 35 DC	+ 10 Point(s)
Presence of Windows XP = 2	+ 10 Point(s)
Number of accounts which do not require kerberos pre-authentication: 2	+ 5 Point(s)
Presence of duplicate accounts = 4	+ 5 Point(s)
Number of computer without password change: 13	+ 5 Point(s)

Privileged Accounts rule details [14 rules matched on a total of 42]

Unconstrained delegations are configured on the domain: 205 account(s)	+ 1025 Point(s)
Number of GPO items that can be modified by any user: 3	+ 45 Point(s)
Everyone can take control of a key domain object by abusing targeted permissions.	+ 25 Point(s)
Presence of Admin accounts which do not have the flag "this account is sensitive and cannot be delegated": 17	+ 20 Point(s)
Presence of service accounts in the domain admin group (at least 2 accounts have a password which never expire): 6	+ 15 Point(s)
Presence of unknown account in delegation: 8	+ 15 Point(s)
A large number of users or computers can take control of a key domain object by abusing targeted permissions.	+ 15 Point(s)
Number of admin with a password older than 3 years: 9	+ 10 Point(s)
4 domain controller(s) have been found where the owner is not the Domain Admins group or the Enterprise Admins group	+ 10 Point(s)
Number of admins not in Protected Users: 20	+ 10 Point(s)
At least one member of an admin group is vulnerable to the kerberoast attack.	+ 10 Point(s)
The group Schema Admins is not empty: 2 account(s)	+ 10 Point(s)

Trusts rule details [3 rules matched on a total of 11]

5 unknown domain(s) used in SIDHistory	+ 50 Point(s)
At least one inactive trust has been found: 3	+ 20 Point(s)
Number of files deployed hosted in another domain: 2	+ 10 Point(s)

Anomalies rule details [16 rules matched on a total of 56]

Number of password(s) found in GPO: 16	+ 320 Point(s)
Last change of the Kerberos password: 1625 day(s) ago	+ 50 Point(s)
Suspicious admin activities detected on 44 user(s)	+ 40 Point(s)
At least one policy has been found where the LM hash can be used [1]	+ 5 Point(s)
At least one trusted INTERMEDIATE certificate found has a MD5 signature [1]	+ 5 Point(s)
The group Everyone and/or Anonymous is present in the Pre-Windows 2000 group.	+ 5 Point(s)
The old protocol NTFRS is used to replicate the SYSVOL share	+ 5 Point(s)
At least one user, computer or group has been added as a member to the PreWin2000 compatible group	+ 2 Point(s)
At least one trusted INTERMEDIATE certificate found has a SHA1 signature [1]	+ 1 Point(s)
A DNS Zone is configured with unsecure updates	+ 1 Point(s)
At least one trusted certificate found has a relatively weak RSA key [16]	+ 1 Point(s)

Nb User Accounts	Nb Enabled	Nb Disabled	Nb Active	Nb Inactive	Nb Locked	Nb pwd never Expire	Nb SidHistory	Nb Bad PrimaryGroup	Nb Passwor not Req.
8991	3823	5168	3071	752	0	1243	273	18	1

Showing 1 to 1 of 1 entries

Inactive objects (Last usage > 6 months)	*[752]*
Objects with a password which never expires	*[1243]*
Objects having the SIDHistory populated	*[273]*
Objects having the primary group attribute changed	*[18]*
Objects which can have an empty password	*[1978]*
Objects trusted to authenticate for delegation	*[168]*
Objects without kerberos preauthentication	*[2]*

Group Name	Nb Admins	Nb Enabled	Nb Disabled	Nb Inactive	Nb PWd never expire	Nb Smart Card required	Nb Service accounts	Nb can be delegated	Nb external users
Account Operators	0	0	0	0	0	0	0	0	
Administrators	17	15	2	3	8	0	1	15	
Backup Operators	3	2	1	2	2	0	0	2	
Certificate Operators	0	0	0	0	0	0	0	0	
Certificate Publishers	0	0	0	0	0	0	0	0	
Dns Admins	0	0	0	0	0	0	0	0	
Domain Administrators	14	13	1	2	6	0	1	13	
Enterprise Administrators	5	4	1	1	2	0	0	4	
Print Operators	15	13	2	2	6	0	1	13	
Replicator	0	0	0	0	0	0	0	0	

Ein Anfang wurde gemacht. Was dann?

- Einführung „least privileges administrative models“
- Privilegierte AD-Benutzer dürfen sich an Clients nicht anmelden
- Einführung LAPS
- Konfiguration von Überwachungsrichtlinien und hochdrehen der Protokollierung
- Konfiguration der Passwortrichtlinien
  → https://delinea.com/resources/password-strength-checker
- Überprüfung der bestehenden Passwörter (gegen Datenbanken wie „haveibeenpwnd“)
- Abschneiden alter Zöpfe wie LAN Manager (LM) und NT LAN Manager (NTLM) v1, SMB v1, LDAP und Einführung sicherer Verbindungen (z.B. IPSec)
- Einführung eines zweiten Faktors für die Authentifizierung (z.B. Cisco Duo, Helo etc.)
- Patchen, patchen , patchen…….
- Microsoft Tools (z.B. Credential Guard, APPLocker,usw.)

- Security Information Event Management System (SIEM z.B. Logpoint)
- Netze segmentieren
- Bitlocker Verschlüsselung
- Privileged Access Workstation (PAW)
- Privileged Identity Management (PIM)
- Privileged Access Management (PAM)
- Identity and Access Management (IAM)
- Solarwinds Access Right Manager (ARM)
- Penetration Tests
- Gruppenrichtlinien konsolidieren und Performance Analyse
- Honeypot
- Uvm.

PIM	PAM	IAM
Concentrates on the rights assigned (typically set by IT departments or System Admins) to various identities. Also assists in the control of unchecked IAM areas.	The layer that secures a certain access level and the data that can be accessed by a privilege. Maintains privileged identities under protection and ensures the ones with admin rights do not engage in abuse of privileges.	Applies to all users in the organization who have an identity, which will be monitored and handled. Keeps the overall network safe.

Unser Geschenk an Sie

- Sie erhalten von uns ein kostenloses AD Security Audit inclusive eines HTML-Dokuments
- Ebenso werden wir das Ergebnis und jeden Punkt auf dem Dokument mit Ihnen ausführlich besprechen.

Wir freuen uns, gemeinsam Ihren Secure Score wieder in den grünen Bereich zu führen.

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

IT for innovators.