TEAL
ALWAYS CHALLENGING IT

IN FÜNF SCHRITTEN ZUM MONATLICHEN SECURITY CHECK

WHITEPAPER

2023

Vorwort

Liebe Leserinnen und Leser,

spätestens seit diesem Jahr nimmt das Thema Cybersecurity in jedem Unternehmen einen enormen Stellenwert ein. Egal, ob DAX-Konzern oder KMU, es besteht Einigkeit, dass Hackerangriffe massiven Schaden in Unternehmen anrichten. Ob durch die erhöhte Nutzung von Remote Arbeit oder der Angst vor einer Erpressung durch eine Ransomware Attacke, es gibt mittlerweile einen Konsens, dass agiert werden muss. Wurde in der Vergangenheit meist nur reagiert und Sicherheitsmaßnahmen erst nach einem Vorfall eingeführt, so möchten sich immer mehr Unternehmen bereits im Vorfeld absichern und nicht erst, wenn es zu spät ist.

Ähnlich wie bei einem Haus kann man sich nicht zu 100 % vor einem Einbruch schützen. Jedoch ist es möglich, Einbrüche massiv zu erschweren und vor allem den potenziellen Schaden zu minimieren. Die TEAL Technology Consulting GmbH ist darauf spezialisiert, Unternehmen dabei zu unterstützen. Wir verbessern Ihre IT-Infrastruktur und deren Prozesse und steigern das Niveau Ihrer IT-Sicherheit nachhaltig. Wir gehen davon aus, dass wir nie JEDEN Angriff verhindern können (Assume Breach). Deswegen ist unser oberstes Ziel, Cyberattacken zu erschweren und deren Auswirkungen effektiv abzumildern.

In diesem Whitepaper möchten wir Ihnen eine Maßnahme erläutern, die wir jedem Kunden empfehlen, egal, ob das Thema Sicherheit gerade erst angegangen wird oder ob schon zahlreiche Maßnahmen umgesetzt sind. Wenn Sie ein Active Directory als zentrale Berechtigungs- und Identitätsverwaltung im Einsatz haben, dann erfahren Sie, wie man durch den monatlichen TEAL Security Check in wenigen Schritten die IT-Sicherheit in Ihrem Active Directory steigern kann.

Viele Grüße und Freude beim Lesen,

Fabian Böhm
(Geschäftsführer)

Erhöhen Sie Ihre AD-Sicherheit mit unserem monatlichen **TEAL Security Check**

Wenn Sie Active Directory als zentrale Identitätsverwaltung im Unternehmen einsetzen, ist es vermutlich historisch gewachsen oder hat sich ggf. durch Zu- oder Verkäufe immer wieder verändert. Nicht verwunderlich, wenn man bedenkt, dass Microsoft Active Directory bereits vor 20(!) Jahren Windows Server 2000 eingeführt hatte. Deswegen empfehlen wir unseren Kunden die Sicherheit des Active Directories kontinuierlich zu überprüfen und Verbesserungen umzusetzen.

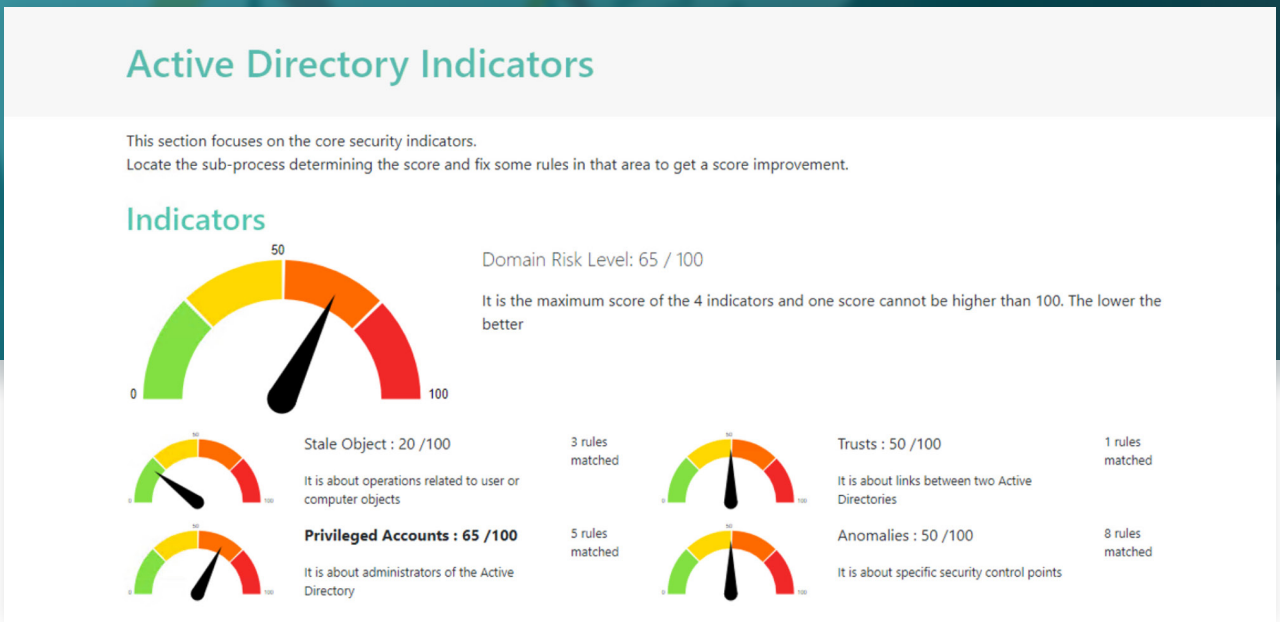
Der TEAL Security Check entdeckt effektiv Fehlkonfigurationen, gibt einen Überblick über die aktuelle Konfiguration und zeigt wichtige Maßnahmen auf, welche die Gesamtarchitektur verbessern. Der TEAL Security Check umfasst fünf wichtige Schritte, die monatlich ausgeführt werden sollten. Ist der Security Check etabliert und kann dieser kontinuierlich um weitere Prüfungen erweitert werden.

1. Active Directory: Gesamtüberblick **mit PingCastle**

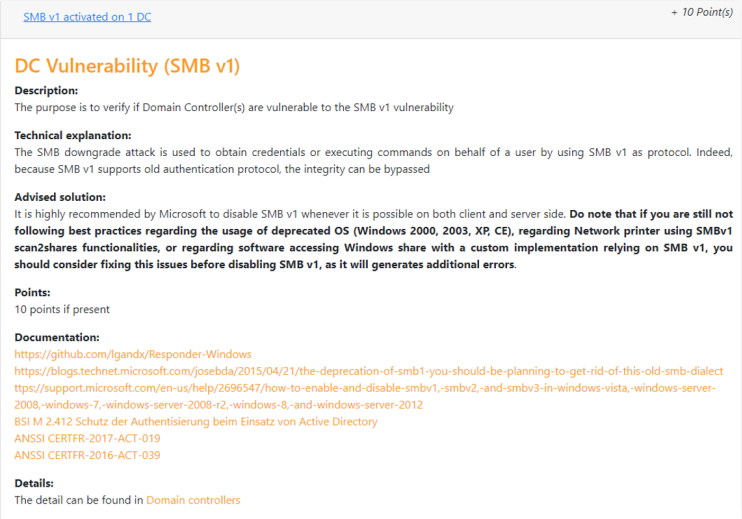
Name: PingCastle
Kosten: Kostenlose nicht kommerzielle Nutzung
Quelle: https://www.pingcastle.com/

Pingcastle wirbt mit dem griffigen Statement „Get Active Directory Security at 80% in 20% of the time.“ Unsere Erfahrung zeigt, dass es sich in den meisten Fällen durchaus bewahrheitet.
Geschrieben wurde Pingcastle von Vincent Le Toux, einem französischen Sicherheitsexperten, der unter anderem auch mimikatz (ein Tool mit dem Pass-the-Ticket/Pass-the-Hash Angriffe ausgeführt werden können) mitentwickelt hat. Für nicht gewerbliche Zwecke ist das Tool frei verwendbar, einfach auszuführen und fasst die Ergebnisse in einen HTML Report zusammen.

TEAL
ALWAYS CHALLENGING IT



Im Dashboard werden verschiedene Risk Scores dargestellt, die den Gesamtzustand des Active Directories verdeutlichen. Die einzelnen Indikatoren verändern sich nach Umsetzen der ersten Maßnahmen und das Gesamtrisiko sinkt. Daneben listet Pingcastle detailliert auf, was und vor allem wie etwas verbessert werden kann. Hier z.B. ein „beliebtes“ Finding zu SMB v1 auf einem der Domain Controller:



SMB v1 activated on 1 DC — *+ 10 Point(s)*

DC Vulnerability (SMB v1)

Description:
The purpose is to verify if Domain Controller(s) are vulnerable to the SMB v1 vulnerability

Technical explanation:
The SMB downgrade attack is used to obtain credentials or executing commands on behalf of a user by using SMB v1 as protocol. Indeed, because SMB v1 supports old authentication protocol, the integrity can be bypassed

Advised solution:
It is highly recommended by Microsoft to disable SMB v1 whenever it is possible on both client and server side. **Do note that if you are still not following best practices regarding the usage of deprecated OS (Windows 2000, 2003, XP, CE), regarding Network printer using SMBv1 scan2shares functionalities, or regarding software accessing Windows share with a custom implementation relying on SMB v1, you should consider fixing this issues before disabling SMB v1, as it will generates additional errors**.

Points:
10 points if present

Documentation:
https://github.com/lgandx/Responder-Windows
https://blogs.technet.microsoft.com/josebda/2015/04/21/the-deprecation-of-smb1-you-should-be-planning-to-get-rid-of-this-old-smb-dialect
ttps://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
BSI M 2.412 Schutz der Authentisierung beim Einsatz von Active Directory
ANSSI CERTFR-2017-ACT-019
ANSSI CERTFR-2016-ACT-039

Details:
The detail can be found in Domain controllers

Unsere Erfahrungen zeigen, dass in Unternehmen, bei denen Cyber-Sicherheit einen hohen Stellenwert einnimmt, aktiv gemanagt sowie stets an Größe und Anforderungen des Unternehmens angepasst wird, ein IT-Angriff bisher keine (großen) Auswirkungen hatte.“

Peter Wirnsperger,
Cyber Risk Leader Deloitte

Wir empfehlen, Pingcastle monatlich auszuführen und nach und nach die empfohlenen Maßnahmen zu bewerten und umzusetzen. So kann in kurzer Zeit die Sicherheit der Active Directory Gesamtstruktur massiv gesteigert werden.

Durch das Punktesystem kann auch dem Management sehr klar verdeutlicht werden, wie stark durch einzelne Maßnahmen das Gesamtrisiko abgesenkt werden kann.

TEAL
ALWAYS CHALLENGING IT

2. Detaillierte Berechtigungsanalyse **mit BloodHound**

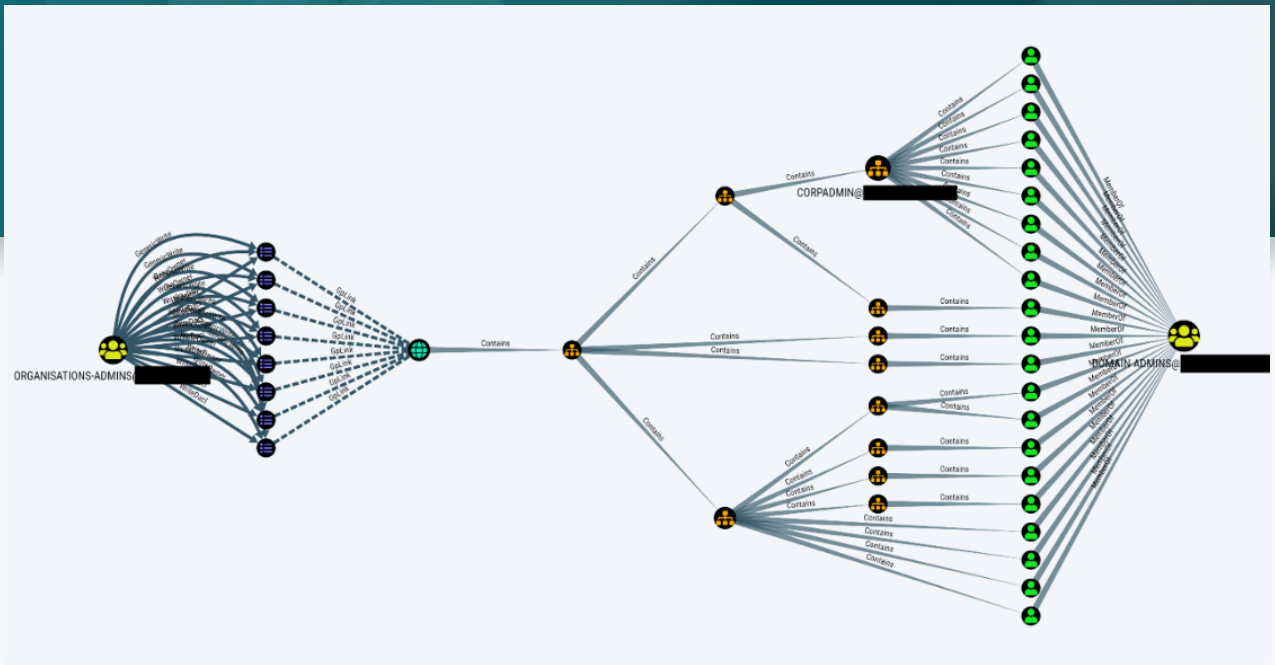
BloodHound ist nicht nur ein sehr effektives Werkzeug für Angreifer. Richtig eingesetzt ist es auch ein wirksames Hilfsmittel für Administratoren. Doch was ist BloodHound überhaupt?

Name: BloodHound
Kosten: Keine – open source
Quelle: https://github.com/BloodHoundAD/BloodHound

Das Open Source Tool wurde von Mitarbeitern von SpecterOps, einer sehr renommierten Security Firma aus den USA, entwickelt. Es sammelt Daten aus dem Active Directory ein, die Erkenntnisse über die komplexe Berechtigungsstrukturen liefern. Die Beziehungen können grafisch dargestellt oder mittels Datenbankabfragen ausgewertet werden. Wird BloodHound mit „normalen“ Benutzer-Berechtigungen ausgeführt, liefert es bereits zahlreiche Daten. Ab einer Windows Version >1607, wird zum Auslesen der aktiven Anmeldesessions jedoch ein lokales Admin Recht benötigt. Dennoch geben Daten, welche „nur“ mit Benutzerrechten eingesammelt wurden, bereits einen sehr guten Überblick über potenzielle Angriffspfade.

TEAL
ALWAYS CHALLENGING IT

Im folgenden Bild sehen wir z.B., dass Angreifer über Berechtigungen auf eine GPO eine Kompromittierung auf verschiedene hoch privilegierte Konten durchführen könnten.



Dies ist nur ein Beispiel einer BloodHound Abfrage. Man sieht aber auch andere kritische Konfigurationen, wie z.B. auf welchem Computer Anmeldeinformationen von wichtigen Accounts hinterlegt sind und über welchen Pfad z.B. ein Domänen Admin Account kompromittiert werden kann.

Regelmäßige BloodHound Scans liefern wichtige Erkenntnisse, um Fehlkonfigurationen zu beheben und den definierten Zustand zu überwachen. Es empfiehlt sich, ein Standard Query Set zu definieren, das jedes Mal ausgeführt wird. Um Ihnen eine Vorstellung einer Abfragen-Sammlung zu geben, haben wir nachfolgend drei unserer Standardabfragen exemplarisch aufgeführt. Verändern sich die Werte im Vergleich zum Vormonat negativ, muss dringend gehandelt werden Analysieren Sie, wieso sich die Werte verändert haben und prüfen Sie, ob es eine gewollte Änderung ist oder nicht.

73%

der Firmen mit mehr als 1000 Mitarbeitern schätzen das Risiko durch einen Hackerangriff gravierend geschädigt zu werden als „sehr groß" bzw. „eher groß" ein. –

Deloitte Cyber Security Report 2019

TEAL
ALWAYS CHALLENGING IT

1.

Wie viel Prozent der Benutzer haben einen Angriffspfad zu einem Domain Administrator Konto?

```
MATCH (totalUsers:User {domain:‘<DOMAIN>‘}) WITH COUNT(DISTINCT(totalUsers))
as totalUsers MATCH p = shortestPath((pathToDAUsers:User {domain:‘<DOMAIN>‘})-
[r:MemberOf|HasSession|AdminTo|AllExtendedRights|AddMember|ForceChangePasswor-
d|GenericAll|GenericWrite|Owns|WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|AllowedToDelega-
te|ReadLAPSPassword|Contains|GpLink|AddAllowedToAct|AllowedToAct|SQLAdmin|ReadGMSAPass-
word|HasSIDHistory|CanPSRemote*1..]->(g:Group {name:‘DOMAIN ADMINS@<DOMAIN>‘})) WITH
totalUsers, COUNT(DISTINCT(pathToDAUsers)) as pathToDAUsers
```

2.

Wie viel Prozent der Computer haben einen Angriffspfad zu einem Domain Administrator Konto?

```
MATCH (totalComputers:Computer {domain:‘<DOMAIN>‘}) WITH COUNT(DISTINCT(totalComputers))
as totalComputers MATCH p = shortestPath((pathToDAUsers:Computer {domain:‘<DOMAIN>‘})-
[r:MemberOf|HasSession|AdminTo|AllExtendedRights|AddMember|ForceChangePassword|GenericAl-
l|GenericWrite|Owns|WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|AllowedToDelegate|ReadLAP-
SPassword|Contains|GpLink|AddAllowedToAct|AllowedToAct|SQLAdmin|ReadGMSAPassword|HasSID-
History|CanPSRemote*1..]->(g:Group {name:‘DOMAIN ADMINS@<DOMAIN>‘})) WITH totalComputers,
COUNT(DISTINCT(pathToDAUsers)) as pathToDAUsers RETURN 100.0 * pathToDAUsers / totalCom-
puters AS percentComputersToDA
```

3.

Wie viel „Hops“ muss ein Angreifer durchschnittlich überwinden, um ein Domain Administrator Konto anzugreifen?

```
MATCH p = shortestPath((pathToDAUsers:User {domain:‘<DOMAIN>‘})-[r:MemberOf|HasSessio-
n|AdminTo|AllExtendedRights|AddMember|ForceChangePassword|GenericAll|GenericWrite|Owns-
|WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|AllowedToDelegate|ReadLAPSPassword|Contains|G-
pLink|AddAllowedToAct|AllowedToAct|SQLAdmin|ReadGMSAPassword|HasSIDHistory|CanPSRemo-
te*1..]->(g:Group {name:‘DOMAIN ADMINS@<DOMAIN>‘})) RETURN toInteger(AVG(LENGTH(p))) as
avgPathLength
```

Ersetzen Sie <DOMAIN> mit dem Domänennamen Ihrer Domäne in Großbuchstaben

TEAL
ALWAYS CHALLENGING IT

3. Wirksamkeit potenzieller Angriffe eindämmen **durch Passwortänderung** von kritischen Active Directory Konten

Dass Admin-Kennwörter, aber auch Kennwörter von Servicekonten regelmäßig geändert werden müssen, ist mittlerweile Konsens. Wir möchten an dieser Stelle jedoch zwei besonders wichtige Active Directory Accounts hervorheben. Der monatliche TEAL Security Check bietet die optimale Gelegenheit, die Kennwörter des DSRM und KRBTGT Kontos zu ändern.
Über dieses Thema haben wir übrigens auch einen ausführlichen Blogartikel geschrieben.

DSRM

Zunächst sehen wir uns das Active Directory Service Restore Mode (DSRM) Passwort an. Eigentlich ist das Passwort dazu gedacht, im Notfall einen ausgefallenen Domain Controller offline wiederherzustellen. Für Angreifer bietet sich allerdings die Gelegenheit, einen funktionierenden Domain Controller im Restore Mode zu starten und offline die AD Datenbank zu verändern, z.B. um sich einen administrativen Account zu erstellen. Der Vorteil für den Angreifer ist, dass auf diesem Weg keinerlei Logs erzeugt werden. Die Gefahr eines unbemerkten Backdoor Accounts ist damit sehr hoch.

Das DSRM Kennwort sollte regelmäßig für jeden Domain Controller geändert werden. Dies kann einfach mit dem Tool ntdsutil.exe (Set DSRM Password) durchgeführt werden.

KRBTGT

KRBTGT ist ein vordefiniertes Konto, unter dem das Key Distribution Center (KDC) ausgeführt wird und das die Kerberos-Tickets verschlüsselt. Gelangt ein Angreifer in den Besitz des KRBTGT Passwort Hashes, kann ein unbegrenzt gültiges „Golden Ticket" erzeugt werden. Durch das Golden Ticket hat der Angreifer die Möglichkeit, jeden beliebigen Benutzer zu impersonifizieren (dieser muss nicht einmal im Active Directory existieren) und beliebige Gruppenmitgliedschaften zu seinem Ticket hinzuzufügen. Als ob das nicht schon schlimm genug wäre, kann sich ein Angreifer aber auch beliebige SIDs in die SID-History schreiben und somit aus einer beliebigen Subdomain den ganzen Forest kompromittieren!

Alle Tickets sind so lange gültig, bis das KRBTGT Kennwort ZWEIMAL geändert wurde! Das Kennwort des KRBTGT Accounts kann ganz gewöhnlich mit Active Directory Users and Computers geändert werden. Das verwendete Kennwort ist dabei irrelevant.

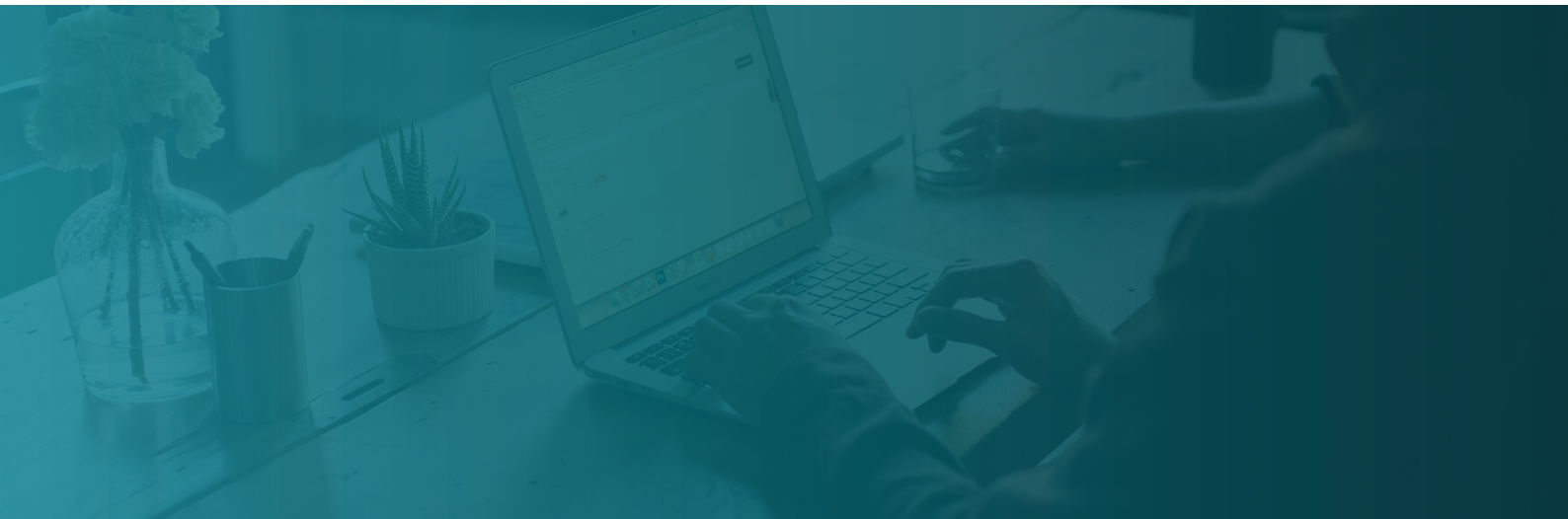
Es wird automatisch ein langes, komplexes Kennwort generiert. Zu beachten ist, dass zwischen den Passwortänderungen standardmäßig 10 Stunden liegen müssen (abhängig von der konfigurierten Ticket Lifetime). Wird das Kennwort vorher geändert, verlieren sämtliche bereits ausgestellte Tickets ihre Gültigkeit. Alternativ bietet Microsoft auch ein passendes Script für die Änderung, welches u.a. sicherstellt, dass das neue Kennwort erfolgreich zu allen Domain Controllern repliziert wurde.

Ransomware Attacke @ Merck

Eine Ransomware Attacke, ausgelöst durch die Malware NotPetya, kostete dem US Pharma Konzern Merck mehr als 600 Millionen US-Dollar. Durch den Angriff waren Produktion, Forschung und Vertrieb nahezu eine Woche stillgelegt.

Das E-Mail-System funktionierte nicht und den Mitarbeitern war es untersagt, ihre Computer zu benutzen. Der Schaden übertraf 2017 andere Ransomware Angriffe, wie z.B. bei FedEx (→300 Millionen US-Dollar) und Maersk (→200 Millionen US-Dollar), bei weitem.

(https://www.silicon.de/41662161/notpetya-attacke-kostet-pharmakonzern-merck-ueber-600-millionen-dollar)



TEAL
ALWAYS CHALLENGING IT

4. Worst Case – Recovery des Active Directories durch eine funktionierende **Backup Strategie**

Ein Active Directory besteht in der Regel aus mehreren Domain Controllern an verschiedenen Standorten. Da die Active Directory Datenbank zwischen den jeweiligen Domain Controllern ständig repliziert wird, ist es normalerweise nicht notwendig, eine Datenbanksicherung vollständig zurückzuspielen. Fällt ein einzelner Domain Controller aus, kann dieser einfach durch einen neuen ersetzt oder von einem Backup wiederhergestellt werden. Anschließend erhält der neue Domain Controller die aktuelle Datenbank repliziert und das Recovery ist abgeschlossen. Einzelne Objekte lassen sich mit dem Active Directory Recycle Bin oder einem Einzelobjekt-Restore wiederherstellen.

Dennoch sollten Unternehmen einen Plan für ein Worst Case Szenario wie einer Datenbankkorruption oder schlimmer einem Ransomware Angriff besitzen. In solchen Fällen kann entweder das Active Directory komplett neu aufgebaut, oder ein hoffentlich aktuelles und sicheres Backup zurückgespielt werden. Genau deswegen ist es aus unserer Sicht erforderlich, monatlich die Backup- und Restore-Konzepte zu valideren.

FOLGENDE GRUNDPRINZIPIEN SOLLTEN DABEI BEACHTET WERDEN:

- Ein vollständiger Restore sollte die letzte Option sein.
- Domain Controller Backups müssen verschlüsselt und an einem sicheren Ort gelagert sein. Ein Zugriff ist nur durch Tier0 / Domain Administratoren erlaubt.
- Eine Sicherung sollte täglich auf mindestens zwei Domain Controllern durchgeführt werden. Die Domain Controller müssen Globaler Catalog sein und der Operations Master sollte mit in der Sicherung enthalten sein.
- Wir empfehlen ein Full Server Backup und nicht nur ein System State Backup. Hintergrund ist schlicht, dass im Fall der Fälle nicht erst ein OS installiert werden muss. Wir glauben, dass es schneller ist, ein Full Backup zurückzuspielen.

Um die Backups zu validieren, empfehlen wir, zum einen ein oder mehrere Testobjekte aus der Gesamtstruktur zu löschen und über einen Einzelobjekt Restore aus dem Backup wiederherzustellen.

Daneben sollte das Full Backup in einer gekapselten Umgebung auf eine Maschine / VM zurückgespielt werden. Hat man in der gekapselten Umgebung einen funktionierenden DC, kann nach einigen simplen Tests, wie z.B. einem Anmeldevorgang von einem Testclient etc. davon ausgegangen werden, dass das Backup valide ist.

TEAL
ALWAYS CHALLENGING IT

5. Erkennen von Angriffen mit den richtigen **Überwachungsmethoden**

Nach unserer Erfahrung gibt es immer noch viele Unternehmen, die kein ausreichendes Auditing bzw. Logging konfiguriert haben. Werden doch Daten gesammelt, fehlt oft die Zeit, gründlich die Log Dateien zu analysieren.

Eine Datensenke in SCOM, SPLUNK oder ähnlichen Werkzeugen ist nur dann sinnvoll, wenn zum einen die richtigen Daten dort abgelegt werden und zum anderen die Daten richtig ausgewertet bzw. korreliert werden.

82% der Unternehmen gehen davon aus, dass die Zahl der Cyberattacken auf ihr Unternehmen in den nächsten zwei Jahren zunehmen wird. –

Wirtschaftsschutz in der vernetzten Welt Studienbericht 2020 BITKOM

Genau hier möchten wir ansetzen und ein Bewusstsein dafür schaffen, welche Dinge überwacht werden sollten, was auf einen Angriff hindeutet und wie man mit dem Thema Active Directory Monitoring starten kann. Ist der Start gelungen, kann kontinuierlich an der Verbesserung der Überwachung bis hin zu speziellen SIEM Use Cases gearbeitet werden.

UM KONKRET ZU WERDEN: WAS WÜRDEN WIR AUF JEDEN FALL ÜBERWACHEN?

- Wurden Sicherheitslogs geleert? Wenn ja, wieso? Wenn Events an zentrale Systeme weitergeleitet werden, kann geprüft werden, was zuvor geschehen ist.
- Ist in der letzten Zeit der Built-in Admin Account (RID:500) verwendet worden? Ist dies der Fall, sollte ein entsprechendes Ticket dazu vorhanden sein. Grundsätzlich sollte der Administrator Account aber nicht verwendet und das Passwort z.B. in einem Tresor aufbewahrt werden. Zugriffe auf das Kennwort müssen protokolliert und ggf. nur mithilfe eines vier-Augen-Prinzips erlaubt sein.
- Hoch privilegierte Gruppen wie z.B. Domain Admins, Schema Admins usw. sollten ebenfalls überwacht werden. Änderungen an diesen Gruppen sollten ebenfalls in einem Change dokumentiert und begründet sein.
- Wurde neue Software auf den Domain Controllern installiert? Grundsätzlich sollte auf einen DC so wenig wie möglich installiert sein. In jedem Fall darf aber niemand ungewünscht Software auf einem Domain Controller installieren.
- Sind die Domain Controller auf einem aktuellen Patchstand? Wenn die Domain Controller auf Physik installiert sind, sollte zwingend auch die Hardware einen aktuellen Patchstand vorweisen.
- Wurden GPOs, die auf Domain Controller wirken, verändert und wenn ja, welche Einstellung?

Use Cases: TEAL ist erfahrener Dienstleister in Sachen Infrastruktursicherheit

Die aufgezeigten Schritte des TEAL Security Checks basieren auf unseren langjährigen Erfahrungen, in denen wir bereits mehrere große Kunden bei der Einführung einer sicheren Administrationsumgebung mit organisatorischen und technischen Maßnahmen unterstützen konnten. So haben wir z.B. bei einem internationalen Nutzfahrzeughersteller oder einem großen Versicherungskonzern unsere Dienstleistungen erbracht:

VERSICHERUNGSKONZERN:

Ausgangssituation

Im Rahmen eines großen Strategieprogramms richtete der international tätige Versicherungskonzern mit 40.000 Mitarbeitenden sein IT-Portfolio neu aus. Ziel war es, die Zusammenarbeit zwischen den einzelnen Konzerngesellschaften zu verbessern und verstärkt globale Services zu nutzen. Diese Services sollten an zentraler Stelle neu entstehen und möglichst sicher betrieben werden. Im ersten Schritt sollte eine globale Authentifizierungsplattform sowohl für Kerberos- als auch Token-based Services entstehen.

Lösungsweg

TEAL unterstützte den Kunden bei der Definition der Architektur und der Implementierung dieser globalen Authentifizierungsplattform in zwei neuen Co-located Datacentern. Die Authentifizierungsplattform besteht aus einer Active Directory Architektur auf Basis von Microsofts Enhanced Security Administrative Environment (ESAE, mehr dazu in unserem Blog) für Kerberos-basierte Dienste und einer ADFS Plattform für Token-basierte Applikationen. Administrative Rechte werden durch eine Privileged Access Management (PAM) Lösung nur temporär gewährt, um das Angriffsrisiko von gestohlenen Passwörtern (und deren Auswirkungen) zu minimieren. Durch den Einsatz von nahezu ausschließlich Windows Server 2016 Core wurde die Angriffsfläche weiter reduziert. Zukünftig kann die Überwachung der Verwendung von hohen Privilegien durch die vollständige Integration in ein SIEM System und die Kopplung der Rechtevergabe an Change und Incident Tools weiter verbessert werden.

Ergebnis

Durch die neue Authentifizierungsplattform nach ESAE Vorbild, ist die Grundlage für die globalen Shared Services gelegt. Diese Systeme können nun in einer sicheren Umgebung betrieben und dem Endkunden zur Verfügung gestellt werden.

NUTZFAHRZEUGHERSTELLER:

Ausgangssituation

Ein führender internationaler Nutzfahrzeughersteller mit über 30.000 Mitarbeitenden stand vor der Herausforderung, ein umfassendes Strategieprogramm zur Neuausrichtung der IT-Infrastruktur und Erhöhung der IT-Sicherheit umzusetzen. Ein wesentlicher Beitrag zur Erhöhung der Sicherheit ist hier die Absicherung des Active Directories. Dafür gibt es im Konzern eine Blaupause auf Basis des Microsoft ESAE Ansatzes. Ziel des Projektes war es, die Blaupause auf die lokalen Gegebenheiten zu adaptieren und umzusetzen.

Lösungsweg

TEAL unterstützte den Nutzfahrzeughersteller bei der Analyse der Konzernblaupause, bei der Konzeption der Zielarchitektur und der Implementierung der Secure Administration Umgebung (SAE). Die Lösung besteht aus drei Active Directory Forests für Produktion („Gold Forest“), Administration („Red Forest“) und dem Hypervisor („Iron Forest“) mit entsprechendem Admin Tiering. Jedes Tier wird durch zahlreiche Maßnahmen wie zum Beispiel 2-Faktoren-Authentifizierung, Privilege Administration Workstations (PAWs), Security Baseline GPOs und sicheren Betriebsprozessen abgesichert. Dadurch wird ein außerordentlich hohes Schutzniveau gegen Pass-the-Hash und Pass-the-Ticket-Attacken erreicht.

Ergebnis

Durch das Projekt konnte das Sicherheitsniveau der besonders schützenswerten IT-Assets erheblich gesteigert werden und somit wurde die Grundlage für weitere Maßnahmen zur Erhöhung der IT-Sicherheit gelegt. Zusammen mit TEAL konnte der Nutzfahrzeughersteller nicht nur die Konzernblaupause umsetzen, sondern darüber hinaus noch verbessern. So ist die SAE-Architektur ein maßgeblicher Treiber im Gesamtkonzern für die IT-Sicherheit geworden.

TEAL
ALWAYS CHALLENGING IT

Der TEAL Security Check ist Teil eines dreitägigen Security Assessments in dem Ihnen aufgezeigt wird, wie:

- ✓ Angreifer in Ihr Unternehmensnetzwerk gelangen und wie Sie sich dagegen schützen können,
- ✓ der Zustand Ihrer Umgebung ist, indem wir diese im Detail analysieren,
- ✓ Sie sich effektiv durch den Einsatz von technischen und organisatorischen Maßnahmen schützen können und die potenziellen Auswirkungen eines Angriffs abmildern können.

Kontaktieren Sie uns, um mehr über den TEAL Security Check oder unser Assessment zu erfahren.

FABIAN BÖHM
0211/93675225
info@teal-consulting.de