OFFENSIVE SERVICES

AWARE7

Active Directory

Whitepaper August 2022

Moritz Gruber

Mario Klawuhn

Prof. Dr. Matteo Grosse-Kampmann

Inhaltsangabe

Einleitung

Bei Ihrer täglichen Arbeit erhalten Pentester Einblicke in die internen Netzwerke von Unternehmen. Dabei können diese viele Einblicke in die tägliche Arbeit von Administratoren erhalten. Dennoch haben Pentester eine gesonderte Position, weil diese aus einer anderen Sicht auf das Netzwerk blicken. Wenn ein Pentester einen Netzplan sieht, sucht dieser Schwachstellen, Single Point of Failures oder allgemein nach Möglichkeiten, den Betrieb zu stören.

Ein internes Netzwerk besteht aus vielen Komponenten die bei einem Pentest untersucht werden. So werden nicht nur das Netzwerk als solches, sondern auch Server und Active Directory getestet. Gerade dieses stellt das Herzstück eines Unternehmens dar. Hier werden alle Accounts der Mitarbeiter verwaltet, alle Zugriffsrechte auf Datei-Freigaben und E-Mails laufen über diese wenigen Kernkomponenten. Daher ist es essentiell, diese Systeme korrekt abzusichern und zu warten.
Dies war in den seltensten Fällen vollumfänglich durchgeführt worden. Daher stellt dieses Werk eine Sammlung von Maßnahmen dar, damit Sie einem Angreifer das Leben möglichst schwer machen.

INSIDER-THREAT - DIE BEDROHUNG VON INTERN

Bedrohungen für die Sicherheit eines Unternehmens können von den unterschiedlichsten Akteuren ausgehen. Über die letzten Jahrzehnte hat sich die Ansicht verbreitet, dass alle Hacker-Angriffe von außen über das Internet stattfinden. Dennoch gibt es viele Angreifer-Modelle, welche nicht dem klassischen externen Angreifer entsprechen.

So gibt es neben dem externen Angreifer auch Szenarien, in welchem von einem Supply-Chain Angriff ausgegangen wird. Darunter versteht sich ein Angreifer, dem es gelingt, Systeme eines Unternehmens durch kompromittierte Komponenten zu übernehmen. Den meisten Angreifern, die in das interne Netzwerk eines Unternehmens eindringen, gelingt dies über kleine Unachtsamkeiten. Dies können Phishingmails, ungesicherte öffentliche Netzwerkdosen, veraltete Server oder auch unsichere VPN-Zugangsdaten sein.

Ein Angreifer, welcher in das interne Netzwerk vordringen konnte, verhält sich zu Beginn meist passiv und sammelt weitere Informationen, um sich sukzessiv im Netzwerk auszubreiten. Dabei werden viele Techniken wie Lateral Movement oder Privilege Escalation angewendet, um am Ende Zugriff auf einen Account mit administrativen Berechtigungen zu erlangen. Als Lateral Movement wird eine Technik bezeichnet bei der sich Angreifer nach dem initialen Einbruch im internen Netzwerk von System zu System bewegen. Unter dem Begriff Privilege Escalation werden viele Angriffe zusammengefasst, die es einem Angreifer erlauben, seine Zugriffsrechte, meist auf einem einzelnen System, zu erhöhen.

Die Ziele und auch die Motivation eines solchen Angriffs können dabei sehr vielfältig sein. So kann es einem Mitarbeitenden, der mit seiner Arbeit nicht mehr zufrieden ist oder gekündigt wurde vor allem darum gehen möglichst viele Betriebsprozesse nachhaltig zu stören. Aber auch Wirtschaftsspionage ist eine häufige Motivation eines solchen Insider-Threats. Dabei kann es um Entwürfe neuer Produkte oder um Zugriff auf Daten von Kunden gehen. Diese Angriffe laufen dabei relativ ähnlich ab. Zur Modellierung solcher InsiderThreats wurde von Lockheed Martin das Cyber Kill Chain Modell entwickelt. Dieses unterteilt jeden Angriff in sieben Phasen.

- Reconnaissance - Informationssammlung
- Weaponization - Entwicklung eines lauffähigen Exploits
- Delivery - Verbreitung des Exploits, beispielsweise per Mail
- Exploitation - Ausnutzen der Exploits und Übernahme des Opfer-Systems
- Installation - Installation weiterer Schadsoftware
- Command and Control - Rückmeldung der Schadsoftware beim Angreifer
- Actions on Objectives - Exfiltration oder Verschlüsselung von Daten

SIMULATION VON INSIDER-THREATS DURCH ACTIVE DIRECTORY PENTESTS

Interne Angreifer agieren im Netzwerk mit allen dort betriebenen Systemen. Daher ist es von essenzieller Bedeutung zu evaluieren, was ein Angreifer im Zusammenspiel mit der Netzwerkinfrastruktur, den Servern, den Clients sowie des Active Directories erreichen kann. Ein interner Angriff, der auf einem Windows Client durch eine infizierte E-Mail startet, wird sich nicht auf andere Clients beschränken, sondern kann Sicherheitslücken und Fehlkonfigurationen im ganzen Netzwerk ausnutzen. Darum sollten die Elemente eines internen Netzwerks auch nie separiert betrachtet werden.

Um einen Eindruck davon zu erlangen, wie sich ein Insider-Threat im internen Netzwerk bewegt und was für Systeme dieser angreift, sollte dieser simuliert werden. Gerade für die Simulation von Angriffen empfiehlt es sich, Pentests durchzuführen. Bei einem Pentest handelt es sich um eine Sicherheitsanalyse, bei der Angriffe und das Verhalten von Bedrohungen nachgeahmt werden. Dadurch kann evaluiert werden, was für Schwachstellen und Fehlkonfigurationen auf den Systemen im Netzwerk vorhanden sind. Ein automatisierter Schwachstellenscan wird meist als kosteneffiziente Alternative angeboten. Gerade aber wenn es um das Zusammenspiel unterschiedlicher Netzwerkkomponenten, Server und Active Directory geht empfiehlt sich die Durchführung eines manuellen Penetrationstests durch ausgebildete Tester.

Ein Test eines internen Netzwerks besteht dabei meist aus zwei separierten Phasen. In der ersten Phase wird ein interner Angreifer modelliert, der keine Zugangsdaten zu Systemen und Diensten des internen Netzwerks hat. Dabei soll evaluiert werden, was für Möglichkeiten ein nicht autorisierter Angreifer besitzt. In einer weiteren Phase werden die Pentester dann mit gültigen Zugangsdaten oder einem Standardgerät eines normalen Benutzers ausgestattet. Dieses Szenario simuliert nun einen Insider-Threat, der beispielsweise über eine Phishingmail, einen Benutzer-Account übernommen hat.

Gerade ein solch zweistufiger Pentest ermöglicht es einem Unternehmen, viel über den Aufbau des internen Netzes zu lernen. So dokumentiert solch ein Pentest nicht nur alle identifizierten Schwachstellen, sondern ermöglicht es der IT ebenfalls festzustellen, ob diese in der Lage gewesen wären, diese Angriffe frühzeitig zu erkennen und auch zu verhindern. Des Weiteren kann anhand eines solchen Tests und dessen Aufarbeitung evaluiert werden, ob der Verlauf des Angriffs mit den gesammelten Logdaten rekonstruiert werden kann.

BEISPIEL-UMGEBUNG

Um die Tipps die hier vorgestellt werden an einem Modell demonstrieren zu können, wurde die fiktive Firma ”Franken Logistik”, mit dem einschlägigen Slogan ”Ihr Weg ist unser Ziel” ins Leben gerufen. Im Rahmen dieser Veröffentlichung wurde ein internes Netzwerk aufgebaut, dass die Infrastruktur der Franken Logistik abbildet. Der Aufbau des internen Netzwerks ist an echte Netzwerke angelehnt, welche bei internen Pentests vorgefunden wurden. Folgende Grafik zeigt den Netzplan der Franken Logistik:

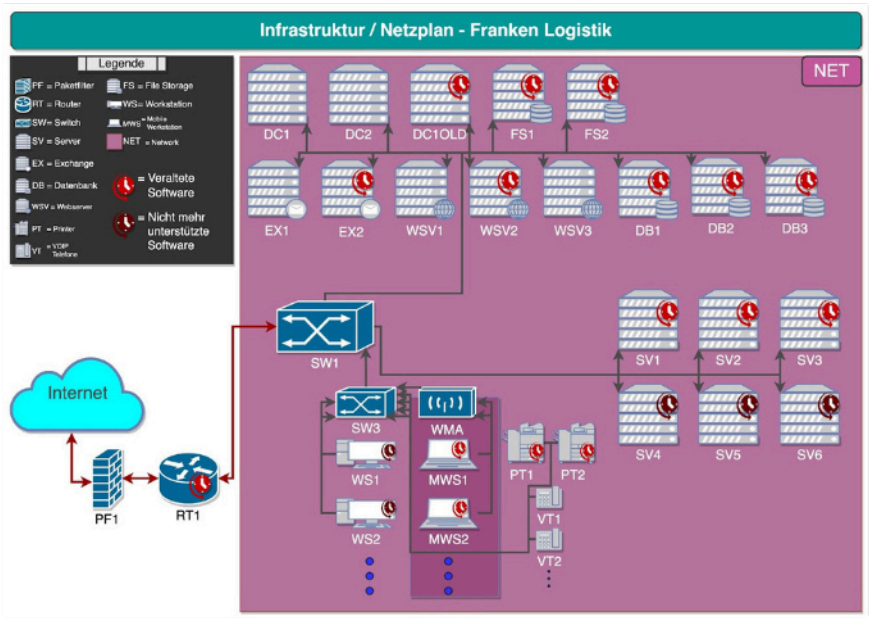

Abbildung 1: Infrastruktur -/ Netzplan der Franken Logistik

Das Netzwerk der Franken Logistik setzt keine Netzwerkseparierung ein. Alle Geräte (Server, Clients, etc) befinden sich in einem Netzwerk. Zwischen dem Internet und dem Router (RT1) befindet sich ein Paketfilter (PF1) als Firewall. Vom Router geht der Traffic zu einem Core-Switch (SW1) von dem aus die Anfragen an die entsprechenden Systeme weiter geroutet werden.

Im Netzwerk befinden sich zwei produktive Domain Controller (DC1, DC2) und ein veralteter nicht produktiv genutzter (DC1OLD). Neben den Domain Controllern stehen im Netzwerk noch zwei File Storage Server (FS1, FS2) und zwei Exchange Server (EX1, EX2) zur Verfügung. Für die Webseiten der Franken Logistik und deren externen Webdiensten, werden im Netz drei Webserver (WSV1, WSV2, WSV3) mit entsprechenden Datenbanken (DB1, DB2, DB3) betrieben. Diese kommunizieren mit Clients von außerhalb über das Internet.

Für interne Anwendungen und Dienste laufen drei Windows Server (SV1, SV2, SV3) im Netzwerk. Zusätzlich laufen noch drei stark veraltete Windows Server (SV4, SV5, SV6) als Altlasten im gleichen Netz. Die Mitarbeiter können ihre Arbeitsrechner direkt per LAN oder WLAN in das Netzwerk einbinden (WS, MWS). Für jeden Mitarbeiter steht noch ein VOIP Telefon (VT) zur Verfügung. Im Büro stehen zwei Officeprinter (PT1, PT2), welche ebenfalls in das Netzwerk eingebunden sind.

Im Netzwerk befinden sich mehrere Komponenten mit veralteter Software, was in der Grafik durch die hellroten Uhren dargestellt wird. Neben der veralteten Software werden zusätzlich noch Komponenten mit nicht mehr unterstützter Software eingesetzt (dunkelrot markiert). Für die nicht mehr unterstützten Softwares werden keine (Sicherheits-)Updates von den Herstellern zur Verfügung gestellt. Im Laufe dieser Veröffentlichung werden sieben Tipps vorgestellt, wie das eben dargestellte Netzwerk besser vor Hacker-Angriffen abgesichert und gehärtet werden kann.

Platz 1 - Trennung von Netzen

MITRE ATT&CK Vector: T1210.000 - Exploitation of Remote Services

Ein weitverbreitetes Problem, das bei den meisten der intern durchgeführten Pentests identifiziert wird, ist eine fehlende oder unzureichende Trennung der Netzbereiche. Meist ist dies ein Problem, das bei Unternehmen mit einer lange bestehenden IT-Landschaft auftritt. So befinden sich beispielsweise alle Systeme in einem Netzbereich. Die Landschaft ist dementsprechend heterogen, beispielsweise Windows-Clients neben Linux Servern neben Management-Interfaces eines Switches oder Lagerverwaltungssystemen.

Besonders die Trennung der Gäste WLAN-Netze von den produktiven Netzen stellt eine sehr große Bedrohung für den sicheren Betrieb dar. Angreifern gelingt es häufig, über das unverschlüsselte Gäste-WLAN in das interne Office-Netzwerk zu gelangen. Dies ermöglicht es einem externen Angreifer zu einem Insider-Threat zu werden ohne das großer Aufwand betrieben werden muss.

Gerade bei Systemen, die besonders vulnerabel sind, empfiehlt es sich, diese durch Netztrennungen zu separieren. So finden sich in Produktionsnetzen viele Maschinen, auf denen Windows XP installiert ist. Bei diesen ist häufig, aufgrund des speziellen Aufgabenbereichs, kein Update möglich und so bleiben diese im Netzwerk. Sie stellen ein lukratives Ziel für Angreifer dar. Gerade hier lohnt sich eine Trennung der Netze. So kann sichergestellt werden, dass diese Maschinen weiterhin sicher betrieben werden können, ohne die Gefahr von internen Angreifern fürchten zu müssen.

EINFLUSS AUF DIE INFORMATIONSSICHERHEIT

Eine Separierung der Systeme in einzelne Netzbereiche hilft dabei, Sicherheitsvorfälle und Angriffe lokal zu begrenzen. Dadurch kann die Ausbreitung eines Virus oder eines lokalen Angreifers ausgebremst oder sogar verhindert werden.

Als besonders hilfreich hat es sich erwiesen, die Backupserver vom Rest des Netzes zu trennen, um so Ransomware die Möglichkeit zu nehmen, diese Server ebenfalls zu verschlüsseln. Diese Separierung der Netze erlaubt es einem Administrator bei einem Sicherheitsvorfall schnell die Ausbreitung von Angriffen beschränken zu können, indem Netzbereiche vollständig getrennt werden. Der BSI-Grundschutz Katalog fordert ebenfalls den Einsatz von separierten Netzen.

Dies ist beispielsweise in NET.1.1.A4 definiert und verlangt mindestens die Aufteilung in die drei folgenden Netzbereiche:

- Internes Netzwerk
- Demilitarisierte Zone (kurz DMZ)
- Außenanbindungen, bspw. Internetanbindung

Bei all diesen Netzen ist eine Trennung mittels einer Firewall durch das BSI gefordert. In den Maßnahmen NET.1.1.A5 und NET.1.1.A6 fordert das BSI weitere getrennte Netze. NET.1.1.A5 fordert beispielsweise, die Clients und Server im internen Netzwerk zu separieren. Genauso sollen nach dem BSI IT-Grundschutz Systeme mit ähnlichem Sicherheitsniveau gruppiert werden. Woraus sich beispielsweise eigene Netze für VOIP-Telefone oder Switche und Router ergeben.

PLANUNG UND IMPLEMENTIERUNG

In diesem Kapitel wird beschrieben, wie die im Kapitel Beispiel-Umgebung dokumentierte Netzwerkumgebung separiert werden kann. In diesem Beitrag erfolgt keine Empfehlung von speziellen Netzwerkprodukten wie Firewalls oder Switches, mit denen sich die Umsetzung durchführen ließe. Daher wird dieses Kapitel auf die Planung der zu erstellenden VLANs eingehen und nicht auf die Konfiguration einer dedizierten Firewall. Wie in Tabelle 1 zu sehen ist, werden viele unterschiedliche Netzwerkkomponenten genutzt. In einem ersten Schritt sollten diese aufgelistet und kategorisiert werden. Mit diesen Kategorien können dann, wie in Tabelle 1 zu sehen ist, Netzbereiche definiert werden. Damit die gesamte Verkabelung nicht neu verlegt werden muss, sollten VLANs statt physikalischer Trennung genutzt werden.

Auch bei dem Beispiel-Unternehmen der Franken-Logistik wird auf VLANs gesetzt, weswegen in der Tabelle 1 die jeweilige VLAN-ID gelistet ist. Ein weiter wichtiger Schritt bei der Planung eines separierten Netzes ist die Definition der Netzwerkübergänge. Dabei muss definiert werden, welche VLANs auf andere VLANs zugreifen kann. Eine mögliche Darstellung dieser Netzwerkübergänge ist in Tabelle 2 zu sehen. Dort werden Netzwerkübergänge, welche von der Firewall erlaubt werden, mit einer 1 und geblockte mit einer 0 markiert. So müssen Windows Clients aus dem Office Netz keinen Zugriff auf die interne Netzwerkinfrastruktur oder das Backup Netz erhalten. Dafür können diese auf das Drucker und Server VLAN zugreifen, da dieses für Ihre normale Arbeit notwendig sind.

Name	IP-Range	IDs	Funktion
DMZ	192.168.20.0/24	2	Bereitstellung von Diensten für das Internet.
Office	192.168.21.0/24	3	Betrieb der Windows Clients.
Server	192.168.22.0/24	4	Betrieb der Server für das Active Directory.
VOIP	192.168.23.0/24	5	Betrieb aller VOIP-Telefone.
Drucker	192.168.24.0/24	6	Betrieb aller Netzwerk-Drucker.
Backup	192.168.30.0/24	7	Separierung der Backup-Systeme.
Netzwerk	192.168.31.0/24	8	Netzwerk für die Management-Interfaces der Netzwerk-Infrastruktur.

Tabelle 1: Tabellarische Auflistung aller Netzbereiche für die Franken Logistik

VLAN -IDs	2	3	4	5	6	7	8
2	-	0	0	0	0	0	0
3	0	-	1	0	1	0	0
4	0	0	-	0	0	0	0
5	0	0	0	-	0	0	0
6	0	0	0	0	-	0	0
7	0	1	1	0	0	-	0
8	1	1	1	1	1	1	-

Tabelle 2: Übergänge zwischen den einzelnen VLANs. Ein “-” bedeutet es handelt sich um dasselbe VLAN. Eine “1” bedeutet das Linke VLAN auf der y-Achse darf auf das VLAN der x-Achse zugreifen. Mit einer “0” wird ein geblockter Netzwerkübergang gekennzeichnet.

Bei einem Entwurf wie diesem werden zwei einfache Prinzipien verwendet. Einmal das Need-to-know-Prinzip, nach welchem die Rechte vergeben werden, auf andere VLANs zuzugreifen. Es werden damit nur die Berechtigungen vergeben, welche für die Arbeit dieser Systeme notwendig sind und keine weiteren. Das zweite Prinzip ist in diesem Fall Security-by-Design. Bevor die Implementierung des Netzwerks durchgeführt wird, wird definiert, was für Zugriffsrechte und Absicherungen in den einzelnen VLANs vorhanden sein sollen. Damit befolgt dieser Entwurf zwei wichtige Prinzipien beim Entwurf von sicheren Systemen und Netzen.

Platz 2 - Software Restriction Policies

MITRE ATT&CK Vector: T1204.002 - User Execution: Malicious File

Unter dem Begriff Software Restriction Policies (kurz SRP) bezeichnet Microsoft eine Methode, welche definiert was für Software auf einem System ausgeführt werden darf. Dies dient bei Windows Clients im Active Directory dazu, den Aktionsradius von Mitarbeitenden und ebenso Angreifern einzuschränken. Dabei sollte die SRP so eingerichtet werden, dass nur noch vertrauenswürdige Software gestartet werden können. Dadurch kann teilweise auch verhindert werden, dass über E-Mail versendete Viren oder Trojaner gestartet werden können.

Die SRPs werden so konfiguriert, dass alle Programme verboten werden. In einem weiteren Schritt werden dann einzelne vertrauenswürdige Programme wieder freigegeben. Die gesamte Konfiguration kann für alle Clients des Active Directories über Gruppenrichtlinien ausgerollt werden.

Microsoft setzt bei Windows 11 mittlerweile auf die “Applocker” Funktion. Diese bietet eine neuere Variante der SRP an. Dennoch funktioniert auch die SRP noch zuverlässig auf allen aktuellen Windowsversionen.

EINFLUSS AUF DIE INFORMATIONSSICHERHEIT

Durch die Software Restriction Policy werden nicht nur .exe-Dateien blockiert, sondern sämtliche Daten, die Programme ausführen wie CMD/BAT oder auch Powershell-Skripte(PS1). Einzig Programme oder auch Pfade die durch den Administrator festgelegt werden, können ausgeführt werden.

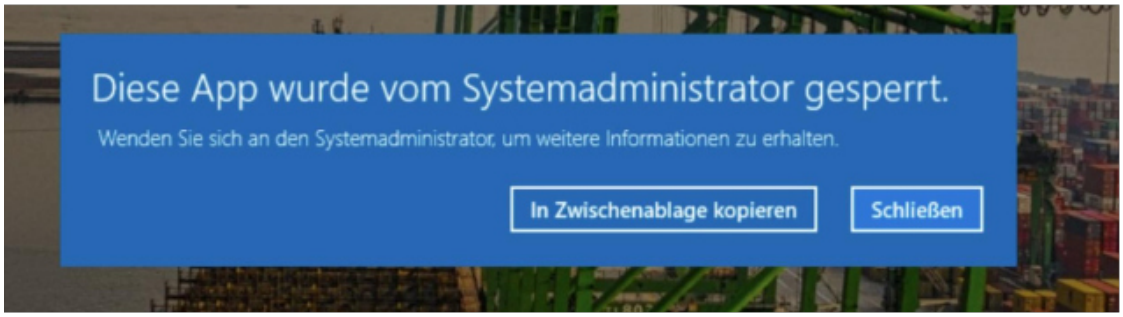

Abbildung 2: Ausführung einer durch Software Restriction Policy geblockten Anwendung

Durch SRP werden nicht nur .exe-Dateien blockiert, sondern sämtliche Daten, die Programme ausführen wie CMD/BAT oder auch Powershell-Skripte(PS1). Einzig Programme oder auch Pfade die durch den Administrator festgelegt werden, können ausgeführt werden. Wenn aus Outlook ein bösartiger Anhang heraus direkt geöffnet wird, wird dieser in einem temporären Ordner gespeichert und dort geöffnet.

Dies wird durch die SRP geblockt. Richtig konfiguriert dürfen nur noch Programme aus “C:\Programme\” gestartet werden und in diesen Ordner dürfen nur Administratoren schreiben und installieren. Durch eine gut konfigurierte SRP können somit viele Angriffe, die im internen Netzwerk von Insider-Threats durchgeführt werden, blockiert werden.

Die BSI IT-Grundschutz Maßnahmen SYS.1.2.2 und SYS.2.2.2 verlangen ebenfalls den Einsatz der Software Restriction Policy. Bei Ihnen handelt es sich um Maßnahmen die definieren wie Windows Server und Windows Clients abgesichert werden sollen.

PLANUNG UND IMPLEMENTIERUNG

Die Konfiguration der SRPs findet auf dem Active-Directory Server statt. Auf diesem System werden alle Gruppenrichtlinien verwaltet. Daher wird dort das Programm "Gruppenrichtlinienverwaltung"verwendet, um die Gruppenrichtlinie für die ausgewählte Domain anzulegen und diese an alle Benutzer und Systeme zu verteilen.

Mittels des “Gruppenrichtlinienverwaltungs-Editors” kann die SRP konfiguriert werden. Dazu muss im Punkt “Benutzerkonfiguration” auf “Windows-Einstellungen” ‘Sicherheitseinstellungen” und dort auf ‘Richtlinien für Softwareeinschränkung” geklickt werden. Bei der Implementierung von SRPs empfiehlt es sich, auf eine Allowlist Filterung zu setzen. Dies bedeutet das jede Software, welche nicht explizit erlaubt ist, auf den Servern und Clients im Active Directory verboten ist. Diese Einstellung findet sich im Ordner “Sicherheitsstufen” und hier sollte die Option “Nicht erlaubt” als Standard gewählt werden, wie in Abbildung 4 gezeigt. Dies kann mit einem Doppelklick auf die jeweilige Option und einem Klick auf “Als Standard” aktiviert werden.

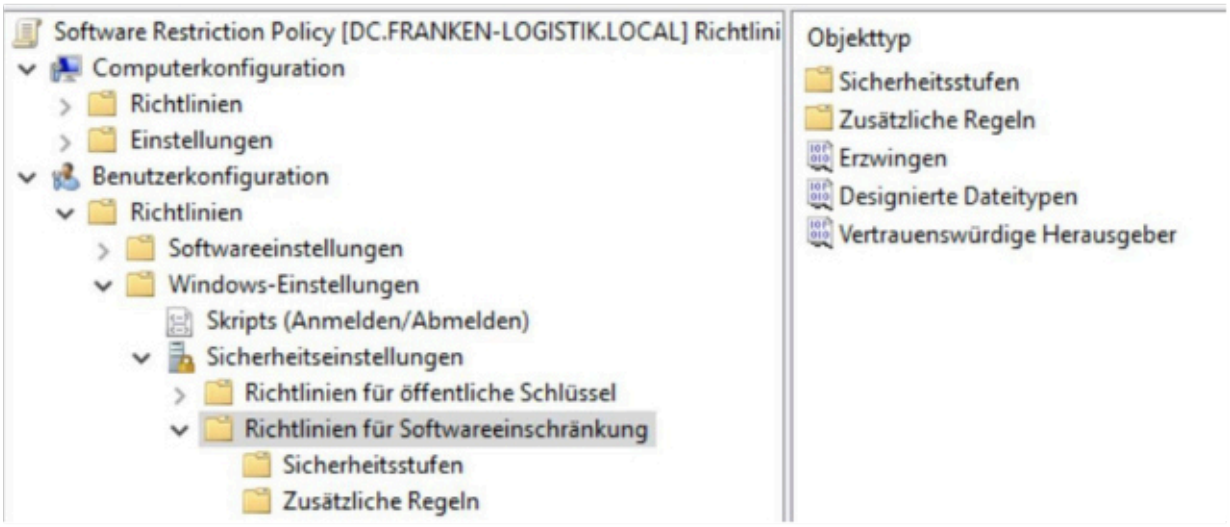

Abbildung 3: Konfiguration der Software Restriction Policy als Gruppenrichtlinie

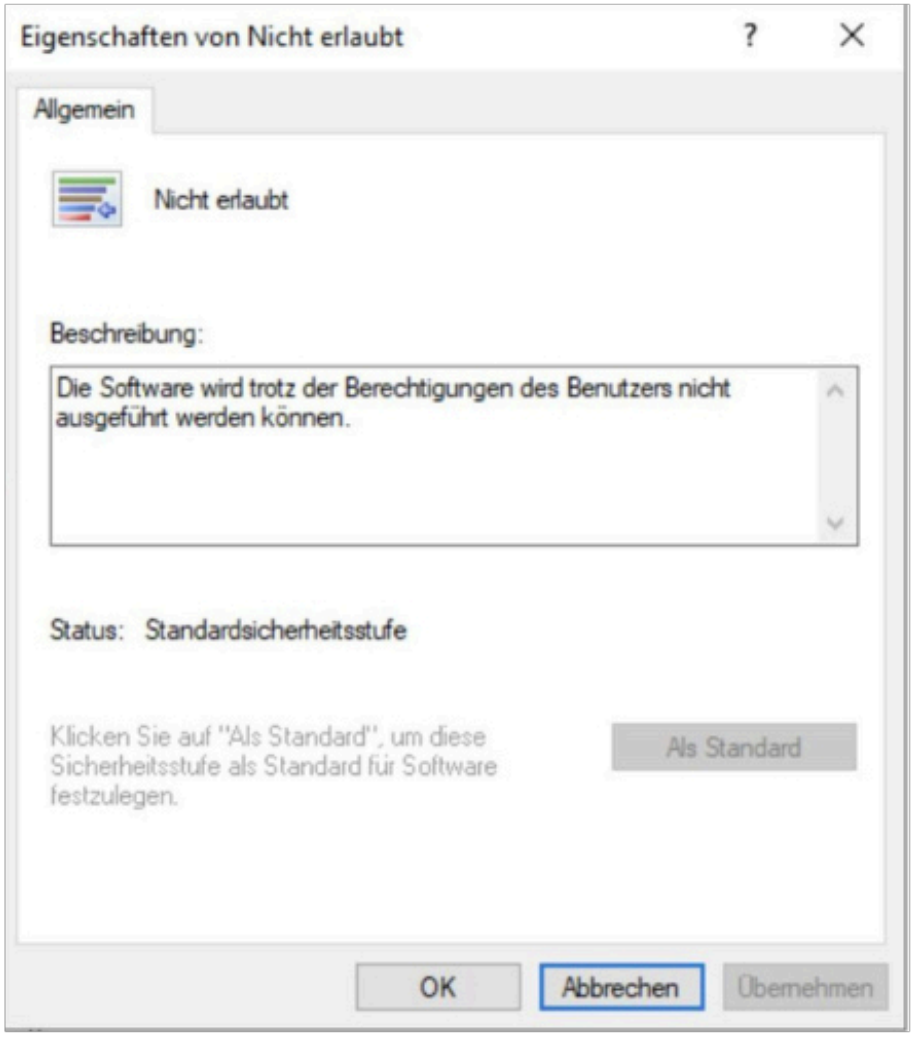

Abbildung 4: Whitebox Filterung als Default der Software Restriction Policy

Damit alle von den Administratoren installierten und verwalteten Anwendungen genutzt werden können, müssen diese explizit freigegeben werden. Dafür bietet es sich an, dass alle Anwendungen, welche durch das Unternehmen freigegeben wurden, nur in den folgenden Ordnern installiert werden.

- C:\Programme\
- C:\Program Files (x86)\

Ein besonderer Vorteil dieser beiden Ordner ist, dass dort nur Benutzer mit administrativer Berechtigung Daten verändern, schreiben oder installieren können. Wenn es nur möglich ist, aus diesen beiden Ordnern heraus Software zu starten, können viele Angriffe gestoppt werden. Viele Viren und Angreifer laden ausführbare Dateien (Schadcode) nach. Die Ausführung dieses Codes kann so verhindert werden.

Um diese Ausnahmen hinzuzufügen, sollte der Punkt “Zusätzliche Regeln” ausgewählt werden. Dort kann über einen Rechtsklick die Option “Neue Pfadregel” ausgewählt werden. Hier sollte einer der oben gelisteten Pfade eingetragen werden und für das Feld “Sicherheitsstufe” die Option “Nicht eingeschränkt” genutzt werden. Für jeden Ordnerpfad, welcher erlaubt werden soll, muss eine solche Regel angelegt werden.

Platz 3 - Deaktivieren von veralteten Protokollen

MITRE ATT&CK Vector: T1204.002 - User Execution: Malicious File

Microsoft legt großen Wert auf die Kompatibilität von Windows. Daher ist es bis heute möglich, veraltete Windows Version, wie Windows 2000 oder Windows XP, in aktuellen Active Directories zu integrieren. Gerade für diesen Zweck unterstützt Microsoft per Default viele alte und häufig unsichere Netzwerk Protokolle.

So finden sich beispielsweise in den aktuellsten Windows Versionen noch Funktionen wie die Authentifizierung über das unsichere NTLM v1 Verfahren oder die Option zum Cachen von administrativen Zugangsdaten.

Diese und viele weitere Funktionen werden von Windows genutzt, um noch kompatibel zu veralteten und nicht unterstützten Versionen zu sein. Viele dieser Funktionen und Protokolle können heutzutage für Angriffe auf das Active Directory genutzt werden. Im Besonderen werden diese für Privilege Escalation Angriffe, also das Erlangen von höheren Berechtigungen, genutzt. In modernen Windows Umgebungen können die meisten dieser unsicheren Funktionen und Netzwerk Protokolle abgeschaltet werden, ohne das es zu Störungen des Betriebs kommt. Diese Abschaltung erfolgt in einem Active Directory über Gruppenrichtlinien, welche an alle Systeme verteilt werden.

EINFLUSS AUF DIE INFORMATIONSSICHERHEIT

Ein wichtiger Punkt bei der Härtung von Windows Systemen mittels Gruppenrichtlinien ist es zu evaluieren, welche Maßnahmen einen wirklichen Effekt auf die Sicherheit haben. In vielen durchgeführten Pentest konnten wir Schwachstellen durch veraltete Protokolle auf Windows Systemen ausnutzen. Dies sind auch potenzielle Einfallstore für interne Angreifer. Daher empfehlen wir, diese einfach zu beseitigenden Schwachstellen zu schließen und die Unterstützung für alte Protokolle zu deaktivieren.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt einen Guide für solche Härtungsmaßnahmen heraus. Dieses Projekt nennt sich “SiSyPHuS” und bietet eine umfangreiche Sammlung von 375 unterschiedlichen Härtungsmaßnahmen an.

PLANUNG UND IMPLEMENTIERUNG

Vor der Implementierung dieser Maßnahmen sollte jeweils evaluiert werden, ob die hier deaktivierten Funktionen im internen Netzwerk produktiv verwendet werden. In den meisten modernen Windows Umgebungen sollte dies aber nicht mehr der Fall sein.

Die Konfiguration für diese Funktionen erfolgt über die Gruppenrichtlinien. Im Folgenden wird nur dokumentiert, wie die jeweiligen Optionen innerhalb einer Gruppenrichtlinie konfiguriert werden. Die Erstellung einer Gruppenrichtlinie wird dabei nicht explizit noch einmal erwähnt (siehe Planung und Implementierung).

DEAKTIVIEREN VON SERVER MESSAGE BLOCK V1 (SMBV1)

Das Server Message Block Protokoll (kurz SMB) dient dazu, Daten zwischen Client und Server auszutauschen. Im Besonderen wird es zur Übertragung von Dateien und Netzwerkfreigaben verwendet. Mittlerweile wird die dritte Iteration von SMB (SMBv3) aktiv von Windows genutzt. Dennoch unterstützen noch alle Versionen die veraltete und unsichere Version 1 des Protokolls.

Zur Deaktivierung von SMBv1 muss in der Gruppenrichtlinie unter “Computerkonfiguration” “Einstellungen” “Windows-Einstellungen” auf “Registry” geklickt werden (s. Abbildung 5) und ein neues “Registrierungselement” erstellt werden. Dort müssen zur Deaktivierung von SMBv1 die folgenden Werte eingegeben werden:

- Aktion: Aktualisieren
- Struktur: HKEY_LOCAL_MACHINE
- Aktion: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- Wertname: SMB1
- Werttyp: REG_DWORD
- Wert: 0

DEAKTIVIEREN DES LANMAN-HASHES BEI NTLMV1

LanMan ist ein Verfahren zum Hashen von Passwörtern. Unter dem Hashen von Passwörtern versteht man ein kryptografische Verfahren, welches dazu dient ein Passwort in einer Form abzuspeichern oder zu übertragen, in der das eigentliche Passwort nicht lesbar ist. Das hier erwähnte LanMan Hash-Verfahren gilt schon seit vielen Jahres als veraltet und angreifbar und wurde bereits vom NTLMv1- und NTLMv2-Verfahren abgelöst. Dennoch ist dieses in Windows weiterhin aktiv und kann noch für Angriffe missbraucht werden.

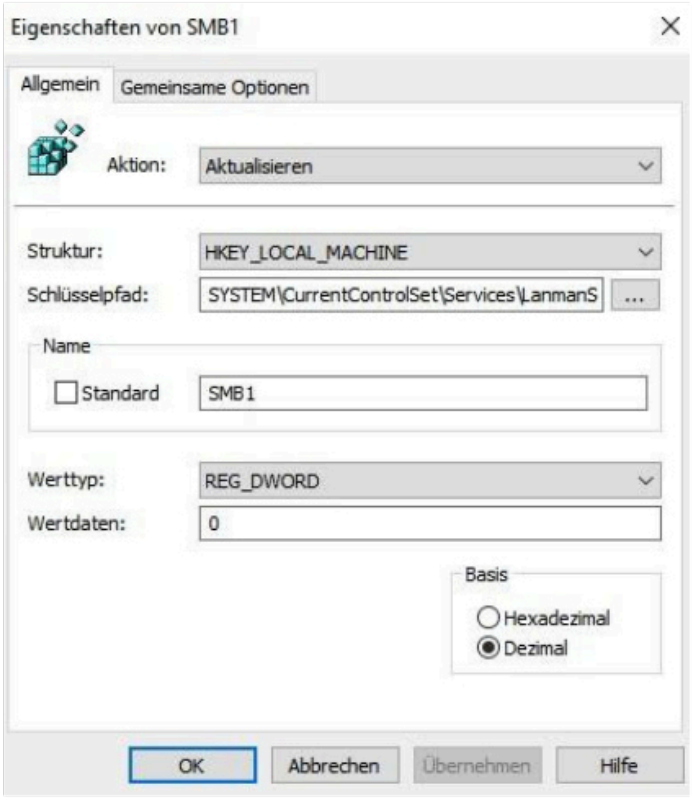

Abbildung 5: Deaktivierung des Server Message Block v1 Protokolls

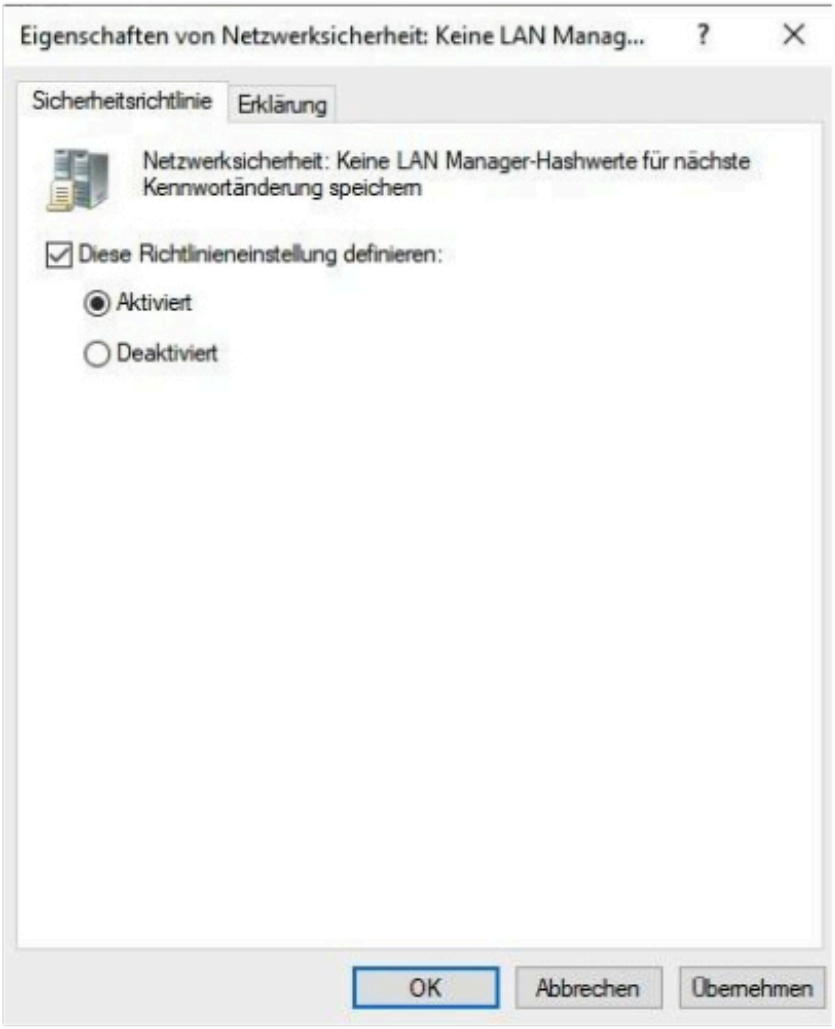

Abbildung 6: Deaktivierung des LAN Manager Hashs

Um dieses Verfahren zu deaktivieren, muss in einer Gruppenrichtlinie die Option “Computerkonfiguration” “Richtlinien” “Windows-Einstellungen” und dort “Sicherheitseinstellungen” ausgewählt werden. Dort muss auf “Lokale Richtlinien” und dort auf “Sicherheitsoptionen” geklickt werden. In der Liste findet sich die Option “Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern” aktivieren, wie in Abbildung 6 gezeigt.

AKTIVIEREN VON SMB MESSAGE SIGNING

Auch das Signieren von SMB Nachrichten muss über einen Eintrag in der “Registry” der Gruppenrichtlinie durchgeführt werden. Dies kann analog zu der Deaktivierung von SMBv1 geschehen. Als Parameter sollten in diesem Eintrag für das neue “Registrierungselement” die Folgenden gesetzt werden:

- Aktion: Aktualisieren
- Struktur: HKEY_LOCAL_MACHINE
- Aktion: System\CurrentControlSet\Services\LanManServer\Parameters
- Wertname: RequireSecuritySignature
- Werttyp: REG_DWORD
- Wert: 1

Platz 4 - Deaktivieren von Makros

MITRE ATT&CK Vector: T1204.002 - User Execution: Malicious File

Der Versand von Word- oder Excel-Dokumenten ist aus dem beruflichen Kontext kaum wegzudenken. Dennoch birgt dieser auch Gefahren für die Informationssicherheit von Unternehmen. In Office-Dokumenten kann mit der Programmiersprache VBA dynamischer Inhalt generiert werden. Diese Eigenschaft kann aber auch von Angreifern genutzt werden, um Schadcode nachzuladen.

Viele der erfolgreichen Ransomware-Kampagnen und auch die Forschung haben gezeigt, das die in Office verwendete Warnung vor Makros von vielen Benutzern ignoriert wird. Daher sollten hier technische Maßnahmen genutzt werden, um die Gefahr vor Makros in Office Dokumenten zu mitigieren, auch wenn durch die in Kapitel Platz 2 - Software Restriction Policies beschriebene Software Restriction Policy die Ausführung des vom Makro nachgeladenen Schadcodes verboten sein sollte. Dennoch darf die Gefahr von Schadcode in Makros nicht unterschätzt werden. Bei fehlerhafter SRP Konfiguration oder Schwachstellen in dieser kann es immer Möglichkeiten geben, die SRP zu umgehen. Office-Dokumente die Makros enthalten können an ihrem Dateinamen erkannt werden. So hat eine Word-Datei mit Makros nicht mehr die Endung “.docx” sondern “.docm”. Analog verhält es sich bei Excel-Dateien und der Endung “.xlsx”/".xlsm".

EINFLUSS AUF DIE INFORMATIONSSICHERHEIT

Die Verbreitung von Schadsoftware über bösartige Makros in Office Dokumenten wie Word oder Excel ist eine der größten Gefahren für Unternehmen. Mithilfe von Makros können Office-Dokumente automatisiert werden. Dennoch wird bei Office-Dokumenten mit Makros, die aus dem Internet geladen werden, Programmcode ausgeführt, dessen Herkunft unbekannt ist. Dieses Risiko sollte durch die Deaktivierung von Makros, welche aus dem Internet geladen werden, behoben werden. Für die Benutzenden, die für Ihre Arbeit auf Makros angewiesen sind, können Ausnahmen eingerichtet werden.

Das BSI behandelt ebenfalls im IT-Grundschutz den sicheren Einsatz von Office Produkten. Die Maßnahmen, welche durch das BSI empfohlen werden, sind dabei in APP.1.1 zu finden. In diesem Maßnahmenkatalog beschäftigen sich unter anderem die Punkte APP.1.1.A10 und APP.1.1.A13.

PLANUNG UND IMPLEMENTIERUNG

In den Gruppenrichtlinien können ebenfalls die Funktionen der Microsoft Office Produkte konfiguriert werden. Daher kann die Deaktivierung der Makros in Office ebenfalls über Gruppenrichtlinien an alle Benutzer des Active Directories ausgerollt werden. Für die Deaktivierung von Makros sollte in der neu angelegten Gruppenrichtlinie auf “Computerkonfiguration” dort auf “Richtlinien” und dort auf “Microsoft Office 2019” geklickt werden. Dort finden sich dann die “Sicherheitseinstellungen”, über die in der Option “VBA für Officeanwendungen deaktivieren” die Officemakros deaktiviert werden können.

Neben der kompletten Deaktivierung von Makros können auch nur Makros, die aus dem Internet stammen, blockiert werden. Darunter fallen Makros aus E-Mails und Makros die über den Browser heruntergeladen wurden. Diese können ebenfalls über Gruppenrichtlinien deaktiviert werden. Dafür sollte diesmal in der Gruppenrichtlinie im Ordner “Microsoft Office 2019” auf “Word-Optionen” und dort auf “Sicherheit” und “Trust-Center” geklickt werden. Hier kann die Ausführung von Makros aus dem Internet über die Option “Ausführung von Makros in Office-Dateien aus dem Internet blockieren” deaktiviert werden.

Platz 5 - Aufteilen von Admin-Accounts

MITRE ATT&CK Vector: T1078.002 - Valid Accounts: Domain Accounts

Ähnlich wie in Kapitel 1 beschrieben ist nicht nur die Trennung von Netzen wichtig, sondern auch von Rechten. Oft reicht es einem Angreifer, einen hoch privilegierten Administrator-Account zu übernehmen. In viele Unternehmen haben die Administratoren über einen Account auf alle Geräte Zugriff. Dies schließt sowohl Clients und Server als auch Domain Controller ein. Falls nun ein Angreifer die Kontrolle über so einen Admin-Account erlangt, hat dieser sofort Zugriff auf die gesamte Infrastruktur. Dieses Beispiel verdeutlicht, wie wichtig die Trennung von Rechten ist auch innerhalb eines Tätigkeitsfeldes oder dem Aufgabengebiet einer Person.

Dadurch, dass heutzutage das Passwortmanagement meistens über Passwortmanager erledigt wird, ist es heutzutage auch kein Problem, gerade Administratoren mehrere Accounts für verschiedene Tätigkeiten zu zuweisen. DIe Accounts sollten zusätzlich über einen zweiten Faktor gesichert werden.

EINFLUSS AUF DIE INFORMATIONSSICHERHEIT

Das Berechtigungsmanagement in einem Unternehmen sollte dem Prinzip von ”Least Privilege” folgen. Das heißt, dass ein Nutzer nur die Rechte haben sollte, die er für eine Aufgabe zwingend benötigt. Demnach hat z.B. auch ein Administrator mehrere Admin-Accounts. So wird sichergestellt, dass Berechtigungen isoliert und atomar sind. Falls durch eine Sicherheitslücke oder einen Fehler seitens des Administrators dessen Account kompromittiert werden, kann der Angreifer nicht direkt auf alle Systeme, Netze und Accounts zugreifen. So sollte evaluiert werden, welche Berechtigungen für welche Tätigkeiten benötigt werden und wie diese sinnvoll aufgeteilt werden können.

In Bezug auf eine Windows Domain ist im Kontext der Administration zu empfehlen, vier verschiedene Accounts zu verwenden. Somit sollte ein Administrator einen normalen User Account haben, wie jeder andere Mitarbeiter auch, einen Admin Account zur Administration von Clients, einen für die Administration von Servern und einen eigenen zur Administration von den Domain Controllern. Somit ist eine hinreichende Berechtigungsisolation vorhanden und die Folgen einer Kompromittierung eines dieser Accounts wird stark eingeschränkt. Bei einer Kompromittierung eines Domain Admin Accounts ist es zwar möglich, diese Sicherheitsmechanismen über die GPOs wieder zu deaktivieren, dennoch ist auch für den Domain Admin Account diese Herangehensweise aus Sicherheitssicht mehr als sinnvoll. Durch dieses Konzept werden Administratoren darin gehindert, sich an anderen Systemen außer den Domain Controllern anzumelden. Dies führt dazu, dass die Credentials dieser Accounts nicht auf einem Server oder Client liegen, wo ein Angreifer diese gegebenenfalls kompromittieren könnte.

Das BSI gibt hierfür im IT-Grundschutz Maßnahmen für das Berechtigungsmanagement vor. Diese können im Baustein ORP.4 - Identitäts- und Berechtigungsmanagement nachgelesen werden.

PLANUNG UND IMPLEMENTIERUNG

Zur Umsetzung dieses Konzeptes können sogenannte WMI-Filter genutzt werden. Dazu erstellt man einen neuen WMI-Filter und legt eine Query in diesem fest. Durch diese Query kann der Filter Systeme filtern, zum Beispiel Server und Clients. Um einen neuen WMI-Filter zu erstellen, geht man in der Gruppenrichtlinienverwaltung unter der Domain auf WMI-Filter und legt über einen Rechtsklick einen neuen Filter an (s. Abbildung 7).

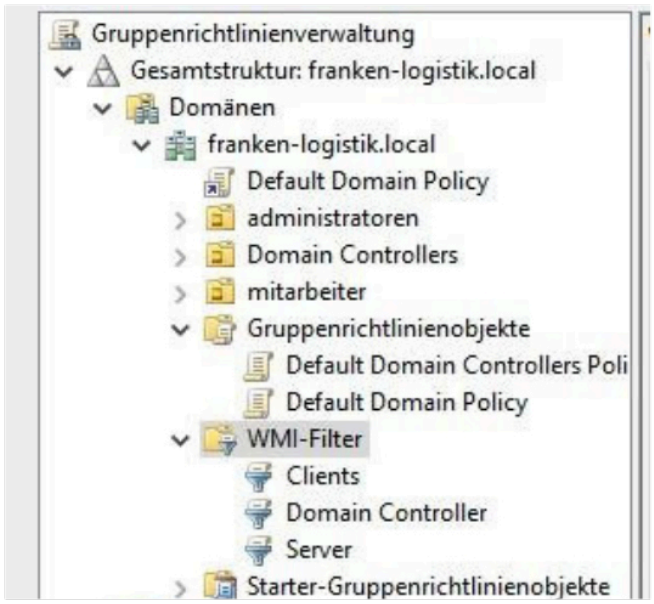

Abbildung 7: WMI-Filter erstellen

Einige Query Beispiele:

- Desktops: SELECT * FROM Win32_ComputerSystem WHERE PCSystemType="1"
- Notebooks und Mobilgeräte: SELECT * FROM Win32_ComputerSystem WHERE PCSystemType="2"
- Server: SELECT * FROM Win32_OperatingSystem WHERE ProductType="3"
- Domain Controller: SELECT * FROM Win32_OperatingSystem WHERE ProductType="2"

Danach kann man eine Group Policy auswählen und einen WMI-Filter, wie in Abbildung 8 gezeigt, auswählen.

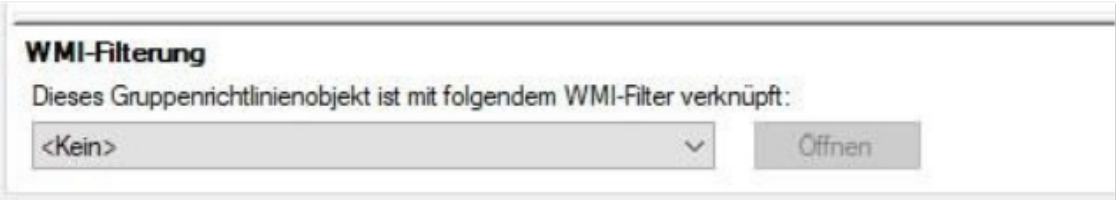

Abbildung 8: WMI-Filter setzen

Durch die WMI-Filter ist somit eine Unterscheidung und Trennung möglich. Die Rechte müssen dann dementsprechend für die jeweiligen GPOs für die einzelnen Admin-Rollen gesetzt werden. Die GPO für den Remotezugriff kann beispielsweise so gesetzt werden:

Computerrichtlinie\Richtlinien\Windows-Einstellungen\
Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von
Benutzerrechten\Anmelden über Remotedesktopdienste zulassen

So kann über diese GPO und weitere dafür gesorgt werden, dass sich die jeweiligen Admin-Accounts nur an ihrem jeweiligen Zuständigkeitsbereich anmelden können.

Platz 6 - Authentifizierung über mehrere Faktoren

MITRE ATT&CK Vector: T1595.002 - Active Scanning: Vulnerability Scanning

Viele Unternehmen setzen heutzutage beim Thema Authentifizierung immer noch ausschließlich auf Passwörter und verwenden keine weiteren Authentifizierungsfaktoren.

Da Passwortrichtlinien zusätzlich oft nicht hinreichend sicher genug erstellt werden, bietet diese Kombination ein hohes Gefahrenpotenzial für die Sicherheit von Unternehmen. Aber selbst wenn Passwortrichtlinien nach ”Best Practice” konfiguriert und unternehmensweit durchgesetzt werden, bieten diese keinen ausreichenden Schutz. Sicherheitslücken in Protokollen, Fehlkonfigurationen in Systemen oder Netzwerken, Keylogger und vieles mehr können zu einer Kompromittierung eines eigentlich starken Passworts führen. Falls ein Passwort kompromittiert wird, ist sofort der gesamte Account betroffen. Ein Angreifer kann sich (gegebenenfalls unbemerkt) mit diesem Account im Netzwerk oder an einem System authentifizieren und weitere Angriffe fahren. Da die Administrator-Accounts auf gleiche Weise abgesichert sind, kann es unter Umständen auch passieren, dass der Angreifer administrative Rechte erlangt.

Somit ist es für eine sichere Authentifizierung zwingend notwendig, weitere Faktoren mit einzubeziehen.

EINFLUSS AUF DIE INFORMATIONSSICHERHEIT

In der Informationssicherheit spricht man im Kontext der Authentifizierung von drei Kategorien:

- Something you know - Etwas was du weißt - z.B. Passwörter
- Something you have - Etwas was du hast - z.B. Token
- Something you are - Etwas was du bist - z.B. Fingerabdruck

Um dafür zu sorgen, dass ein Account nicht vollständig kompromittiert wird, falls ein Authentifizierungsfaktor kompromittiert wurde, sollten mindestens zwei Authentifizierungsfaktoren verwendet werden.

Da biometrische Authentifizierungsfaktoren ihre eigenen Herausforderungen mitbringen, wie beispielsweise ein erhöhter Aufwand bei der Umsetzung der DSGVO, wird in der Realität meistens auf Passwörter plus Token, Smartcard, FIDO, OTP, 2FA-SMS-Code oder Ähnliches gesetzt. Das ganze sorgt dafür, dass selbst wenn ein Passwort kompromittiert wird, nicht direkt der ganze Account betroffen ist.

PLANUNG UND IMPLEMENTIERUNG

Im Folgenden wird beschrieben, wie innerhalb einer Windows Domäne die Authentifizierung mit Smartcards erzwungen und durchgesetzt werden kann. Bei der Wahl der Smartcards ist darauf zu achten, dass diese eine PIN verwenden, dies ist normalerweise der Standard. Wenn ein Nutzer sich anmelden will, muss dieser dann seine Smartcard an den Rechner anschließen, seine persönliche PIN eingeben, um die Smartcard freizuschalten und dann über die Smartcard authentifiziert werden. Dadurch werden zwei Authentifizierungsfaktoren benötigt. Einmal die Smartcard ”Etwas was du hast” und die persönliche geheime PIN ”Etwas was du weißt”.

Um die Smartcard Anmeldung zu aktivieren und zu erzwingen, muss in einer neuen GPO oder einer vorhandenen, die Richtlinie wie folgt aktiviert werden: Als Erstes aktiviert und erzwingt man den Smartcard-Login wie in Abbildung 10 gezeigt.

Computer Configuration\Policies\Windows Settings\
Security Settings\Local Policies\Security Options\Interactive
logon: Require smart card

Abbildung 10: Policy Path: Smartcard aktivieren

Computerrichtlinie\Richtlinien\Windows-Einstellungen\
Sicherheitseinstellungen\Lokale Richtlinien\Interaktive
Anmeldung: Windows Hello for Business oder Smartcard erforderlich

Abbildung 11: Pfad in der Gruppenrichtlinienverwaltung: Smartcard aktivieren

Hierdurch kann sich ein Nutzer nur noch mit einer Smartcard oder Windows Hello Business anmelden.

Als Nächstes muss noch festgelegt werden, was passieren soll, falls eine Smartcard abgezogen wird.

Dafür setzte man die Policy auf Automatisch [Achtung: Bei der von uns verwendeten Windows Version war ein Tippfehler in der Policy: Scmartcard]. Damit wird der Arbeitsplatz automatisch gesperrt, falls die Smartcard abgezogen wird.

Falls sich nun ein Nutzer versucht anzumelden, wird er aufgefordert, sich mit einer Smartcard zu authentifizieren (s. Abbildung 12).

Es ist noch darauf zu achten, dass bei der Zuweisung der GPO nicht die standardmäßige Gruppe ”Authentifizierte Benutzer” gewählt werden kann.

Die Anmeldung per Smartcard sollte für alle Administratoren verpflichtend sein, für normale Anwender ist dies empfehlenswert, muss allerdings im Einzelfall entschieden werden.

Abbildung 12: Smartcard wird gefordert

Platz 7 - KISS-Prinzip

MITRE ATT&CK Vector: T1078.002 - Valid Accounts: Domain Accounts

Das KISS-Prinzip stammt von einem Ingenieur von Lockheed Martin und steht für das Akronym “ Keep it simple and straightforward”. Das KISS-Prinzip bedeutet allgemein gesprochen, das eine Lösung gefunden werden soll, die einfach und verständlich ist. Dieses Paradigma wird häufig in Guidelines zur Softwareentwicklung verwendet, kann aber genauso auf die Administration von Netzwerken angewendet werden.

Bei vielen der durchgeführten internen Pentests konnte festgestellt werden, das die intern genutzten Netzwerke nicht korrekt dokumentiert waren. So konnten zuständige Administratoren teilweise nicht benennen, wofür Systeme genutzt werden. Teilweise waren ganze Netzbereiche oder öffentliche IPs und Systeme unbekannt. Dies sind Probleme, die sich oft auf zu komplexe Netzwerke zurückführen lassen. Wenn die internen Netzwerke bei Unternehmen immer nur wachsen, ohne restrukturiert oder vereinfacht zu werden, führt dies zu vielen Problemen bei der Administration und Sicherung.

Daher empfiehlt es sich bei der Planung von Netzen zu evaluieren, wie diese aufgebaut werden sollten, und dabei kann das KISS-Prinzip ein möglicher Ansatz sein.

EINFLUSS AUF DIE INFORMATIONSSICHERHEIT

Den konkreten Einfluss auf die Informationssicherheit und auf die Planung sowie den Betrieb des internen Netzwerks kann schwer beziffert werden. Dennoch ist es empfehlenswert sicherzustellen, dass die betriebenen Netze wartbar bleiben. Einige Netze von Kunden, bei denen Pentests durchgeführt wurden, waren über Jahrzehnte so gewachsen, das größere Änderungen an diesen kaum mehr möglich waren. Des Weiteren waren Angriffe aufgrund der Menge an Systemen und dem daraus entstehenden Netzwerkverkehr kaum noch erkennbar.

PLANUNG UND IMPLEMENTIERUNG

Bei diesem letzten Tipp handelt es sich um die Vorstellung eines Konzepts das beim Betrieb und der Planung von Netzwerken und Systemen verwendet werden kann. Daher kann hier keine genaue Anleitung für eine Implementierung erfolgen. Dennoch wird im Folgenden auf Punkte eingegangen, bei denen das KISS-Prinzip Anwendung finden kann.

Als Grundlage dafür dient der Netzplan der Franken-Logistik im Kapitel Beispiel-Umgebung. Beim Betrieb und der Absicherung von internen Netzwerken nach dem KISS-Prinzip sollte beachtet werden, nur die Systeme zu betreiben, welche auch notwendig für die internen Arbeitsabläufe sind. Im Fall des Netzplans der Franken-Logistik finden sich dort einige veraltete Systeme, die weiter betrieben werden, obwohl diese bereits ersetzt wurden. Dies ist beispielsweise der Fall bei “DC1OLD”,“SV4”,“SV5” oder “SV6”. Für alle diese Systeme sind bereits neue Systeme vorhanden, welche die alten ersetzen. Diese alten Systeme vergrößern somit nur die Angriffsfläche, mehren die Angriffsvektoren und blockieren Ressourcen. Auch die bereits in Kapitel 1 vorgeschlagene Netztrennung führt zu einer Vereinfachung der Netzwerkumgebung. Durch die klare Gruppierung von Systemen gleicher Funktion in separate Netze wird somit auch die Verständlichkeit und somit Wartbarkeit deutlich erhöht.

Daneben sollte noch beachtet werden, dass die Anzahl der Systeme, die durch die IT verwaltet und gewartet wird, handhabbar bleibt. Bei internen Pentests wurden bereits Netzwerke getestet, welche über 600 Systemen enthielten. Dieses Netzwerk wurde von einem IT-Team mit drei Mitgliedern verwaltet. Dies führt dazu, dass ein Großteil der getesteten Systeme hohe bis kritische Schwachstellen enthält. Daher empfiehlt es sich, die Anzahl der Systeme zu reduzieren, um somit mehr Zeit für die sichere Konfigurationen der eigenen Systeme zu haben.

Wie bei der Franken-Logisitk zu sehen ist, werden viele Systeme mit veralteter Software genutzt. Dies ist ebenfalls eine Schwachstelle, die bei vielen durchgeführten Pentests identifiziert werden konnte. Hier empfiehlt es sich, eine möglichst einfache Lösung zu nutzen und wo es möglich ist, auf automatische Updates zu setzen.

Schlussworte

Die hier beschriebenen Härtungsmaßnahmen sollen keinesfalls eine allumfassende Sammlung darstellen. So gibt es noch viele weitere Maßnahmen, welche je nach eingesetzter Software sinnvoll sein können. Dennoch sollten die hier beschriebenen Maßnahmen einen großen Gewinn für die Informationssicherheit eines Unternehmens darstellen. Besonders Maßnahmen wie die Software Restriction Policy und Einschränkung von Office-Makros können einen erhöhten Schutz vor gängigen Mail-Viren und Ransomware bieten.

Wenn alle hier beschriebenen Maßnahmen auf das Netzwerk der Franken-Logistik angewendet werden, würde dieses wie in Abbildung 13 aussehen. In diesem Netzwerk fehlen die veralteten und nicht mehr genutzten Systeme und das Netzwerk ist in logische VLANs aufgetrennt. Somit sollte die Administration des Netzwerks sowie das Erkennen von Angriffen deutlich leichter fallen.

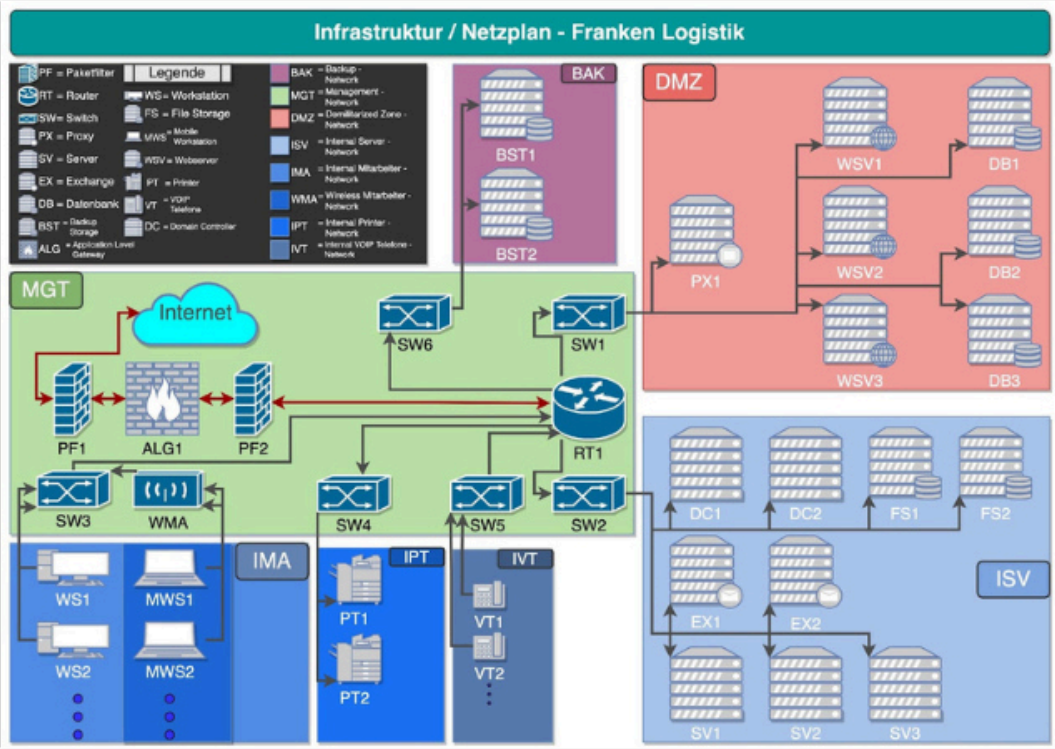

Abbildung 13: Netzwerk der Franken Logistik nach Umsetzung der Tipps

Neben der Härtung der Systeme sollte auch in regelmäßigen Abständen evaluiert werden, ob die angewendeten Maßnahmen effektiv die Systeme vor Angreifern schützen. Dies sollte wie in der Einführung beschrieben über die Simulation von internen Angreifern und Threats passieren. Dafür empfiehlt es sich, professionelle Pentester für die Simulation und Durchführung von Angriffen zu beauftragen. Da ein Pentest immer nur das Lagebild der Sicherheit zu einem bestimmten Zeitpunkt aufzeigen kann, sollten solche Tests in regelmäßigen Abständen durchgeführt werden. Durch die Einführung eines Informationssicherheitsprozesses und der Verstetigung der Bemühungen lassen sich Budgets planen und einsetzen. Bei solch einem internen Test werden die Pentester beim Kunden vor Ort sein und in Absprache mit den Administratoren die Sicherheit des Netzes und der Systeme evaluieren. Ein interner Pentest kann jedoch auch "remote" durchgeführt werden, mit Hilfe von speziellen Pentest-Boxen, welche ins Netzwerk gesetzt werden müssen. Hier müssen die Administratoren nur sicherstellen, dass eine VPN Verbindung von Außen für die Penetrationstester möglich ist.

Über die AWARE7

Die AWARE7 GmbH ist ein Cyber Security Unternehmen aus Gelsenkirchen das Technologien und Produkte entwickelt sowie Dienstleistungen anbietet, die zur Förderung, Steigerung und Erhaltung des IT-Sicherheitslevels dienen. Durch die praktische Arbeit und die regelmäßige Veröffentlichung von wissenschaftlichen Artikeln gelingt es uns komplexe Betrugs- und Angriffsmethoden zu erklären und zu entdecken, um Unternehmen und Behörden zu schützen.

IT-Sicherheit funktioniert nur, wenn die Technik sicher und die Menschen sensibilisiert sind. Komplexe Angriffe nutzen menschliche Schwachstellen in Kombination mit technischen Sicher- heitslücken aus. Betrachten Sie das IT- Sicherheitsniveau in ihrem Unternehmen ganzheitlich auf menschlicher und technischer Ebene. Wir sind in Sachen Sicherheit ganzheitlich an Ihrer Seite.

AWARE7

Kontakt

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen
info@aware7.de

Chris Wojzechowski
Geschäftsführer
+49 209 88306761
chris@aware7.de