Mitgeliefert, aber ungenutzt

Absicherung mit Windows-Bordmitteln

Microsoft liefert mit seinem Windows-Universum etliche Sicherheitsfunktionen als Bordmittel mit, die jedoch weithin nicht zum Einsatz kommen – oft aus Unwissenheit, Zeitmangel oder Sorge, dass hierdurch auch legitime Nutzer behindert würden. Ein genauerer Blick lohnt sich jedoch, meint unser Autor.

Von Carsten Hilgenbrink, Heilbronn

In der Microsoft-Welt bleiben immer noch viele mitgelieferte Mechanismen zur Absicherung der Systeme ungenutzt – dabei haben sie den Vorteil, dass keine zusätzlichen Anschaffungskosten und Einkaufsvorbereitungen anfallen, sondern die jeweilige Lösung direkt erprobt werden kann. In der Regel lassen sich Microsofts Bordmittel über oft schon im Einsatz befindliche zentrale Verwaltungslösungen wie Gruppenrichtlinien flächendeckend ausrollen.

Woran „hängt“ es also? Drittanbieter- oder auch weitere Microsoft-Lösungen, die zusätzliche Lizenzen erfordern, decken gegebenenfalls mehr Anwendungsfälle ab oder sind einfacher zu verwalten. Zudem hat die Härtung beziehungsweise Absicherung von Systemen bisweilen den Ruf, die Arbeit sowohl für Endanwender als auch für Administratoren zu erschweren. Einige Maßnahmen stellen tatsächlich nicht nur Hürden für Angreifer dar, sondern eben in einigen Fällen auch für die eigenen Mitarbeiter, da man mit ihnen das Verhalten des Betriebssystems ändert. Den Anwendern sollte der Sprung über diese Hürde so einfach wie möglich gemacht werden, während ein Angreifer einen sehr viel längeren „Anlauf“ benötigen sollte – Springen müssen aber letzten Endes beide. Sorgt man bei den eigenen Leuten für Aufklärung und gibt Hilfestellung bei Änderungen in der Bedienung, fördert dies die Akzeptanz und die Motivation, zur Unternehmenssicherheit beizutragen.

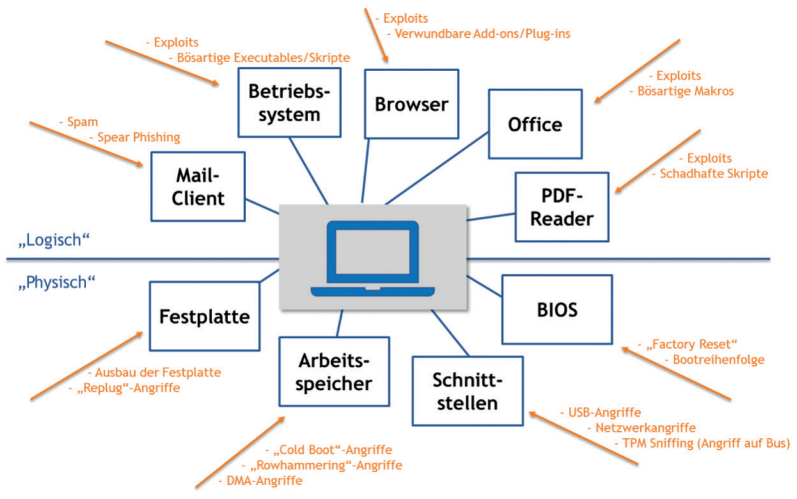

Abbildung 1: Beispielhafte Betrachtung möglicher Angriffsvektoren auf einen Windows-Client

Dennoch verhindert eine Mischung aus Angst vor erhöhtem Aufkommen an Supportanfragen sowie chronischer Unterbesetzung in der IT nicht selten die Implementierung oder zumindest Erprobung von eingebauten Sicherheitsfeatures – auch ein fehlender Überblick über vorhandene, bereits abgedeckte und noch offene Angriffsvektoren für die eigene Umgebung ist hier oft ein weiteres Hindernis. Dabei kann man viele der Windows-Bordmittel im Audit- oder „Was-wäre-wenn“-Modus erproben, was „gefahrenfrei“ Resultate und Erfahrungen mit den Maßnahmen auf produktiven Clients und Servern ermöglicht. Dabei zeigt sich dann oft, dass weniger Seiteneffekte und Produktivitätseinschränkungen auftreten als erwartet.

Überblick verschaffen

Um zu identifizieren, welche Bordmittel einen Mehrwert im Unternehmen bringen, empfiehlt es

sich, zunächst die Angriffsvektoren der genutzten Systeme zu betrachten und diesen die bereits implementierten Schutzmaßnahmen und Sicherheitslösungen gegenüberzustellen. Für einen Windows-Client kann das etwa aussehen wie in Abbildung 1.

Bei der Bedrohungslandschaft für Clients ist neben der logischen Ebene mit Betriebssystem und installierten Applikationen auch die physische Ebene mit Datenträgern inklusive sensibler Informationen und Zugangsdaten oder Schnittstellen mit direktem Zugriff auf den Arbeitsspeicher zu beachten. Des Weiteren darf die Absicherung von Netzwerkschnittstellen und Protokollen nicht vergessen werden, da sie ebenfalls Angriffsmöglichkeiten auf den Client und letztlich – nach dessen erfolgreicher Kompromittierung – auf das Unternehmensnetzwerk darstellen.

Ein guter Ansatz zur Identifikation von Bedrohungen auf hoher Flughöhe ist die Matrix MITRE ATT&CK (https://attack.mitre.org), die einen Überblick über gängige Angriffstechniken und -taktiken sowie Kategorien möglicher Gegenmaßnahmen liefert. Zur Unterstützung bei der Identifizierung von Lücken im Sicherheitskonzept kann man darüber hinaus das Def3nd-Framework hinzuziehen (https://d3fend.mitre.org). Bordmittel und weitere vorhandene Maßnahmen müssen dann nur noch den Kategorien der Gegenmaßnahmen zugeordnet werden, um ein erstes Bild der eigenen Bedrohungslandschaft zu erhalten – dieses umfasst jedoch keine qualitative Bewertung der Schutzmaßnahmen.

Alles an Bord!

Sowohl auf der logischen als auch auf der physischen Ebene vereint Microsoft unter dem Namen „Defender" ein wahres Sammelsurium an Sicherheitsfeatures, das weit über *Defender Antivirus* hinausgeht.

Security by Default

Microsoft hat es in der Vergangenheit nicht geschafft, „Security by Default" in seinen Produkten umzusetzen. Dies war gewiss nicht zuletzt der Kompatibilität und einfacheren Integrationsmöglichkeit in gewachsene Umgebungen geschuldet. Gerade in jüngster Zeit rächt sich der Mangel an sinnvollen sicheren Standardeinstellungen jedoch durch regelmäßig neu entdeckte und einfach ausnutzbare Schwachstellen: Beispielsweise haben veraltete Anmeldeverfahren gepaart mit unzureichend abgesicherten Endpunkten an Exchange oder Outlook Web Access (OWA) Angreifer die Kompromittierung von Systemen unnötig einfach gemacht. Und kaum jemand erinnert sich wohl gern an die PrintNightmare-Schwachstellen im schon etwas in die Jahre gekommenen Spooler-Dienst, der standardmäßig auf Windows-Clients, -Servern und leider auch auf Domänen-Controllern aktiv ist.

Das Release von Windows 11 hat Microsoft zum Anlass genommen, einige essenzielle Sicherheitsfeatures und deren hardwareseitige Voraussetzungen bereits zum Installationsvorgang einzufordern (TPM 2.0, UEFI mit Secure Boot). Sofern bestimmte Hardware wie eine CPU mit Virtualisierungserweiterungen vorhanden ist, werden auch weitere Features – besonders zum Schutz von Zugangsdaten für domänenintegrierte Geräte – automatisch aktiviert, zum Beispiel der „Credential Guard" mit *Enterprise SKU* oder ein Speicherschutz über *Hypervisor-based Code Integrity (HVCI)*. Diese Features sind zwar auch für Windows 10 und teilweise für Windows-Server verfügbar (vgl. Abb.), aber auf ihre Aktivierung wird dort nicht aktiv hingewiesen, geschweige denn werden sie als Default aktiviert.

Im Server-Bereich gibt es ebenfalls Verbesserungen: So wird Windows Server 2019 mit aktivem *Windows Defender Antivirus* ausgeliefert sowie mit Unterstützung für *Defender Exploit Guard* zum Schutz vor typischen Schwachstellen in ausführbaren Anwendungen und zum Schutz vor Zugriffen unerwünschter oder schädlicher Programme (etwa Ransomware) auf bestimmte Ordner. Bei Server 2022 sind HTTPS und TLS 1.3 standardmäßig aktiviert.

Feature	Windows 10	Windows 11 (22H2 Neuinstallation)	Windows Server
SecureBoot/Trusted Boot	o	●	● (ab Server 2022)
BitLocker	● (Mit AD Join)	● (Mit AD Join)	o (ab Server 2016)
DMA-Schutz	o	o	o (nicht für VMs)
VBS	o	●	o (ab Server 2016)
HVCI	o	●	o (ab Server 2016)
HVCI Shadow Stack	–	●	–
Defender Firewall zentrale Regeln	o	o	o
NetBios und LLMNR deaktiviert	o	o	o
WPAD deaktiviert	o	o	o
AppLocker	o	o	o
WDAC	o	o	o
Credential Guard	o	●	o (ab Server 2016)
LSA PPL	o	●	o (ab Server 2016)
Exploit Protection	●	●	● (ab Server 2016)
Network Protection	o	o	o (ab Server 2019)
Controlled Folder Access	o	o	o (ab Server 2019)
Attack Surface Reduction	o	o	o (ab Server 2019)

Legende	
nicht verfügbar	–
verfügbar aber nicht aktiv	o
im Standard aktiv	●

Überblick zu Features, Voraussetzungen und Standardeinstellungen bei verschiedenen Windows-Varianten

Selbst die lokale Firewall heißt mittlerweile *Windows Defender Firewall* mit erweiterter Sicherheit, hat aber keine Abhängigkeiten vom ursprünglichen Antivirus-Programm – andere Features hingegen erfordern, dass Defender Antivirus die primäre Virenschutzlösung auf den Clients ist.

Windows 10/11 bietet für Unternehmen mit Enterprise Edition des Betriebssystems die umfassendsten Bordmittel, um den Client gegen etliche Angriffsvektoren abzusichern. Microsoft-Kunden, die bisher die Pro-Variante von Windows 10/11 einsetzten, mussten bis September 2022 hingegen auf einige Features, wie WDAC und AppLocker, verzichten. Derzeit verbleibt von den hier vorgestellten Bordmitteln allerdings nur noch *Credential Guard* als exklusives Enterprise-Feature.

Physische Angriffsvektoren

Secure Boot und Trusted Boot

Secure Boot ist ein UEFI-Feature, das mithilfe von Signaturen sicherstellt, dass ausschließlich legitime Komponenten und Firmware gestartet werden. Nutzt man ein geeignetes Trusted-Platform-Module (TPM), lässt sich zudem die Integrität des Boot-Vorgangs anhand eines im TPM sicher abgelegten Hashwerts gewährleisten. *Trusted Boot* stellt anschließend sicher, dass auch Kernel, Boot- und Antimalware-Treiber nicht manipuliert wurden. Sollte der Startvorgang verändert worden sein (z. B. durch ein Boot-Kit, ausgetauschte Treiber oder alternative Bootmedien), verlangt das System zum Entsperren von BitLocker den Recovery-Key. Secure und Trusted Boot sollten mittlerweile auf aktuellen Geräten standardmäßig aktiviert sein – Secure Boot ist eine zwingende Voraussetzung für Windows 11.

BitLocker

Mit *BitLocker* bieten Windows 10 und 11 die Möglichkeit, sowohl fest eingebaute Datenträger als auch Wechseldatenträger zu verschlüsseln. Für die Systempartition kann das Schlüsselmaterial, das zum Booten und Entschlüsseln notwendig ist, zusätzlich durch ein TPM abgesichert werden. Bei Aktivierung der Pre-Boot-Authentifizierung (PBA) verlangt das System die Eingabe einer individuellen PIN, um das TPM zu entsperren und das dort abgelegte Schlüsselmaterial zur Entschlüsselung der Systempartition zu nutzen.

Ohne PBA bootet Windows nach positivem Ergebnis der Secure-Boot-Integritätsprüfung bis zum Anmeldebildschirm. Einem Angreifer bietet sich hier nun eine größere Angriffsfläche, da mindestens einige Systemdienste bereits gestartet wurden. Das BitLocker-Laufwerk wird transparent entschlüsselt, das Schlüsselmaterial wurde ohne Eingabe einer PIN freigegeben und liegt im Arbeitsspeicher. Die Übertragung des Schlüsselmaterials vom TPM-Chip zur CPU lässt sich je nach Mainboard-Layout mit bestimmter Hardware und einem Logic-Analyzer (Kostenpunkt circa 800 €) während des Startvorgangs mitschneiden. Ein Angreifer erhält so den BitLocker-Schlüssel und kann die geschützte Festplatte an einem anderen System mounten, um die Daten auszulesen oder zu manipulieren.

Sofern ein Gerät im ausgeschalteten Zustand in die Hände eines Angreifers gelangt, verhindert PBA zudem Direct-Memory-Access-(DMA)-Angriffe, die direkt in den Arbeitsspeicher lesen und schreiben.

DMA-Schutz

Einige Hardwareschnittstellen – wie USB-C mit Thunderbolt, PCI oder FireWire – können grundsätzlich direkt auf Bereiche im Arbeitsspeicher zugreifen und somit Speicherinhalte zur Laufzeit von Programmen, inklusive dort vorhandener Zugangsdaten, lesen und schreiben. Ein Angriffsvektor ist hier, den Adressbereich im Hauptspeicher (RAM), der die Passworteingabe für Benutzeranmeldungen überwacht, zu manipulieren – dadurch ließe sich eine Anmeldung am System ohne Passwort durchführen.

Ist eine I/O-Memory-Management-Unit-(IOMMU)-fähige CPU verbaut, kann man den Kernel-DMA-Schutz aktivieren: Dieser verhindert den Vollzugriff auf den Arbeitsspeicher über neu angeschlossene DMA-fähige Geräte. Gewünschte DMA-Geräte, etwa eine Dockingstation, können von einem angemeldeten Anwender zugelassen und als vertrauenswürdig deklariert werden. Ein Angreifer, der einen gesperrten oder nicht mit PBA geschützten Laptop entwendet hat, kann seine neueren DMA-fähigen Geräte jedoch nicht am Betriebssystem aktivieren und somit keinen vollen Zugriff auf den Arbeitsspeicher erlangen. Ist der Kernel-DMA-Schutz aktiv, erhalten neu angeschlossene Geräte, die über IOMMU-fähige Treiber verfügen, einen isolierten Bereich im RAM zugewiesen – ist kein kompatibler Treiber vorhanden, wird dem Gerät bis zur Benutzerfreigabe gar kein Zugriff gewährt.

Abbildung 2: Der Status der Windows-Bordmittel lässt sich in den meisten Fällen in der Windows-Sicherheit-App einsehen.

Der DMA-Schutz wirkt jedoch nicht auf Legacy-Schnittstellen wie FireWire oder PCExpressCard. Falls diese Schnittstellen in einem Laptop oder PC noch verbaut sind, können DMA-Geräte grundsätzlich deaktiviert werden, bis ein Anwender sich anmeldet. Die Gruppenrichtlinie hierfür heißt „Deaktivieren neuer DMA-Geräte, wenn dieser Computer gesperrt ist". Dies sorgt unter Umständen jedoch für Probleme mit Dockingstations.

Virtualisierungsbasierte Sicherheit

Die Idee hinter der virtualisierungsbasierten Sicherheit (VBS) ist die Isolation sicherheitskritischer Prozesse vom restlichen Betriebssystem. Zu diesen sicherheitskritischen Funktionen zählen beispielsweise der Prozess zur Verwaltung der Benutzerzugangsdaten oder der Prozess zur Verifizierung von Kernel-Treibern, Hersteller-Treibern oder Software.

Für die Implementierung von VBS greift Microsoft auf seine eigene Virtualisierungstechnologie *Hyper-V* zurück: Damit wird der eigentliche Betriebssystemkernel auf der Hardware zu einer Art Gast-Betriebssystem. Gleichzeitig wird ein zweiter, kleinerer Kernel gestartet, der ausschließlich dazu dient, sicherheitskritische Funktionen auszuführen (z. B. die Benutzerauthentifizierung).

Ein klassischer Zugriff auf diese Hypervisor-Schicht, wie etwa zur Steuerung von virtuellen Maschinen (VMs), besteht jedoch nicht. Der Hypervisor stellt lediglich sicher, dass das potenziell verwundbare Betriebssystem nicht direkt auf die sicherheitskritischen Komponenten in isolierten Arbeitsspeicherbereichen zugreifen kann. Stattdessen muss das Betriebssystem dafür spezielle Schnittstellen des Hypervisors nutzen (vgl. Abb. 3). Auch ein Angreifer, der den Betriebssystemkernel übernehmen konnte, hat somit keinen direkten Zugriff auf dessen sicherheitskritische Arbeitsspeicherbereiche des Betriebssystems, da diese in den *Secure Kernel* ausgelagert sind. VBS bildet die Grundlage für die folgenden Verfahren:

- Credential Guard
- Windows Defender Application Control (WDAC) mit HVCI
- Kernel Mode Hardware-Enforced Stack Protection
- Windows Defender Application Guard (hier nicht vorgestellt)

Einige Funktionen lassen sich optional mit einer UEFI-Sperre konfigurieren, um die gewünschten Einstellungen vor Veränderungen durch einen Angreifer zu schützen, der seine Rechte erfolgreich lokal erweitern konnte. Allerdings erschwert dies auch die Administration aus der Ferne, falls eine der geschützten Einstellungen zu Problemen führt und deaktiviert werden soll. In der Regel ist dann physischer Zugriff zum Löschen der UEFI-Variable nötig.

Hypervisor-based Code Integrity

Hypervisor-based Code Integrity (HVCI) basiert auf VBS und schützt Kernelspeicheradressen vor Angriffen über Shellcode oder unsignierten Code, die Schwachstellen im Kernel ausnutzen. HVCI realisiert den Schutz auf Kernel-Ebene, indem Speicherbereiche nie gleichzeitig schreibbar und ausführbar sind (W^X). Angreifer können daher keinen Speicherbereich im echten Kernel erreichen, auf dem sie Shellcode schreiben und anschließend ausführen können.

Hierzu wird der Speicherbereich des echten Kernels nochmals über den Hypervisor virtualisiert und seine Adressierung „übersetzt" (Second-Layer-Address-Translation, SLAT). Aus Sicht des Kernels des Betriebssystems sind daher die physischen Adressen des Speichers nicht bekannt. Somit kann nur über die Hypervisor-Schicht und die dort geltenden Definitionen der Berechtigungen auf einer Speicheradresse auf das physische RAM zugegriffen werden.

Einige Angriffsvektoren gehen darüber hinaus, indem zunächst im User-Mode (!) der Schadcode auf einem Speicherbereich platziert und anschließend bei vorhandener Kernel-Schwachstelle ein Pointer auf den User-Mode-Speicherbereich gesetzt wird. Genau genommen manipulieren Angreifer hierbei nicht die Berechtigungen auf der Adresse im Speicher im Kernel-Mode, sondern machen aus der User-Mode-Page eine Kernel-Page. Hiergegen kann HVCI nicht schützen, da es an dieser Stelle gar nicht aktiv wird.

Vor solchen sogenannten Return-Oriented-Programming-(ROP)-Angriffen soll das mit Windows 11 22H2 eingeführte Feature *Kernel Mode Hardware-Enforced Stack Protection* schützen: Hierbei wird beim Programmstart ein Abbild der Sprungadressen gespeichert und vor Ausführung einer Execute-Anweisung mit den angefragten Speicheradressen abgeglichen – bei Abweichungen wird der Prozess terminiert und der Angreifer kann seinen injizierten Shellcode nicht zur Ausführung bringen. Dieses Feature setzt jedoch moderne CPUs ab AMD Zen3 und Intel Tiger Lake voraus.

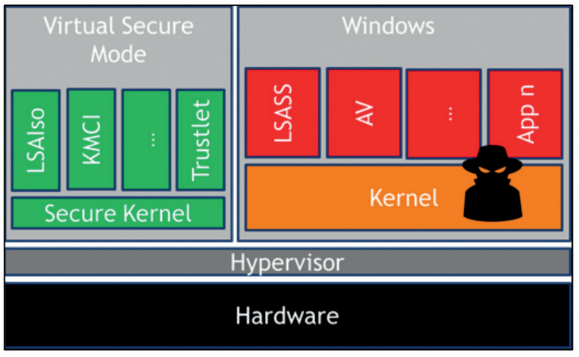

Abbildung 3: Virtualisierungsbasierte Sicherheit durch Isolation sicherheitskritischer Prozesse in einem eigenen Kernel

Netzwerkschnittstellen

Windows Defender Advanced Firewall: Client Isolation / LOLBAS

Die *Windows Defender Firewall* auf Clients ist in vielen Unternehmen bestenfalls aktiviert, jedoch oft nur mit einem lokalen Regelwerk konfiguriert, in das sich jede installierte Anwendung im Zuge des Setups mit einer Allow-Regel eintragen kann.

Zwar stehen Clients und Server in der Regel hinter (zentralen Netzwerk-) Firewalls, um die netzwerkseitige Angriffsfläche aus dem Internet gering zu halten – innerhalb des Client-Netzwerksegments ist dann aber häufig nichts weiter reguliert. Alle Clients können somit untereinander kommunizieren, obwohl es nur einzelne legitime Anwendungsfälle hierfür gibt (z. B. VoIP mit Peer-to-Peer-Anrufen). Werden Systeme voneinander isoliert, nimmt man Angreifern die Möglichkeit, erlangte Zugangsdaten – beispielsweise des lokalen, nicht mit LAPS gesicherten Administrators eines Clients – für Pass-the-Hash-Angriffe auf anderen Clients zu verwenden. Hierzu sollten über die Windows-Firewall eingehende Verbindungen von anderen Clients (außer von den Systemen der Helpdesk-Administratoren) verboten werden.

Die gewünschten Regeln sollten zentral per Gruppenrichtlinie verteilt werden. Standardmäßig werden jedoch zentrale und lokale Regeln, also auch all die unerwünschten Aufweichungen des Regelwerks, zusammengeführt: Um die Kontrolle über Netzwerkverbindungen zu behalten, kann die Firewall per Gruppenrichtlinie *Windows Firewall with Advanced Security – LDAP* (in Computer Configuration / Windows Settings / Security Settings) so konfiguriert werden, dass sie keine lokalen Regeln anwendet (Abb. 4).

Der Gedanke einer Isolation im gleichwertigen Segment gilt ebenso für Server: Webserver A muss in der Regel nicht mit Webserver B kommunizieren, sondern nur mit einem oder einigen Anwendungs- oder Datenbankservern sowie eventuell dem Verzeichnisdienst oder anderen zentralen Infrastruktur-Servern.

Ein weiterer Anwendungsfall zum Schutz der Clients mit der Windows Defender Firewall ist das Blockieren von Netzwerkzugriffen durch „Living off the Land Binaries and Scripts“ (LOLBAS) oder sogenannten Dual-Use-Binaries, die Angreifer häufig nutzen, um unauffällig Schadcode auf das System zu holen. Beispielsweise lässt sich certutil.exe zum Nachladen von Schadcodes missbrauchen – die initiale Attacke enthält dann nur ein Makro oder eine ISO-Datei, die an Mailfiltern, die ausführbare Dateien blockieren, vorbeikommt. Auch wo eingehende Verbindungen gut überwacht und reglementiert werden, ist es doch wahrscheinlich, dass eine ausgehend initiierte Verbindung, also der über die erste Stufe der Malware angestoßene Download, nicht berücksichtigt und gefiltert wird.

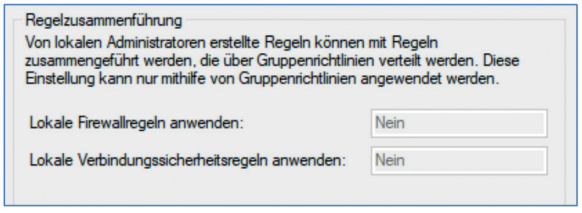

Abbildung 4: Die Zusammenführung von zentralen und lokalen Regeln für die Windows-Client-Firewall sollte deaktiviert werden.

Der in Abbildung 5 gezeigte Auszug an Firewall-Regeln für ausgehende Verbindungen zeigt Deny-Einträge für einige bekannte LOL-Binaries zu beliebigen Netzwerkadressen. Beispielsweise darf hierdurch die PowerShell keine Verbindungen ins Internet aufbauen, wohl aber auf interne Netzwerkressourcen zugreifen, um etwa Startup-Skripte vom SYSVOL-Verzeichnis des Domänen-Controllers zu laden. Eine Liste bekannter LOLBAS findet man beispielsweise im gleichnamigen Projekt auf https://lolbas-project.github.io.

Veraltete Netzwerkprotokolle

Eher eine Härtungsmaßnahme als ein Bordmittel ist die Deaktivierung veralteter Namensauflösungsprotokolle, die in aktuellen Unternehmensumgebungen dank DNS-Server heute keine Verwendung mehr finden sollten. Gemeint sind *NetBIOS, Link-Local Multicast Name Resolution (LLMNR)* und das Web-Proxy-Autodiscovery-(WPAD)-Protokoll. Sie haben gemein, dass sie sich für Man-in-the-Middle-Angriffe im lokalen Netzwerk ausnutzen lassen: Abgefangene Authentisierungsdaten können beispielsweise im Falle von NetNTLMv2-Hashes sowohl zu legitimen Zielen wie Dateiservern weitergeleitet als auch für Offline-Brute-Force-Angriffe zur Passwortberechnung verwendet werden.

Ein Computer sendet NetBIOS- oder LLMNR-Abfragen im lokalen Subnetz als Broadcast, wenn kein Eintrag zu einem aufzulösenden Namen in der Hosts-Datei auf dem lokalen Computer vorhanden ist oder der DNS-Server keinen Eintrag für diesen Namen kennt. In der Regel handelt es sich dabei um Anfragen zu nicht (mehr) existenten Zielsystemen oder um Tippfehler eines Anwenders oder Administrators (z. B. „\\Dileserver“ statt „\\Fileserver“). Der angefragte Name spielt für einen Angreifer im Netzwerk keine Rolle – er antwortet einfach auf alle Anfragen und gibt die IP-Adresse seiner Maschine zurück: Das ursprünglich anfragende System sendet anschließend seine NTLM- oder Kerberos-Authentisierungsdaten in der Annahme an den Angreifer, dass es sich hierbei um ein legitimes Ziel handelt.

_____ *NetBIOS:* Ab Release 22H2 gibt es eine offizielle Gruppenrichtline, die dieses veraltete Protokoll deaktiviert *(Computer Configuration / Administrative Templates / Network / DNS Client / Configure NetBIOS settings)*. Zuvor musste man mithilfe von Skripten oder einzelnen Einträgen in der Registry arbeiten, um NetBIOS flächendeckend zu steuern. NetBIOS kommt jedoch gegebenenfalls in Verbindung mit Druckern im Homeoffice auch heute noch zum Einsatz.

_____ *LLMNR:* Zur Steuerung von LLMNR gibt es bereits seit Längerem eine Gruppenrichtlinie zur Deaktivierung des Protokolls *(... DNS Client / Turn off Multicast name resolution)*.

_____ *WPAD:* lässt sich ab Windows 10 1809 und Windows Server 2019 mit dem Registry-Schlüssel *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableWpad* deaktivieren.

Anwendungs- und Betriebssystemebene

AppLocker vs. Defender Application Control

Was wäre, wenn nur vordefinierte Software gestartet werden könnte? Ausführbare Dateien, die etwa per E-Mail vom Angreifer zum Anwender gelangen, könnten dann nichts ausrichten, da das entsprechende Programm nicht auf der Whitelist steht. Der Abgleich von Datei-Hashes mit einer Liste bekanntermaßen „bösartiger" Hashes erscheint im Vergleich dazu als ein sehr aufwendiges und durch gezielte Mutation von Programmen einfach zu umgehendes Vorgehen. „Application-Allowlisting" ist hingegen eine effiziente Methode, um breit gestreuten Angriffen entgegenzuwirken.

Hier spendiert Microsoft gleich zwei Bordmittel: *AppLocker* und *Windows Defender Application Control (WDAC)* – mittlerweile beide nicht mehr nur für Enterprise-Kunden. Beide Features basieren ähnlich wie eine Firewall auf Regelwerken mit unterschiedlichen Typen. So können Code-Signing-Regeln direkt mehrere Anwendungen eines Herstellers, beispielsweise Microsoft selbst, zur Ausführung zulassen. Das erleichtert es, ein pragmatisches Regelwerk mit überschaubarem Aufwand zu erstellen.

Kompliziertere Fälle, wie veraltete oder intern entwickelte Anwendungen, die nicht signiert sind und von einem Netzlaufwerk gestartet werden, erfordern wiederum eine spezifischere Regel auf Basis des Ausführungspfads oder des Datei-Hashs.

Beiden Verfahren ist gemein, dass sie Starthilfe in Form von Standardregeln und eines Auditmodus liefern: Während bei AppLocker Regeln für bestimmte Benutzer oder Gruppen gelten können, werden die Regeln mit WDAC allerdings systemweit angewandt, was es etwas unflexibler macht. AppLocker-Regelsätze werden per Gruppenrichtlinie verteilt und als Registry-Schlüssel auf den Systemen abgelegt. WDAC wird zwar ebenfalls per Gruppenrichtlinie verteilt, jedoch in Form von kompilierten Richtliniendateien – optional, aber auch idealerweise, in signierter Form. Damit liefert WDAC einen besseren Manipulationsschutz, da Registry-Schlüssel von Administratoren einfach zu ändern sind – zumal die Standardregeln von AppLocker Administratoren globale Ausführungsrechte auf dem System einräumen.

Dennoch ist AppLocker durch die Anwendung von Regeln nach Benutzergruppen das einsteigerfreundliche Mittel zur Anwendungskontrolle mit dem Schutzziel, Anwender vor unvorsichtig geöffneten Dateianhängen und deren Folgen zu schützen. Es gibt jedoch bekannte Umgehungsmöglichkeiten, zum Beispiel über per Standardregeln ausgenommene Ordner mit Schreibrechten für Anwender.

WDAC bietet diesbezüglich einen besseren Schutz mit dem Schutzziel, systemweit vorzugeben, welche Dateien, Treiber, Skripte und auch COM-Objekte ausgeführt sowie geladen werden dürfen. Hier bedarf es im Vergleich zu AppLocker jedoch eines genaueren Gestaltens der Regelwerke, da sich eben keine Ausnahmen – beispielsweise für Administratoren – konfigurieren lassen. Da die Anpassung seitenlanger XML-Dokumente unübersichtlich ist, gibt es für WDAC auch ein Hilfstool mit GUI von Microsoft: den *WDAC Wizard*.

Um WDAC einen noch besseren Integritätsschutz zu spendieren, kann man die durchsetzende Komponente mittels HVCI und VBS schützen – WDAC lässt sich aber auch ohne VBS zur Anwendungssteuerung implementieren.

LSA PPL

Nach der initialen Kompromittierung eines Clients bewegen sich Angreifer zunächst horizontal („seitwärts") im Netzwerk, bis sie einen Client finden, an dem ein höher privilegiertes Domänenkonto

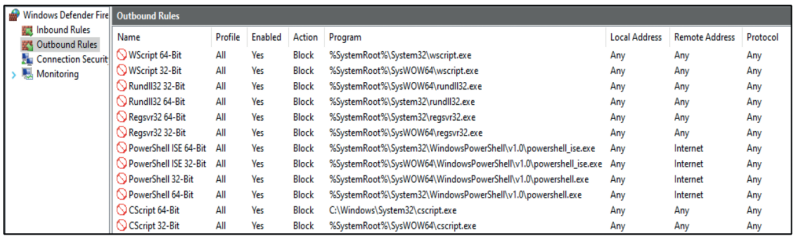

Abbildung 5: Beispielhafte Deny-Regeln für einige LOLBAS

angemeldet ist, um dann dessen Credentials aus dem Arbeitsspeicher zu holen. Hierzu kommen oft Werkzeuge wie Mimikatz zum Einsatz, die sich an den Prozess der Credential-Verwaltung, die LSASS.exe, hängen und den Speicherbereich des Prozesses nach Zugangsdaten durchsuchen. Möglich wird dies zum Beispiel durch das DEBUG-Privileg, das Administratoren grundsätzlich zugewiesen ist. Um den Zugriff auf den LSASS-Prozess abzusichern, gibt es zwei Bordmittel: *Credential Guard* und *Protected Process Light (PPL)*.

Werden Prozesse als PPL definiert, dann können sie nur solche Kernel-Treiber laden, die auch den Windows-Hardware-Quality-Labs und Microsoft-Secure-Development-Lifecycle (MSDL) durchlaufen haben. Zudem können nur andere geschützte Prozesse Code in geschützte Prozesse injizieren oder deren Speicherbereiche lesen. Ist ein solcher Treiber oder Prozess nicht vorhanden, kann selbst mit SYSTEM- oder Admin-Rechten nicht auf den Speicherbereich eines PPL zugegriffen werden.

Der Entwickler des bereits erwähnten Hacker-Werkzeugs Mimikatz konnte in der frühen Phase der Entwicklung des Tools jedoch eine WQHL- und SDL-Signatur für seinen Kernel-Treiber erlangen und somit diesen Schutz umgehen. Dieser Treiber sollte allerdings von allen gängigen Antimalwareprogrammen als schädlich erkannt und blockiert oder gelöscht werden. Bei Neuinstallationen von Windows 11, Version 22H2 ist LSA standardmäßig als PPL aktiviert – zudem wurde mit dieser Version eine neue Gruppenrichtlinie zur Steuerung eingeführt *(Computer Configuration / ADMX / System / Local Security Authority / Configure LSASS to run as a protected process)*.

Credential Guard

Credential Guard nutzt zur Absicherung des LSASS-Prozesses die Isolationsschutzfunktion der VBS: Statt die Credentials im normalen Kernel über LSASS zu verwalten, liegen diese nur noch verschlüsselt vor – das zugehörige Schlüsselmaterial befindet sich im Secure-Kernel in der LSAIso.exe. Ein Auslesen des Speicherbereichs liefert dann keine wiederverwertbaren Zugangsdaten zurück. Allerdings schützt Credential Guard nur Domänenanmeldedaten – und einige Anmeldeverfahren sind nicht mehr möglich, unter anderem die Verwendung von NTLMv1, MS-CHAP-v2 und Kerberos mit DES-Verschlüsselung.

Defender Exploit Guard

Voraussetzung zum Einsatz der Funktionen *Network Protection, Controlled Folder Access* und *Attack Surface Reduction* ist, dass Windows Defender das primäre Antimalwareprogram auf dem System ist – *Exploit Protection* kann hingegen auch in Verbindung mit anderen Virenschutzlösungen eingesetzt werden.

Exploit Protection

Der Exploitschutz ist der direkte Nachfolger des *Enhanced Mitigation Experiance Toolkit (EMET)* und ist mittlerweile standardmäßig aktiviert. Hier können Schutzmaßnahmen entweder systemweit oder anwendungsspezifisch aktiviert werden, um typische Methoden von Anwendungsexploits zu verhindern. Um beispielsweise die Vorhersage von Arbeitsspeicheradressbereichen eines Programms durch den Angreifer zu erschweren, kann die „Speicherverwürfelung“ (Address Space Layout Randomization, ASLR) aktiviert werden. Anpassungen lassen sich über die Windows-Sicherheit-App vornehmen – in den systemweiten Einstellungen sind die meisten Schutzfunktionen mittlerweile standardmäßig aktiviert.

Network Protection

Schutz vor Phishing oder dem Besuch bekannter schädlicher Webseiten liefert *Network Protection*. Microsoft Edge, aber auch fremde Browser werden im sogenannten Block-Modus von Network Protection unterstützt – der Auditmodus ist nur den Browsern aus dem Hause Microsoft vorbehalten. Die *Smart-Screen*-Komponente überprüft eingegebene URLs und IP-Adressen auf schlechte Reputation und verhindert den Zugriff auf bekanntermaßen bösartige Seiten. Zur risikoarmen Erprobung steht bei diesem Feature auch der Auditmodus zur Konfiguration bereit – dieser deckt jedoch nicht alle Bereiche ab. Ist der Zugriffsschutz im Block-Modus aktiviert, werden hingegen beispielsweise auch Webseitenaufrufe aus der PowerShell heraus ausgewertet. Setzt man die kostenpflichtige Funktion *Defender for Endpoint* ein, besteht zudem die Möglichkeit, den Anwender entscheiden zu lassen, ob er eine blockierte Seite dennoch besuchen möchte.

Controlled Folder Access

Nach der Aktivierung des Features *Controlled Folder Access* dürfen nur von Microsoft ausgewählte Programme und Anwendungen mit guter Reputation in von Microsoft ausgewählte schützenswerte Ordner schreiben. Der Hintergrund ist klar: automatisierte Ransomware. Beide Listen, also erlaubte Programme und zu schützende Ordner, lassen sich um eigene Einträge erweitern – die voreingestellten Einträge allerdings nicht entfernen. Die Reputationsermittlung von Anwendungen erfolgt unter anderem auf Basis des Verbreitungsgrads im Unternehmen. Hier kann man zunächst im Auditmodus evaluieren, ob legitime Zugriffe blockiert würden, um die Listen entsprechend anzupassen.

Attack Surface Reduction

Im Laufe der Zeit wurden Muster und wiederverwendete Angriffstechniken bei der Kompromittierung

von Windows-Betriebssystemen identifiziert. Diesen ist mit aktuell 16 Regeln zu begegnen, die oft ausgenutzte Angriffsverhalten erkennen und verhindern. In den meisten Fällen sind die regulierten Aktivitäten für normale Anwender nicht zu bemerken – beispielsweise das Starten eines Kind-Prozesses aus einer Office-Anwendung wie Word. Angreifer versuchen hingegen bisweilen schon über eine E-Mail mit einem Office-Dokument und Makros eine PowerShell zu starten, um hierüber den eigentlichen Schadcode nachzuladen oder interaktiven Zugriff zu erhalten.

Andere Auswirkungen sind weniger verträglich: Die Regel zur Verhinderung der Prozesserstellung über WMI wirkt gleichermaßen bei Angreifern wie auch bei der Softwareverteilung über den „System Center Configuration Manager" (SCCM). Es empfiehlt sich also, auch hier alle Regeln im Auditmodus zu evaluieren, bevor man sie aktiv einsetzt.

Sicherung lokaler Admins

Local Admin Password Solution – LAPS

Um das Kennwort des lokalen Administrators zu verwalten, gibt es schon länger die *Local Admin Password Solution (Legacy LAPS)* – in der früheren Variante noch mit einem zu installierendem Client und einer Server-Komponente versehen, wird die neue Version *Microsoft LAPS* mit den April-Updates 2023 direkt ins Windows-Betriebssystem integriert.

Hintergrund ist die Gefahr für Pass-the-Hash-Angriffe, wenn auf zwei Systemen dasselbe Passwort eines gleichnamigen lokalen Kontos vorhanden ist: Durch die automatische Passwortänderung über LAPS werden einzigartige Passwörter für das konfigurierte administrative Konto sichergestellt. Zum Abrufen werden die Passwörter am AD-Computerobjekt hinterlegt – nur berechtigte Konten oder Gruppen können das Klartextpasswort anzeigen lassen und damit verwenden. Weitere Neuerungen in Microsoft LAPS sind eine optional verschlüsselte Passworthistorie, eine erzwungene Rotation nach Verwendung des verwalteten Kontos und ein Schutz vor Versuchen, das Passwort über andere Wege zu ändern, beispielsweise lokal auf dem Client über die Kommandozeile.

Gruppenrichtlinienbeschränkte lokale Gruppen

Angreifer legen sich nach erfolgreicher Kompromittierung gerne ein eigenes lokales Konto auf einem System als Mitglied der lokalen Administratoren an, um Persistenz zu erlangen. Mittels Gruppenrichtlinie und „eingeschränkter Gruppen" lässt sich definieren, welche Konten und Gruppen Mitglied in welchen lokalen Gruppen sind. Wird die Gruppenrichtlinie *(Computer Configuration / Windows Settings / Security Settings / Restricted Groups)* angewandt, werden alle nicht-definierten Konten aus der Gruppe entfernt.

Fazit

Je nach Angriffsszenario erschweren oder verhindern korrekt implementierte Schutzfunktionen einen Zugriff auf einen Windows-Client oder auf nachgelagerte Systeme über bestimmte Angriffsvektoren. In der Regel wirken Bordmittel gut gegen breit gestreute Angriffe, die auf den Faktor Mensch abzielen – auch gezieltere Angriffe mit ausgereifteren Phishing-Methoden werden durch die volle Ausnutzung der Bordmittel für den Angreifer wesentlich aufwendiger und damit unattraktiver.

Für staatliche Akteure und Advanced Persistent Threats (APTs), also sehr versierte Angreifer mit großen finanziellen Möglichkeiten und damit Zugriff auf noch unbekannte Zero-Day-Exploits, sind die Bordmittel hingegen höchstens noch lästig, da die Angreifer dann mehrere Schutzschichten umgehen müssen. Das kostet Zeit und erfordert den Einsatz unterschiedlicher Angriffstechniken – beides Faktoren, die zur Erkennung eines Angriffs auf Verteidigerseite hilfreich sind. Man sollte jedoch davon ausgehen, dass motivierte und trainierte Angreifer einen Weg finden, diese Maßnahmen auf einem Client zu umgehen.

Aus diesem Grund sind neben technischen Maßnahmen auch Konzepte für ein ganzheitlich hohes Schutzniveau im Unternehmen entscheidend: Diese sollten beispielsweise für administrative Tätigkeiten die Nutzung separater Secure Workstations oder Privileged-Access-Workstations (PAWs) vorsehen, die keine Angriffsfläche durch Office, E-Mail und Surfen bieten, da die entsprechenden Anwendungen darauf nicht installiert oder auf ein Minimum eingeschränkt werden. Mittels Netzwerksegmentierung und Firewalls sollte man administrative Schnittstellen von Clients und Servern (RDP, RSAT, PowerShell-Remoting) nur von diesen PAWs, nicht aber von regulären Clients oder anderen Servern aus erreichbar machen. In Kombination mit Tiering, also dem Klassifizieren von Systemen in unterschiedlichen Schutz- und Vertrauensschichten, sowie dem konsequenten Einsatz unterschiedlicher administrativer Konten pro Schicht, werden kritische Zugangsdaten dann gar nicht erst auf anfälligeren Systemen exponiert. ■

Carsten Hilgenbrink ist Senior Berater bei der cirosec GmbH.

<kes>+

Die Zeitschrift für Informations-Sicherheit

NEU

Mit <kes>+ bleiben Sie auf dem Laufenden über die Entwicklungen in der Informationssicherheit:

- **Fachzeitschrift** <kes> **inkl. Specials** 6x jährlich per Post und digital
- Zugang zu **aktuellen Online-Fachartikeln** und **Studien** sowie zu dem **kompletten Online-Archiv**
- Exklusiver Zugriff auf **aktuelle Videos** und **Webinaraufzeichnungen**
- **10 % Rabatt** auf DATAKONTEXT-Online-Schulungen im Bereich Informationssicherheit
- nur 199,00 € im Jahr (inkl. Mwst. und Versand)

Jetzt bestellen: www.kes.de