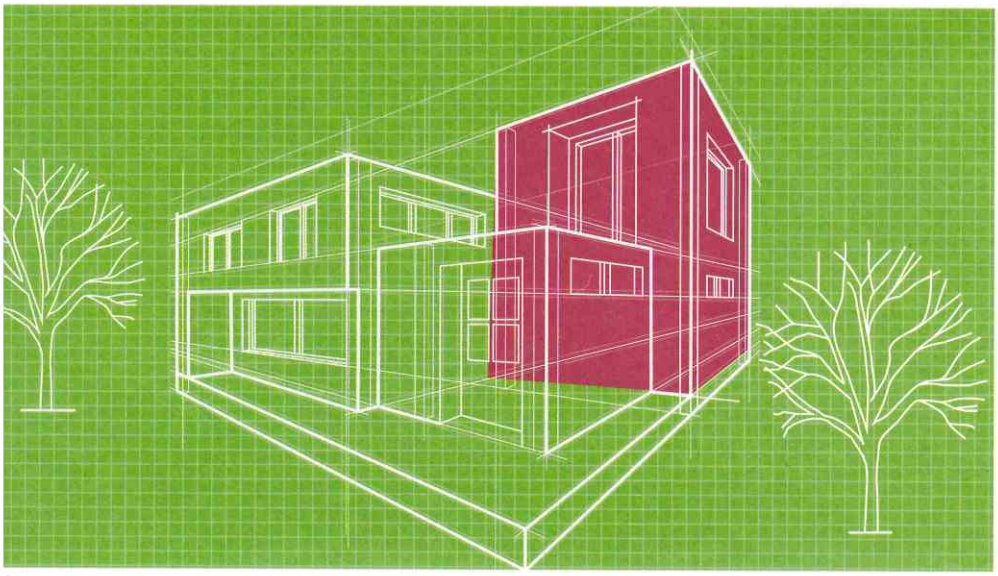


Privilegierte Zugriffe besonders schützen

Privileged Access Workstations sind für die Umsetzung des Enterprise Access Model besonders wichtig und müssen daher sorgfältig abschottet werden.

Von Hagen Molzer

Ein wichtiger Bestandteil des im ersten Teil des Tutorials vorgestellten Enterprise Access Model (Tiering-Modell) zur Absicherung von Active-Directory-Infrastrukturen sind Privileged Access Workstations (PAWs). Dabei handelt es sich um speziell abgesicherte Arbeitsgeräte, von denen aus die zukünftigen Tier-Adminkonten verwendet werden, um zu administrieren.

In der Microsoft-Dokumentation sind sie sehr treffend beschrieben (siehe ix.de/zw57): „Privileged Access Workstations provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors" (zu Deutsch etwa: Privileged Access Workstations stellen ein dediziertes Betriebssystem für vertrauliche Aufgaben zur Verfügung, das vor Internetangriffen und Bedrohungsvektoren geschützt ist).

Ein stark reglementiertes Arbeitsgerät

Durch den sehr spezifischen Einsatzzweck einer PAW und die strengen Einschränkungen wird die Angriffsfläche dieser Geräte deutlich reduziert. So sollte auf einer PAW beispielsweise kein Internetzugriff und kein E-Mail-Empfang möglich sein und es sollten keine PDF- oder Office-Dateien aus nicht vertrauenswürdigen Quellen verarbeitet werden können.

Zudem sollte das Clean-Source-Prinzip für die eingesetzte Software gelten. Das bedeutet, das Betriebssystem-Image ist direkt vom Hersteller herunterzuladen und seine Hash-Prüfsumme mit dem vom Hersteller genannten Wert zu vergleichen. Dasselbe gilt auch für Werkzeuge von Drittherstellern wie Notepad++ oder 7Zip.

Bei der Beschaffung der neuen PAW-Hardware ist überdies darauf zu achten, dass diese nach Möglichkeit alle wichtigen sicherheitsrelevanten Anforderungen erfüllt:

- 64-Bit-CPU (gegebenenfalls bereits basierend auf der Microsoft-Pluton-Sicherheitsarchitektur, siehe ix.de/zw57);
- CPU mit Intel VT-x oder AMD-V;
- CPU-Befehlssatz für Speicherzugriffsschutz (I/O Memory Management; IOMMU);
- SLAT (Second Level Address Translation) oder dessen Intel-Implementierung EPT (Extended Page Table);
- TPM 2.0 (möglichst in die CPU integriert und nicht als separates Bauteil auf dem Mainboard);
- UEFI Secure Boot;
- auf dem Mainboard fest verlöteter Arbeitsspeicher.

In puncto physische Sicherheit der PAW muss jedes Unternehmen wieder den für sich passenden Kompromiss finden. Bei Firmen mit besonders hohem Sicherheitsanspruch kann eine PAW beispielsweise eine Workstation sein, die in einem Metallkäfig in einem speziell gesicherten „PAW-Raum" mit auf biometrischen Authentifizierungsmechanismen basierendem Zutrittskontrollsystem untergebracht ist. Andere Firmen nutzen ein mobiles Notebook und geben den Administratoren über organisatorische Regeln vor, dass sie die PAW zwar im Homeoffice verwenden dürfen, nicht aber in einem Hotel-WLAN oder im Zug.

iX-TRACT

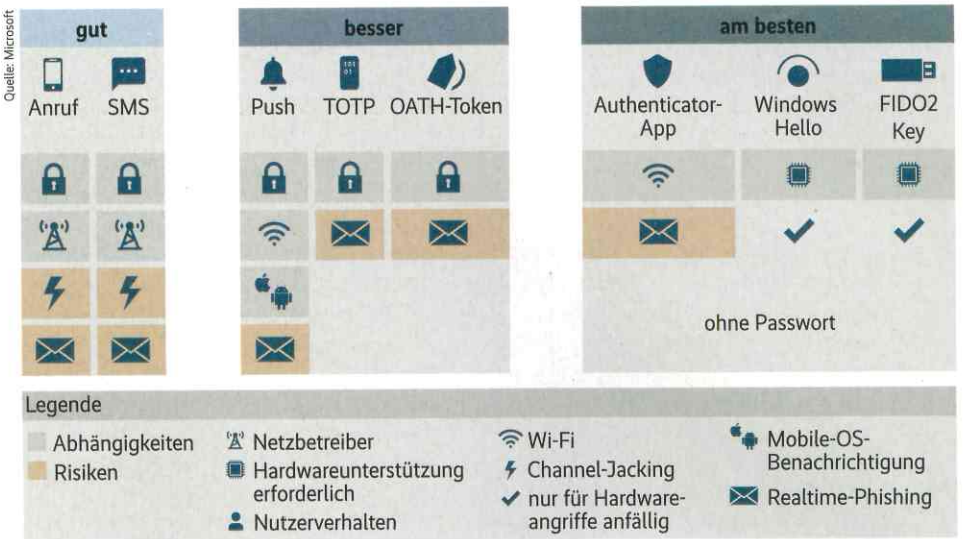
- Für privilegierte Zugriffe auf Systeme sind besonders gesicherte Workstations erforderlich. Dazu gehören hardwareseitige Voraussetzungen, aber auch Restriktionen bei Software und Benutzung.
- Mit zunehmender Anzahl und höherem Härtungsaufwand bei den Privileged Access Workstations steigt auch das Sicherheitsniveau der Infrastruktur.
- Für die Absicherung der Privileged Access Workstations gilt es nicht nur, restriktive Härtungsmaßnahmen umzusetzen, elementar ist außerdem die Authentifizierung und das Schützen der Zugangsdaten.

Tutorialinhalt

Teil 1: Grundlagen – Design, Klassifizierung und Implementierung der Tiers

Teil 2: Privileged Access Workstations (PAW) – Absicherung, Werkzeuge und administrative Zugriffe

Teil 3: Privileged Account/Access Management (PAM), AD-Struktur, Netzwerksegmentierung



Microsoft gibt Hilfestellung bei der Einschätzung der Sicherheit diverser zweiter Faktoren zur Authentifizierung (Abb. 1).

Die Anmeldung der Tier-Adminkonten an der PAW lässt sich zusätzlich über Mehr-Faktor-Authentifizierung absichern. Dabei sollte ein möglichst sicherer zweiter Faktor genutzt werden. Abbildung 1 zeigt, wie Microsoft die Qualität der verschiedenen MFA-Arten einschätzt.

Je nachdem, für welche Implementierungsart des Tiering-Modells man sich im ersten Tutorialteil „Active Directory mit Tiering-Modell schützen" [1] entschieden hat (also welche Tiers ausschließlich von PAWs aus administriert werden dürfen), und je nach Anzahl der Administratoren der betroffenen Tiers kann die Zahl der zu beschaffenden und zu betreibenden PAWs schnell ziemlich groß werden. Deshalb gilt es auch hier wieder, einen Kompromiss zu finden.

PAW-Umsetzung mit getrennten Geräten

Die sicherste Lösung besteht im Anschaffen eines zweiten physischen Geräts, das ausschließlich für die Administration genutzt wird. Auf dem ersten, gegebenenfalls bereits vorhandenen Gerät kann dann weiter regulär gearbeitet werden, inklusive Internet- und E-Mail-Nutzung. Das erlaubt eine strikte Trennung zwischen administrativem und regulärem Arbeiten und es besteht keine Angriffsfläche durch Office-Software oder Webseiten.

Außerdem ist so für die Administration das Clean-Keyboard-Prinzip erfüllt. Dieses schreibt vor, dass bereits der erste Computer der eventuell längeren Zugriffskette für die Administration (also der Computer, an den die physische Tastatur angeschlossen ist, die der Administrator bedient) ein besonders sicheres System sein muss. Warum dieses Prinzip besonders wichtig ist, wird in den nachfolgenden Szenarien noch genauer beleuchtet. Auf separater Hardware bereiten auch besonders strikte Härtungsmaßnahmen keine größeren technischen Probleme.

Der Nachteil dieser Variante ist, dass durch die zusätzlichen Computer Kosten für Hardware, Software und den Verwaltungsaufwand entstehen. Außerdem ist die Arbeit für die Administratoren umständlicher, da sie nun zwei Geräte nutzen und gegebenenfalls transportieren müssen. Je nachdem, wie strikt die Absicherung der PAW umgesetzt wird, sind die Kollaborationsmöglichkeiten der Administratoren eingeschränkt, da kein Teams-Client auf der PAW vorhanden sein darf und kein Internetzugriff besteht.

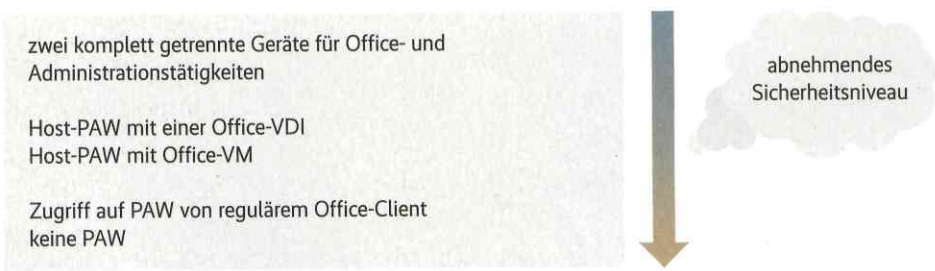
Host-PAW mit Office-VM

Eine mögliche Alternative, die keine Beschaffung neuer PAW-Computer erfordert, ist es, den von den Administratoren bereits verwendeten regulären Computer zu formatieren und nach einer Neuinstallation als PAW einzurichten. Anschließend wird auf der PAW ein Hypervisor installiert (beispielsweise VirtualBox oder VMware Workstation) und der reguläre Computer wird in Form einer VM virtualisiert. Die Anmeldung mit dem Tier-Adminkonto und die administrativen Tätigkeiten erfolgen direkt von der Host-PAW, in der Office-VM dagegen können E-Mails bearbeitet oder Webseiten besucht werden.

Somit spart man sich die Anschaffung eines zweiten Computers und der Administrator hat die PAW und sein reguläres Arbeitsplatzsystem immer dabei, was das Arbeiten komfortabler und flexibler macht. Der letzte Punkt kann aber auch ein Nachteil sein. Der Administrator hat dann nicht mehr die Möglichkeit, die PAW in potenziell unsichere Umgebungen gar nicht erst mitzunehmen. Im schlimmsten Fall könnte die PAW beispielsweise in größeren Besprechungen zur Mittagspause im eingeschalteten Zustand im Konferenzraum zurückbleiben.

Ein weiterer großer Nachteil dieser Variante ist, dass es keine strikte Trennung der beiden Geräte gibt. Das bedeutet, dass sich die PAW und die Office-VM eventuell ein Netzwerkinterface teilen, was die Isolierung der PAW in einem PAW-Netzwerk erschwert oder ganz verhindert. Der Hypervisor bringt eine weitere Angriffsfläche auf die PAW. Über einen VM-Guest-to-Host-Exploit ist es einem fortgeschrittenen Angreifer unter Umständen möglich, aus der Office-VM auszubrechen und den darunterliegenden Hypervisor und damit die PAW zu kompromittieren.

Weitere potenzielle Probleme bestehen beim regulären Arbeiten in der Office-VM. Es kann zum Beispiel zu Performanceproblemen bei der Wiedergabe von Videos oder grafisch anspruchsvollen Anwendungen kommen, da oft die GPU nicht durch die VMs nutzbar ist oder die



Je mehr finanzieller und organisatorischer Aufwand betrieben wird, desto höher ist letztlich auch das Sicherheitsniveau (Abb. 2).

zusätzliche Virtualisierungsschicht andere Probleme bereitet. Auch der Einsatz von Bluetooth-Headsets oder anderer Peripherie etwa in Teams oder Zoom kann beeinträchtigt sein.

Office-VM aus dem Netz

Eine Weiterentwicklung der zuletzt genannten Implementierung ist es, die Office-VM nicht auf der PAW selbst, sondern in einer Virtual Desktop Infrastructure (VDI) im Firmennetzwerk zum Beispiel als Citrix-VM zu betreiben. Aufgrund der stärkeren Trennung der beiden Systeme im Vergleich zum vorigen Szenario besteht dann keine Angriffsfläche durch Guest-to-Host-Exploits und die Isolierung der PAW in PAW-Netzwerk wird viel einfacher umsetzbar.

Die potenziellen Performance- und Peripherieprobleme bestehen jedoch weiterhin. Als Nachteil lässt sich anführen, dass ein „Offline-Arbeiten", also ein Arbeiten in der Office-VM ohne Verbindung zum Firmennetzwerk, nicht mehr möglich ist.

Besser nicht: Zugriff auf PAW von regulärem Office-Client

Ein oft diskutierter Ansatz besteht darin, die PAW auf dem regulären Arbeitsnotebook zu virtualisieren und von der PAW-VM aus zu administrieren. Das widerspricht aber dem Clean-Keyboard-Prinzip und wird von Sicherheitsexperten nicht empfohlen.

Denn ein Angreifer, der das reguläre Notebook kompromittieren konnte, hat viele Möglichkeiten, auch die PAW zu kompromittieren. Er könnte beispielsweise Keylogger- oder Screen-Monitoring-Software installieren oder die PAW-VM einfach an einen anderen Ort kopieren. Abbildung 2 fasst die verschiedenen PAW-Implementierungen entsprechend ihrem Sicherheitslevel zusammen.

Die Maßnahmen zur Absicherung und Härtung der PAW sind vielfältig. Die meisten kennt man häufig schon aus den „normalen" Katalogen von Maßnahmen zur Härtung von Windows. Aufgrund der höheren Sicherheitsanforderungen der PAW sollten sie hier strikter umgesetzt werden. Laxere Einstellungen lösen vielleicht Kompatibilitätsprobleme und Kompromisse bescheren dem Administrator mehr Bequemlichkeiten, letztlich zieht das aber größere Risiken nach sich.

Auch hier gereicht der spezifische Verwendungszweck der PAW zum Vorteil: Härtungsempfehlungen sind in der Regel einfacher umsetzbar als auf regulären Clients, die sehr unterschiedliche Anforderungen erfüllen müssen. Die wichtigsten Maßnahmen zur Client-Härtung – ohne Anspruch auf Vollständigkeit – sind im gleichnamigen Kasten aufgeführt.

Administrative Zugriffe und Werkzeuge

Durch den Einsatz von Tier-Adminkonten ist eine wichtige Maßnahme zum Schutz der hochprivilegierten Identitäten umgesetzt. Diese Konten gilt es nun auf den verwalteten Systemen beziehungsweise im Netzwerk zu schützen. Da mit ihnen andere Systeme verwaltet werden, müssen sie auf Systemen in ihrem jeweiligen Tier verwendbar sein.

Ein Angreifer, der bereits in ein System (zum Beispiel Client, Terminalserver oder Webanwendungsserver) eingedrungen ist, kann ein Tier-Adminkonto unter bestimmten Voraussetzungen kompromittieren, nachdem sich der Administrator mit dem betreffenden System verbunden hat. Je nach verwendeter Anmeldeart des Administrators kann der Angreifer zum Beispiel Passwort-Hashes oder Kerberos-Tickets der privilegierten Konten auf den verwalteten Systemen auslesen, sofern sie sich dort befinden.

In einem Szenario, in dem ein Angreifer einen Tier-1-Webserver über die Ausnutzung einer Schwachstelle in der Webanwendung kompromittiert hat, verfügt er zunächst nur über Rechte auf diesem einen Server. Sollte er im weiteren Verlauf in der Lage sein, den NTLM-Hash eines Tier-1-Adminkontos auszulesen, weil sich der Administrator über RDP mit dem Server verbunden hat, steigt die Zahl der Server, über die er administrative Kontrolle erlangt, möglicherweise stark an. Im schlimmsten Fall hat das Tier-1-Adminkonto auf allen Servern administrative Rechte, wodurch die gesamte Tier 1 fällt.

Die verschiedenen Anmeldetypen von Windows

Um dieses Risiko zu reduzieren, muss man die verschiedenen Anmeldetypen in einem Windows-System kennen. Die

Die wichtigsten Maßnahmen zur Client-Härtung

- Clean-Source-Prinzip für jegliche Hard- und Software
  - aber auch für die Grundinstallation (PAWs sollten beispielsweise nicht über RDP von einem bereits potenziell kompromittierten Rechner installiert werden, sondern aus einer sicheren und „sauberen" Umgebung heraus)
- Basishärtung des Betriebssystems, zum Beispiel nach
  - Microsoft Security Baseline (siehe ix.de/zw57)
  - CIS-Benchmarks des Center for Internet Security (siehe ix.de/zw57)
- besonderer Fokus auf Minimalinstallationen
  - Limitierung und Standardisierung der installierten Software
- Festplattenverschlüsselung (zum Beispiel BitLocker mit Pre-Boot-Authentifizierung)
  - TPM 2.0
- Mehr-Faktor-Authentifizierung für Anmeldung (zum Beispiel über Smartcard oder Windows Hello for Business)
- Least-Privilege-Prinzip
  - keine lokalen Administratorrechte auf der PAW für reguläre Tier-Administratoren
- systemindividuelles Passwort des lokalen Administrators (zum Beispiel über LAPS)
- zeitnahes und regelmäßiges Installieren von Sicherheitsupdates
  - Betriebssystem
  - Drittherstellersoftware
- UEFI Secure Boot
- Antivirensoftware
- EDR-Software
- Windows Defender
  - Exploit Guard – Exploit Protection
  - Exploit Guard – Attack-Surface-Reduction-Regeln
  - Windows Defender Advanced Firewall / Windows-Firewall (eventuell mit IPsec-Verschlüsselung von besonders sensiblem Netzwerkverkehr)
- Credential Guard
- Application Whitelisting (zum Beispiel über AppLocker)
- Kernel DMA Protection (IOMMU)
- Anmeldungen von Non-Tier-Admins explizit verbieten
  - Deny Logon Restrictions

Verbindungsmethoden und wohin Zugangsdaten übertragen sowie zwischengespeichert werden

Verbindungsmethode	Anmeldetyp	Wiederverwendbare Zugangsdaten auf Zielsystem	Kommentare
Log on at console	Interactive	✓	beispielsweise Hardware Remote Access / Lights-out Cards oder netzwerkbasierte KVM-Switches
`runas`	Interactive	✓	
`runas /NETWORK`	NewCredentials	✓	Klont vorhandene LSA-Sitzung für lokalen Zugriff, nutzt jedoch neue Zugangsdaten bei Zugriff auf Netzwerkressourcen.
Remote Desktop (success)	RemoteInteractive	✓	Wenn der RDP-Client Zugriff auf lokale Geräte und Ressourcen gewährt, können diese gegebenenfalls auch kompromittiert werden.
Remote Desktop (failure – logon type was denied)	RemoteInteractive	–	Bei einem fehlerhaften Log-in-Versuch werden Zugangsdaten standardmäßig nur sehr kurz zwischengespeichert.
`Net use * \\SERVER`	Network	–	
`Net use * \\SERVER /u:user`	Network	–	
MMC snap-ins to remote computer	Network	–	Beispiel: Computerverwaltungskonsole, Ereignisanzeige, Device-Manager, Dienste
PowerShell WinRM	Network	–	Beispiel: `Enter-PSSession server`
PowerShell WinRM with CredSSP	NetworkClearText	✓	`New-PSSession server -Authentication Credssp -Credential cred`
PsExec without explicit creds	Network	–	Beispiel: `PsExec \\server cmd`
PsExec with explicit creds	Network + Interactive	✓	`PsExec \\server -u user -p pwd cmd` erstellt mehrere Logon-Sessions.
Remote Registry	Network	–	
Remote Desktop Gateway	Network	–	Authentifizierung an Remote Desktop Gateway
Scheduled task	Batch	✓	Passwort wird zusätzlich als LSA-Geheimnis auf der Festplatte gespeichert.
Run tools as a service	Service	✓	Passwort wird zusätzlich als LSA-Geheimnis auf der Festplatte gespeichert.
Vulnerability scanners	Network	–	Die meisten Scanner nutzen standardmäßig Netzwerkanmeldungen. Unter Umständen nutzen manche Hersteller jedoch auch Non-Netzwerkanmeldetypen und erhöhen somit das Risiko für das Stehlen von Zugangsdaten.

nachfolgenden Informationen dazu stammen aus den beiden Artikeln „Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft" von Microsoft (siehe ix.de/zw57). Zwar sind die Artikel bereits knapp zehn Jahre alt, haben aber an Relevanz kaum eingebüßt, weshalb die Lektüre der beiden Dokumente ausdrücklich empfohlen wird.

Zur Fernverwaltung eines Systems unterscheidet Windows grob die beiden Anmeldetypen

- Interactive Logon und Remote Interactive,
- Network Logon und Network Cleartext.

Zu den Zugriffsarten mit interaktivem Anmeldetyp gehören:

- Remote Desktop (RDP)

- Konsolen-Log-in (auch Remote-Lights-out-Hardware), (Netzwerk-) KVM, VM-Konsole bei Hypervisor
- `runas`
- `runas /NETWORK` (Zugriff auf Netzwerkressourcen)
- `PSExec \\MyServer -u Admin -p Secret123! cmd.exe`

Verräterischer Arbeitsspeicher

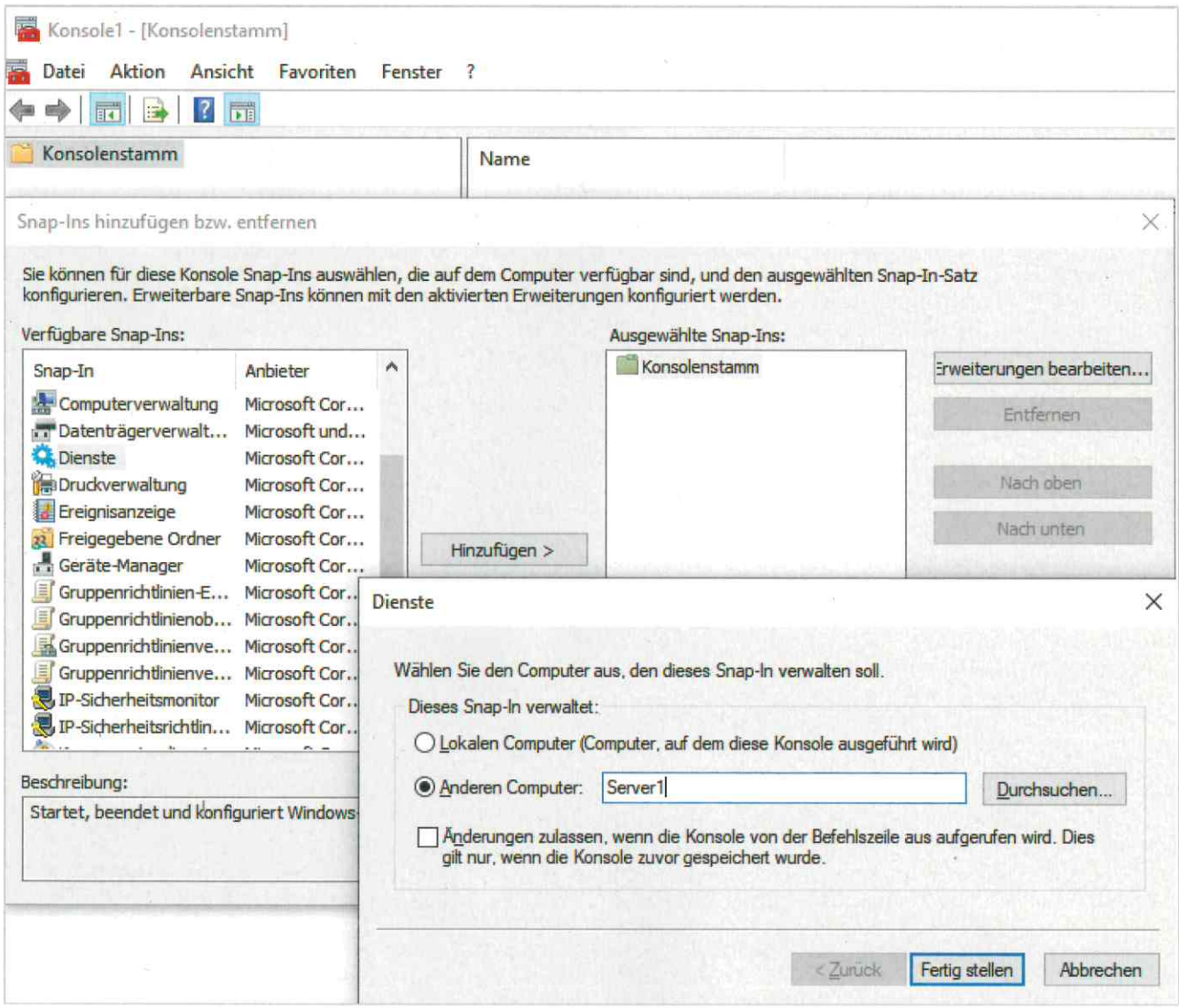
Problematisch bei Zugriffsarten mit interaktivem Anmeldetyp ist die Übertragung von wiederverwendbaren Zugangsdaten des Administrators an das Zielsystem. Dadurch befinden sie sich im Arbeitsspeicher des Systems. Ein Angreifer kann dann zum Beispiel den NTLM-Hash oder Kerberos-Tickets des Tier-Adminkontos extrahieren und wiederverwenden. Beispiele für Netzwerkanmeldungen sind:

- Verbindung zum Zielserver über MMC Snap-In
- `net use \\server\share /u Admin`
- PowerShell Remoting: `Enter-PSSession MyServer`
- Remote Registry
- Remote Desktop Gateway (Authentifizierung erfolgt am RDP-Gateway)
- `PSExec \\MyServer cmd.exe` (ohne explizite Zugangsdaten)

Bei diesem Anmeldetyp liegt der Vorteil darin, dass keine wiederverwendbaren Zugangsdaten des Administrators auf dem System, auf das er zugreift, hinterlassen werden. Ein Single Sign-on (SSO), an das sich Benutzer im Windows-Umfeld gewöhnt haben, ist aber prinzipbedingt nicht möglich. Die SSO-Funktion ist einer der Gründe, warum bei den interaktiven Anmeldetypen die Zugangsdaten überhaupt an das Zielsystem übertragen werden.

Anderenfalls könnte man beispielsweise nicht per RDP auf einen Terminalserver und von dort auf einen Dateiserver im internen Netzwerk zugreifen, ohne auf dem Dateiserver nochmals seine Zugangsdaten einzugeben. Die Authentifizierung kann an der Stelle der Terminalserver übernehmen, da er die Zugangsdaten bereits bei der Anmeldung über RDP erhalten hat. Weitere sicherheitsrelevante Details zu den verschiedenen Zugriffsarten zeigt die Tabelle „Verbindungsmethoden und wohin Zugangsdaten übertragen sowie zwischengespeichert werden" (Microsofts Original ist in den genannten Artikeln zu finden, siehe ix.de/zw57).

Aufgrund der geschilderten Eigenschaften der beiden Zugriffsarten sollte der Administrator wo immer möglich auf interaktive Anmeldungen zur Administration verzichten und auf Netzwerkanmeldungen basierende Zugriffe bevor-



Mit den passenden Werkzeugen gestaltet sich auch die Netzwerkanmeldung weniger aufwendig. Hier wird bei der Remoteverwaltung eines Servers mmc.exe eingesetzt (Abb. 3).

zugen. Das setzt zwar oft eine Umgewöhnung in seiner Arbeitsweise voraus, kann aber letztlich die Administration auch beschleunigen. Denn mit den entsprechenden Werkzeugen mmc.exe (siehe Abbildung 3), den Remoteserver-Verwaltungstools (RSAT) oder mit PowerShell Remoting entfällt die „aufwendigere" interaktive Anmeldung über RDP.

Ein Königreich für einen Slot!

Microsoft hatte ohnehin nie geplant, RDP zum regulären Administrieren eines Servers zu verwenden. Das sieht man auch daran, dass standardmäßig nur zwei RDP-Sitzungen gleichzeitig auf einem Server möglich sind. Insbesondere in größeren Unternehmen käme man als Administrator kaum mehr zum Arbeiten, wenn RDP für die reguläre Administration unerlässlich wäre. Die Haupttätigkeit der Administratoren bestünde dann darin, andere Administratoren anzurufen und um einen der beiden RDP-Slots zu betteln.

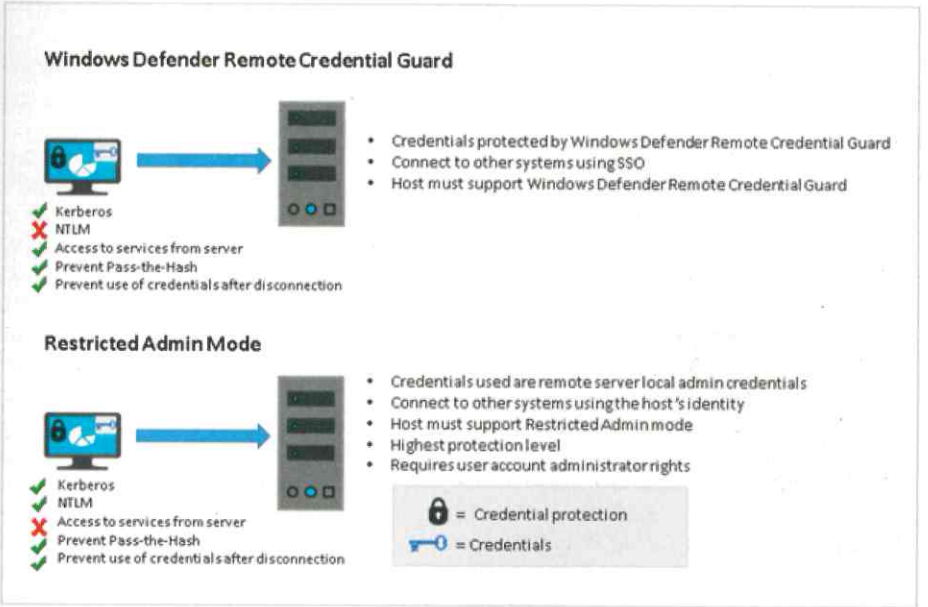
Dennoch gibt es Fälle, in denen man auf die grafische Oberfläche des Betriebssystems angewiesen ist, zum Beispiel wenn für eine Softwareinstallation ein Wizard bedient werden muss oder eine Interaktion mit einer installierten Software notwendig ist, auf die ausschließlich lokal zugegriffen werden kann. In diesen Fällen ist RDP weiterhin ein probates Mittel, die RDP-Verbindung sollte aber zusätzlich absichert werden. Hierfür stellt Microsoft zwei Mechanismen zum Identitätsschutz bereit, Remote Credential Guard und Restricted Admin Mode. Bei beiden werden die Zugangsdaten des zugreifenden Benutzers nicht an das Zielsystem übertragen.

Damit trotz Remote Credential Guard vom RDP-Ziel aus SSO zu Drittsystemen, etwa Dateiservern, möglich ist, werden entsprechende Kerberos-Anfragen an die RDP-Quelle weitergeleitet.

Bei Nutzung des Restricted Admin Mode erfolgt während der Anmeldung automatisch ein Kontextwechsel. Der zugreifende Benutzer hat dann zwar lokale administrative Rechte auf dem RDP-Ziel, der Zugriff auf Drittressourcen im Netzwerk erfolgt jedoch im Kontext des Active-Directory-Accounts des RDP-Ziels (des Computerkontos).

Microsoft empfiehlt für Szenarien, in denen ein RDP-Ziel bereits kompromittiert sein könnte, den Restricted Admin Mode anstelle des Remote Credential Guard. Denn während die RDP-Verbindung bei Nutzung von Remote Credential Guard besteht, hat der Angreifer die Möglichkeit, neue Sitzungen im Kontext des zugreifenden Benutzers für ein begrenztes Zeitfenster zu starten. Abbildung 4 zeigt noch einmal die wichtigsten Eigenschaften der beiden Sicherheitsfunktionen.

Quelle: Microsoft



Die unterschiedlichen Eigenschaften der beiden Sicherheitsfunktionen sind in verschiedenen Einsatzszenarien nützlich (Abb. 4).

Die Konfiguration der RDP-Absicherung kann über Gruppenrichtlinien umgesetzt werden. Unter „Computer Configuration / Administrative Templates / System / Credentials Delegation" befindet sich die Richtlinie „Restrict delegation of credentials to remote servers". Sie bietet die folgenden drei Einstellungen:

- Restrict Credential Delegation
  - Bevorzugt: Remote Credential Guard
  - Fallback: Restricted Admin Mode
- Require Remote Credential Guard
- Require Restricted Admin Mode

Geschütze Benutzer – mehr Maßnahmen

Eine weitere wichtige Maßnahme zum Schutz der Tier-Adminkonten besteht darin, sie in die Active-Directory-Gruppe „Protected Users" aufzunehmen. Dadurch werden automatisch mehrere Härtungsmaßnahmen für diese hochprivilegierten Benutzer umgesetzt. Vor dem produktiven Einsatz sollte diese Maßnahme jedoch ausführlich getestet werden, da sie Auswirkungen auf die Arbeitsweisen der Administratoren haben kann. Durch das Aufnehmen in die Gruppe werden unterschiedliche Schutzmaßnahmen auf den Windows-Geräten in der Domäne und auf den Domänencontrollern aktiviert.

Auf den Windows-Geräten wird beispielsweise bei aktiviertem Windows Digest das Klartextpasswort nicht mehr zwischengespeichert, selbst wenn das Authentifizierungsprotokoll manuell vom Angreifer aktiviert wurde. Und auch Kerberos cacht das Klartextpasswort nach dem Erhalt des initialen Authentifizierungstokens TGT (Ticket Granting Ticket) nicht mehr.

Beim Domänencontroller wird durch die Aktivierung der Schutzmaßnahmen unter anderem die NTLM-Authentifizierung für Mitglieder der „Protected Users"-Gruppe deaktiviert und ein Erneuern der TGTs nach der initialen Gültigkeitsdauer von vier Stunden ist nicht mehr möglich. (ur@ix.de)

Quellen

[1] Hagen Molzer; Active Directory mit Tiering-Modell schützen; iX 2/2023, S. 120

[2] Die im Text erwähnten Microsoft-Artikel und CIS-Benchmarks sind über ix.de/zw57 zu finden.

HAGEN MOLZER

ist Leitender Berater bei der cirosec GmbH. In seinen Schwerpunktbereichen Active-Directory- und Windows-Betriebssystem-Sicherheit führt er Penetrationstests, Beratungsprojekte sowie Red-Team-Assessments durch.