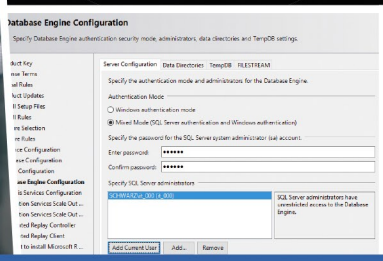
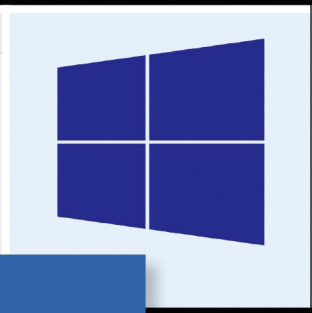
Peter Kloep
Karsten Weigel





Sichere Windows-Infrastrukturen

Das Handbuch für Administratoren

- Von der Planung zu konkreten Maßnahmen
- Kerberos, PKI und CA, Credential Guard und Bitlocker richtig nutzen
- Patching, Auditing, Monitoring und Reporting

Alle Codebeispiele zum Download

Rheinwerk Computing

Kapitel 2
Angriffsmethoden

In diesem Kapitel beschreiben wir einige der bekannten Angriffe auf den Anmelde- und Verzeichnisdienst Active Directory und stellen entsprechende Schutzmechanismen vor. Diese Auflistung erhebt keinen Anspruch auf Vollständigkeit und beschreibt nicht alle möglichen Angriffe, die »in der Welt da draußen« vorhanden sind.

Angriffe auf die IT-Systeme können in unterschiedlichsten Formen erfolgen. Neben dem klassischen Hacker-Angriff über das Internet auf Systeme oder der Phishing-Mail, die versucht, Anmeldeinformationen der Benutzer oder der Administratoren abzugreifen, kann auch das vorsätzliche oder versehentliche Löschen von Daten bzw. Dateien als ein Angriff bewertet werden.

2.1 Geänderte Angriffsziele oder »Identity is the new perimeter« und »Assume the breach«

Im Mittelalter wurden die Tore der Burgen und Stadtmauern wie Schleusen gebaut, sodass die Wachmannschaft jeden Besucher zwischen zwei Toren isolieren konnte, um festzustellen, mit wen man es zu tun hatte und was er in das Innere von Burg oder Stadt transportieren wollte. Diese Strategie wurde auf die IT-Systeme übertragen, indem vor einigen Jahren, als die Vernetzung der Systeme fortschritt und immer mehr Systeme an das Internet angebunden wurden, Firewalls am Übergang zwischen dem internen Netzwerk und dem »bösen« Internet installiert wurden, um diesen Übergang idealerweise in beide Richtungen abzusichern.

Die Erfahrungen der letzten Jahre haben gezeigt, dass sich das Angriffsbild geändert hat. Ziele der Angreifer sind inzwischen häufiger die *Identitätsspeicher* – also die Server bzw. Anwendungen, in denen die *Identitäten* (Konten oder Kennungen) verwaltet werden. Schafft es ein Angreifer, Identitäten zu stehlen, kann er damit auf die Daten (sein eigentliches Ziel) zugreifen.

Der klassische Firewall-Ansatz wird auch durch die Mobilität der Benutzer – und deren Geräte – erschwert. Was nützt eine teure (und hoffentlich gut und sicher konfigurierte) Firewall im Unternehmen, wenn der Benutzer sich über seinen Laptop zu Hause oder mit dem öffentlichen WLAN eines Cafés verbindet und sich damit mögli-

chen Angriffen aussetzt, die von der Firewall des Unternehmens nicht verhindert werden können.

Mit dem Begriff *Identity is the new perimeter* soll verdeutlicht werden, dass die Konten, die verwendet werden, möglichst gut geschützt und überwacht werden. Hierbei helfen z. B. die Einführung eines Tier-Modells (siehe Kapitel 6) und ein entsprechendes Auditing der Anmeldungen (siehe Kapitel 19).

Ein weiteres Schlagwort, das vor einigen Jahren aufkam, ist *Assume the breach*. Ganz frei übersetzt bedeutet das: »Es gibt zwei Arten von Betreibern eines Netzwerks: die einen, die wissen, dass sie kompromittiert sind, und die anderen, die es noch nicht wissen.« Oder anders ausgedrückt: »Gehen Sie davon aus, dass bereits ein Angreifer in Ihrem Netzwerk ist, und verhalten Sie sich entsprechend«.

Die Art und Weise, wie vor einigen Jahren administriert wurde, ist heute nicht mehr zeitgemäß und gefährdet die Sicherheit des Gesamtsystems. Auch heute treffen wir immer wieder Kunden an, bei denen es keine Trennung zwischen normalen Nutzerkonten und administrativen Konten gibt. Wir haben zahlreiche Infrastrukturen gesehen, bei denen der normale Benutzer Mitglied der Gruppe der Domänen-Administratoren war. Dadurch, dass das Domänen-Admin-Konto Zugriff auf Internet und E-Mail hat, war es für einen Angreifer sehr leicht, das gesamte Netzwerk zu übernehmen. Stellen Sie sich einfach vor, solch ein Benutzer surft im Internet und greift auf eine Website zu, auf der sich ein Virus (oder andere Schadsoftware) befindet. Wird diese Schadsoftware auf dem Client ausgeführt, besitzt sie die Rechte eines Domänen-Admins – und damit Rechte auf allen Systemen.

In diesem Fall bleibt nur das Prinzip Hoffnung, dass der Virenscanner auf dem Client die Schadsoftware erkennt und die Ausführung verhindert. Glauben Sie uns: Sie wollen nicht wissen, bei wie vielen Kunden genau das eines der größeren Probleme darstellte. Ganz oft hörten wir dann interessante Statements wie »Wir haben ja eine Firewall« oder »Die Benutzer sollen nicht ins Internet«. Solche Regeln müssen – wenn sie vorhanden sind – auch technisch realisiert werden. Sie sollten sich als Verantwortlicher für einen der Sicherheitsdienste (Firewall, Virenscanner, Identitätsverwaltung) nicht darauf verlassen, dass die Kollegen aus der anderen Abteilung bzw. Zuständigkeit alle Bedrohungen abfangen, sondern für Ihren Bereich alle realisierbaren Schutzmechanismen nutzen.

2.2 Das AIC-Modell

Wenn es um die IT-Sicherheit geht, wird häufig das sogenannte *AIC-Modell* erwähnt. Dieses Modell wird auch als CIA-Modell bezeichnet, was bei vielen Personen aber eine eher unpassende Assoziation hervorruft.

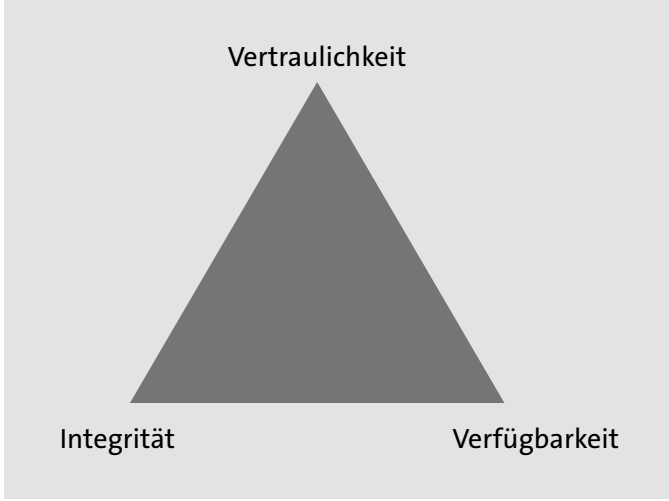


Abbildung 2.1 Die drei Säulen der IT-Sicherheit

Mit dem AIC-Dreieck (siehe Abbildung 2.1) werden die drei Säulen der IT-Sicherheit beschrieben:

- Mit der **Verfügbarkeit** (engl. *Availability*) ist die Erreichbarkeit und Funktion der IT-Systeme gemeint. Die meisten IT-Systeme erfüllen einen Zweck – wie Datenspeicherung und -bereitstellung oder Durchführung von Authentifizierungen. Stehen diese Systeme bzw. Dienste nicht zur Verfügung, hat dies kleinere oder größere Störungen zur Folge.
- Die **Integrität der Daten** (engl. *Integrity*) soll sicherstellen, dass die Daten, die verarbeitet werden, »in Ordnung« und nicht verfälscht worden sind. Hier kommen digitale Signaturen zum Einsatz, die sicherstellen können, dass die Daten vom erwarteten Absender stammen und auf dem Transportweg über das Netzwerk nicht manipuliert worden sind.
- Die **Vertraulichkeit** (engl. *Confidentiality*) beschreibt den Schutzbedarf der Daten und die Methoden, um unberechtigten Personen den Zugriff auf die Daten zu verwehren bzw. um sicherzustellen, dass die Daten nur von berechtigtem Personal gelesen werden können. Hier kommen Datenverschlüsselungen zum Einsatz.

Stellen Sie sich nun diese drei Säulen als einen dreibeinigen Tisch vor. In der Mitte des Tisches liegt eine Kugel, die bedeutet, dass »alles in Ordnung« ist bzw. dass keiner der Mitarbeiter sich beschwert. Wenn Sie nun an einem der höhenverstellbaren Tischbeine schrauben, wird der Tisch aus dem Gleichgewicht geraten und die Kugel von der Mitte wegrollen. Oder anders gesagt: Jede Änderung an den Sicherheitseinstellungen geht zulasten einer der anderen Säulen.

Ein praktisches Beispiel: Sie haben einen Schulungsraum im Unternehmen, in dem sich IT-Geräte befinden. Dieser Raum ist nicht verschlossen. Aus Sicherheitsgründen (zum Schutz der IT-Geräte) bringen Sie nun ein elektronisches Zahlenschloss mit einem Code, den nur berechtigte Personen haben, an der Tür an. Dieser Vorgang wird die Sicherheit für die Geräte im Raum sehr erhöhen (*Confidentiality*). Was passiert nun aber, wenn Sie morgens in den Schulungsraum möchten und die Batterie des Zahlenschlosses leer ist oder Sie die Kombination vergessen haben? Eine erhöhte Sicherheit kann also sehr leicht zulasten der Verfügbarkeit gehen. Hier müssen Sie dann eventuell wieder zusätzliche Gegenmaßnahmen ergreifen, damit die »Kugel wieder in der Mitte des Tisches landet«. IT-Sicherheit ist »unbequem« und bedeutet in der Regel einen erhöhten Aufwand.

Meist werden bei den Überlegungen zur IT-Sicherheit Kompromisse gemacht werden müssen. Es gibt einmal den aktuellen Sicherheitsstand (zumeist ein schlechter Zustand) und Empfehlungen der Hersteller der Systeme (zumeist ein sehr sicherer Standard). Häufig kann dieser sichere Standard aber nicht einfach so übernommen werden, da es Abhängigkeiten gibt, die diesen Standard vielleicht nicht ermöglichen. Hier sollten Sie kritisch prüfen und einen Kompromiss finden, der sowohl die Funktion der Systeme sicherstellt als auch die Sicherheitsanforderungen erfüllt.

2.3 Angriff und Verteidigung

In diesem Abschnitt möchten wir einige mögliche Angriffsmethoden beschreiben, mit denen Sie vielleicht konfrontiert werden. Wir erwähnen aber auch Methoden, wie Sie sich gegen diese Attacken wehren können. Teilweise wird es jedoch ein Kampf gegen Windmühlen sein.

2.3.1 Phishing-Attacken

Eine Phishing-Attacke ist nach wie vor die am meisten verwendete Angriffsmethode. Der Grund dafür liegt auf der Hand: Der Aufwand (Kosten und Zeit), den ein Angreifer für einen solchen Angriff investieren muss, ist sehr gering. Es gibt zahlreiche Quellen, bei denen riesige Mengen an E-Mail-Adressen gekauft werden können. Diese werden dann mit Phishing-Mails attackiert.

Eine Phishing-Mail ist eine E-Mail-Nachricht, die den Empfänger (das Opfer) dazu verleiten soll, auf einen falschen Internet-Link zu klicken, oder die den Benutzer dazu auffordert, Anmeldedaten zu übermitteln oder einzugeben. In den Anfangsjahren waren diese Nachrichten durch schlechte sprachliche Qualität – besonders bei deutschen Phishing-Mails – sehr leicht zu erkennen und als Fälschung zu identifizieren. Mittlerweile sind die meisten Phishing-Mails deutlich besser geschrieben und erhalten kaum noch bzw. keine orthografischen Fehler und verwenden oft die richtigen Farben und Firmenlogos.

Banken und andere Institutionen werden Sie vermutlich niemals dazu auffordern, Ihre Anmeldedaten zu überprüfen oder zu übermitteln. Zusätzlich sollten Sie bei sensiblen Seiten niemals die Links aus E-Mails verwenden, bevor Sie diese geprüft haben. Nutzen Sie stattdessen die gespeicherte Adresse in der Favoritenliste oder geben Sie die gewünschte URL (*Uniform Resource Locator*) direkt in die Adressleiste des Browsers ein und nicht in das Suchfenster der Suchmaschine.

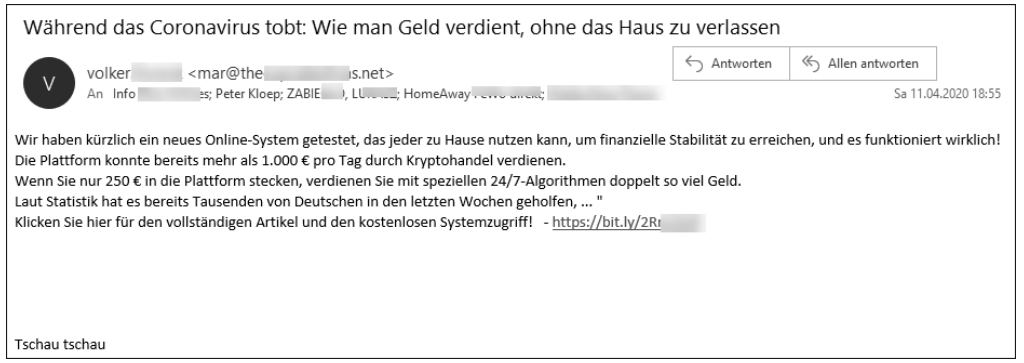


Abbildung 2.2 Beispiel für eine generische Phishing-Mail, die Geld verspricht

Häufig sind Phishing-Mail brandaktuell. So spielt die Mail aus Abbildung 2.2 auf die Corona-Pandemie an und verspricht, schnell und einfach Geld zu verdienen. Verdächtig bei dieser Mail ist der Absendername (volker) hinter dem aber eine völlig falsche E-Mail-Adresse steht. Zusätzlich stehen mehrere (dem Adressaten unbekannte) Empfänger in der An-Zeile. Weitere verdächtige Merkmale sind das Fehlen einer Anrede und der Link am Ende, der auf *bit.ly* verweist (es könnte auch ein anderer Dienst sein, der verkürzte URLs anbietet). Hinter dem Link könnte sich entweder eine gefälschte Webseite verbergen, die Anmeldeinformationen (z. B. für Online-Dienste) abfangen will, oder eine präparierte Webseite, auf der Schadsoftware aktiv ist, die dann den Computer des Aufrufers infizieren und möglicherweise übernehmen will.

Es gibt diverse Indizien, die darauf hinweisen, dass es sich bei einer E-Mail um eine Phishing-Mail oder eine gefälschte Mail handelt. Auch in Abbildung 2.3 können Sie einige der Merkmale erkennen:

- Es wird versucht, Zeitdruck zu erzeugen, sodass der Empfänger dazu verleitet wird, sofort tätig zu werden, und nicht intensiv prüft, ob es sich um eine valide Nachricht handelt. So steht in dieser Mail: »Zahlungsverzug (Bitte pruefen Sie dies heute)«.
- Der Anzeigename des Absenders (Vanessa) stimmt nicht mit der Absende-Mailadresse überein (*raups_hans...@web.de*).

- In der Nachricht geht es nicht um einen möglichen Zahlungsverzug. Der reißerische Betreff soll Sie nur dazu bringen, die Mail zu lesen.
- Der Absender der Mail hat eine *web.de*-Adresse, aber wenn Sie mit der Maus über den hinterlegten Link gehen, wird die Adresse, die verlinkt ist, angezeigt. Dieser Link zeigt auf eine russische Webseite.

Abbildung 2.3 Weiteres Beispiel für eine Phishing-Mail

Ein großer Teil der Phishing-Mail beziehen sich auf Banken oder andere Zahlungsdienstanbieter. Dabei versuchen die Angreifer das Opfer dazu zu bringen, relevante Bankdaten wie Zugangsdaten, Kontodaten oder Kreditkarten preiszugeben. Die Angreifer wollen entweder die erbeuteten Daten weiterverkaufen oder selbst die Daten nutzen, um an Geld zu gelangen oder Waren im Internet zu bestellen. »Interessant« sind diese Mails besonders dann, wenn Sie gar nicht Kunde der Bank sind, aber aufgefordert werden, Ihre Daten zu verifizieren.

Auch in der Mail aus Abbildung 2.4 sind wieder einige Merkmale vorhanden, die erkennen lassen, dass es sich nicht um eine legitime Mail einer Sparkasse handelt:

- Die Absende-Mailadresse ist *@online.de*. Sparkassen oder andere Bankinstitute verwenden eigene E-Mail-Domänen als Absender.
- Der Link zum Aktualisieren verweist auf eine Adresse auf einem Webserver in Indien.

Die Webseiten, die hinter diesen Links stecken, können z. B. wie in Abbildung 2.5 aussehen. Häufig sind es auch Webseiten, die den Originalwebseiten täuschend echt nachgeahmt sind.

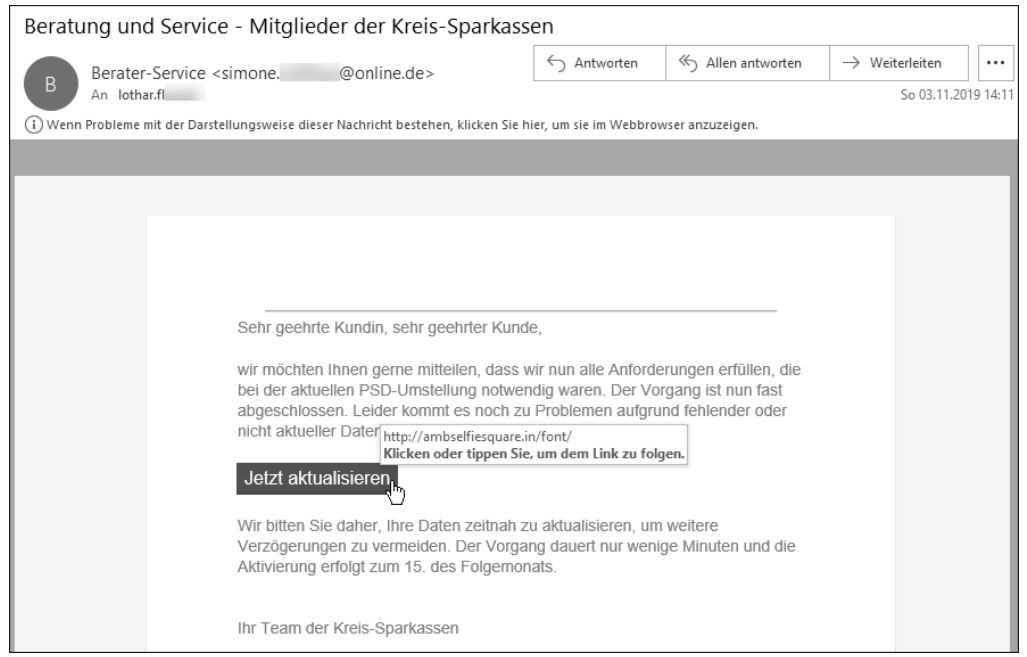


Abbildung 2.4 Beispiel für eine Bank-Phishing-Mail

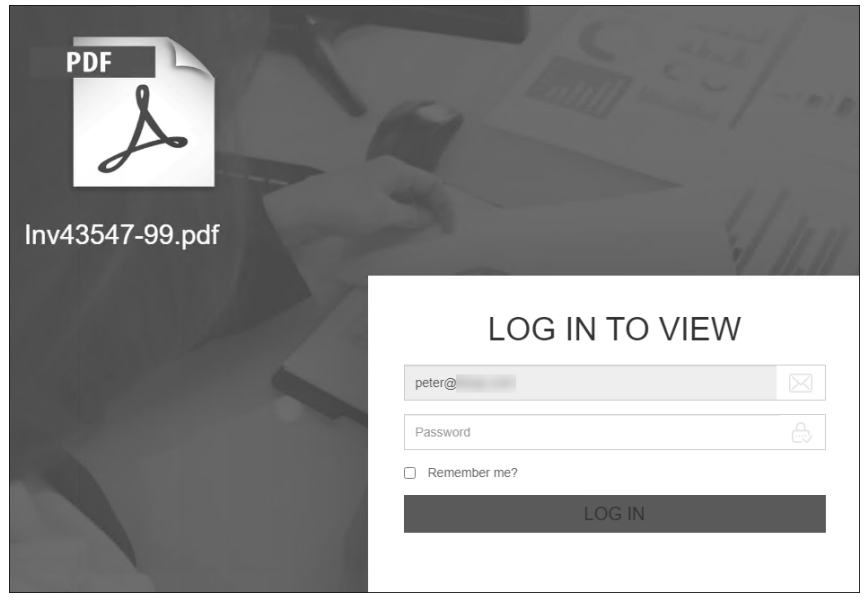


Abbildung 2.5 Webseite, die Sie auffordert, Anmeldedaten einzugeben

Neben den E-Mails, die über Links das Opfer in die Falle tappen lassen, werden auch öfter Mails versendet, die den Schadcode bereits mitbringen. Dieser wird häufig in

ausführbarem Code (z. B. in Skripten) versteckt, und die Icons der Dateien werden entsprechend gefälscht. In solchen Nachrichten werden oft sehr hohe Geldbeträge angegeben, um den Druck zu erhöhen, den Anhang zu öffnen.

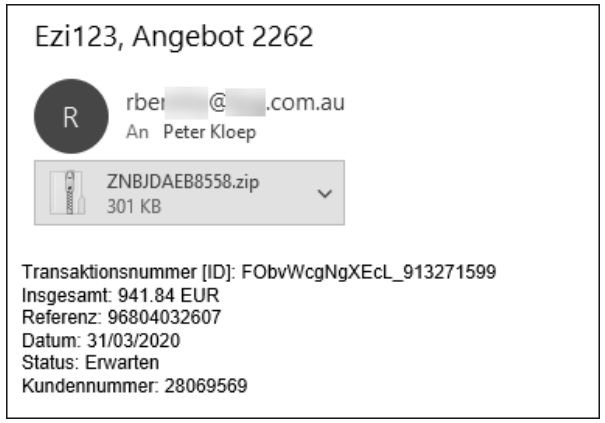


Abbildung 2.6 E-Mail mit gefährlichem Anhang

Wenn Sie diesen Mail-Anhang öffnen und ausführen, kann es sein, dass entweder der Schadcode direkt enthalten ist oder dass eine kleine Routine auf präparierte Webseiten geht und von dort zusätzliche Schädlinge nachlädt und installiert.

Zum Schutz vor Phishing-Mails sollten Sie zuallererst Ihre Anwender schulen und sensibilisieren, sodass die Anwender nicht alle Mails mit dubiosen Absendern oder Anhängen öffnen. Zusätzlich sollten Sie sicherstellen, dass Ihre Antivirenlösung aktiv ist und eventuell enthaltene Schadsoftware erkennt. Ein Filter auf Ihrem Mail-Server kann dabei helfen, Phishing-Mails und Spam-Mails herauszufiltern und von den Anwendern fernzuhalten.

Spam-Mails sind im Gegensatz zu Phishing-Mails harmloser. Spam-Mails dienen dazu, entweder das Postfach oder den Mailserver zu fluten oder Sie dazu zu verleiten, auf Webseiten zu gehen, auf denen dann durch Werbeeinnahmen Geld für den Angreifer generiert wird. Ein wirksamer Schutz, um Schaden durch solche Angriffe zu reduzieren, ist die Verwendung einer Mulitfaktor-Authentifizierung, bei der der Benutzer durch ein weiteres Gerät – Smartphone-App, Schlüsselgenerator oder Telefonanruf des Anbieters verbunden mit der Eingabe eines zusätzlichen PINs – die Anmeldung bestätigen muss. Selbst wenn der Benutzer auf die Spam-Mail hineinfällt und die Anmeldeinformationen gegenüber dem Angreifer preis gibt, kann der Angreifer mit den erbeuteten Informationen keinen Zugriff auf die Ressourcen erlangen, da für eine erfolgreiche Authentifizierung – und damit eine Ausnutzung der Anmeldeinformationen – weitere Faktoren in Form einer zusätzlichen Authentifizierung benötigt werden. Diese können in Form einer Smartphone-App oder eines Einmal-Codes vorliegen.

2.3.2 Ransomware

In den letzten Jahren gab es immer wieder Wellen von Angriffen mit sogenannter Ransomware. Das Ziel dieser Angriffe war es, die Daten auf den Systemen der Opfer zu verschlüsseln und damit Geld zu erpressen. Ob die Daten nach der Zahlung entschlüsselt werden können, bleibt jedoch fraglich. Die Zahlung des Geldes erfolgt meist in Bitcoin.

Der Angreifer versucht zusätzlichen Druck aufzubauen, indem sich der zu zahlende Preis im Laufe der Zeit erhöht. Das große Dilemma bei Ransomware (siehe Abbildung 2.7) wie z. B. *WannaCry* besteht darin, dass dies im Kontext des Benutzers erfolgt und potenziell alle Dateien gefährdet sind, auf die der Benutzer Zugriff besitzt. Das Ausführen im Kontext des Benutzers bedeutet, dass die Schadsoftware durch den Benutzer ausgeführt wird und die Rechte verwendet, die er besitzt. Es muss nicht erst auf dem Computer eine Schwachstelle gefunden und ausgenutzt werden, um die Schadsoftware zu starten und den Schaden zu verursachen. Neben dem Zugriff auf lokale gespeicherte Dateien haben Benutzer in aller Regel auch Zugriff auf Daten, die auf Dateiservern im Netzwerk gespeichert sind. Diese Dateien sind ebenso gefährdet wie die lokalen Dateien auf dem Computer des Benutzers.

Abbildung 2.7 Benachrichtigung einer Ransomware, dass die Dateien auf dem System verschlüsselt worden sind

Wenn sich ein Benutzer eine Ransomware auf den Rechner herunterlädt und ausführt, werden alle Dateien (lokal und über das Netzwerk) verschlüsselt, auf die der Benutzer Zugriff hat. Die bekanntesten Ransomware-Angriffe der vergangenen Jahre waren *WannaCry*, *Petya* und *NotPetya*. Es gibt aber zahlreiche andere Versionen, die den gleichen Schaden anrichten können.

Aktuelle Virenscanner finden die bekannten Verschlüsselungstrojaner. Sollten jedoch neuere Versionen erscheinen oder bekannte Versionen so modifiziert werden, dass sie vom Virenscanner nicht mehr erkannt werden, besteht das Risiko, dass der Verschlüsselungstrojaner ausgeführt wird und ein sehr großer Schaden entstehen kann.

Als Schutz dient – neben dem Virenscanner – eine regelmäßig durchgeführte und getestete Datensicherung. Die Datensicherung sollte auf einem Laufwerk oder Medium gespeichert sein, auf das die Benutzer (und Admins) nicht so einfach zugreifen können. Stellen Sie sich nur einmal vor, ein Administrator führt eine Ransomware aus.

Zusätzlich können Sie für den Benutzern das Ausführen von nicht erwünschten Dateien verbieten. Dazu können Sie entweder Richtlinien für die Softwareeinschränkung oder AppLocker (siehe Abschnitt 11.5.5) verwenden, um das Ausführen von Anwendungen aus nicht erlaubten Quellen zu verhindern (siehe Abbildung 2.8).

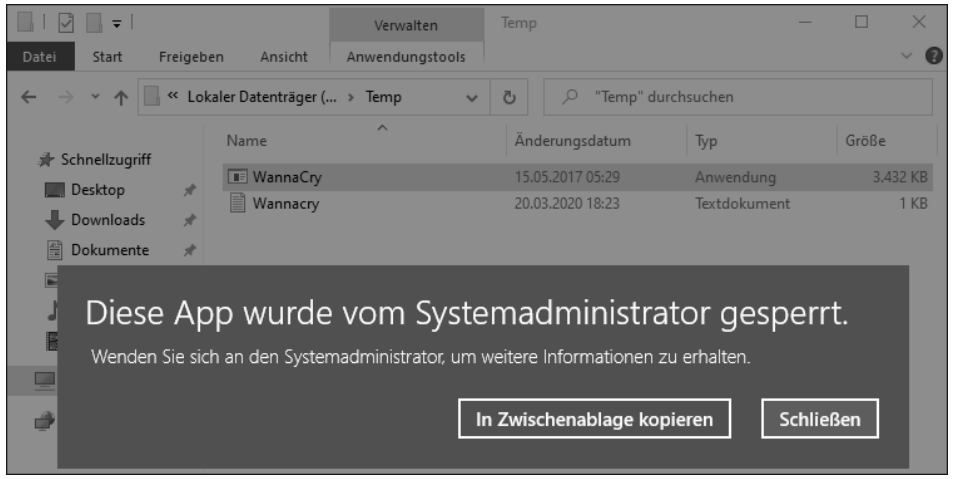


Abbildung 2.8 Richtlinien für die Softwareeinschränkungen haben das Ausführen von WannaCry verhindert.

Sie können sich also mit vorhandenen Schutzmechanismen einfach vor den meisten Verschlüsselungstrojaner schützen. Speicherhersteller wie NetApp bieten ebenfalls Schutzmechanismen an, die erkennen – und verhindern –, wenn eine große Anzahl von Dateien gleichzeitig geändert (verschlüsselt) werden soll. Microsoft bietet diese Art von Schutz auch für Daten an, die auf OneDrive-Ordnern in der Cloud gespeichert werden.

2.3.3 Kennwörter

Kennwörter waren schon immer eine der einfachsten Methoden für Angreifer, Zugang zu Systemen zu erhalten. Je einfacher oder kürzer ein Kennwort ist, desto leichter ist es, das Kennwort zu erraten oder aber ein Kennwort zu erraten, das den gleichen Hashwert besitzt wie das eigentliche Kennwort.

Die meisten Systeme verwenden Hashwerte, um die Anmeldeinformationen zu prüfen. Dabei wird aus dem eingegebenen Kennwort eine Prüfsumme (*Hashwert*) gebildet und dieser dann übertragen. Die Generierung der Hashwerte erfolgt über sogenannte Falltür-Alogrithmen, die sicherstellen, dass aus dem Hashwert das Kennwort nicht zurückberechnet werden kann.

Da die Anzahl der zur Verfügung stehenden unterschiedlichen Hashwerte endlich ist (z. B. bei SHA256 sind es 2^{256} unterschiedliche Hashwerte), aber die Anzahl der möglichen Kennwörter unendlich ist, müssen mindestens zwei unterschiedliche Kennwörter existieren, die den gleichen Hashwert ergeben.

Dieser Umstand wird als *Kollision* bezeichnet. Ein Angreifer muss also nicht das tatsächliche Kennwort erraten, sondern nur ein Kennwort finden, das den gleichen Hashwert ergibt. Es gibt mittlerweile fertige Listen mit Hashwerten, die z. B. das »Erraten« von Kennwörtern mit bis zu acht Zeichen in sehr geringer Zeit ermöglichen. Diese Listen werden als *Rainbow-Tables* bezeichnet. Alle gängigen Kennwort-Tools bieten die Möglichkeit, diese Tabellen zu verwenden.

Sollte das Kennwort mit einer Rainbow-Table nicht herausgefunden werden können, bleibt eventuell nur eine *Brute-Force-Attacke*. Dabei wird jede mögliche Kombination von Zeichen ausprobiert. Abhängig von der Länge des Passworts und der zur Verfügung stehenden Rechenleistung des Angreifers kann eine Brute-Force-Attacke sehr lange dauern.

Je nachdem, gegen welches System der Angreifer den Angriff laufen lässt, ist eine Rainbow-Attacke oder eine Brute-Force-Attacke eine sehr »laute« Aktion, die auf den Zielsystemen sehr viele Fehler protokollieren wird. Nutzt der Angreifer eine Offline-Methode für den Angriff (z. B. mit einer Datensicherung), ist es jedoch sehr schwer bzw. unmöglich, diesen Angriff zu erkennen.

Es gibt immer mehr Bestrebungen der Softwarehersteller, auf ein System ohne Kennwörter umzustellen. Die Benutzer sollen dann andere Formen der Authentifizierung (Multi-Faktor, Biometrie) verwenden, um die Schwäche einer reinen Kennwortanmeldung zu beheben.

2.3.4 Angriffe auf das Netzwerk

Eine andere Möglichkeit, um Ihre Systeme anzugreifen, ist das Netzwerk als solches. Ihre Computer kommunizieren untereinander und mit Serversystemen in aller Regel über Netzwerkverbindungen, die meist kabelgebunden sind oder Wireless LAN

(WLAN) nutzen. Bei den LAN-Verbindungen (LAN, *Local Area Network*) sind die Kabel meist in Kabelkanälen verlegt. Weitere Kabel liegen häufig in abgehangenen Decken, sodass Mitarbeiter und Besucher die Kabel nicht sehen. Dies ist zwar ein Vorteil, da alles »aufgeräumt« aussieht, birgt aber das Risiko, dass jemand Manipulationen an den Kabeln vornehmen kann, ohne dass dies sofort auffällt.

Es gibt einige Angriffsmethoden, die im lokalen Netzwerk durchgeführt werden können. Neben dem Mitschneiden von Informationen mithilfe von Netzwerkscannern oder -sniffern wie *Wireshark* oder dem *Message Analyzer* können Daten, die über das Netzwerk übertragen werden, mitgelesen werden. Sogar Dateien, die übertragen werden, können aus den einzelnen Paketen wieder zusammengesetzt werden, sofern der Datenverkehr nicht verschlüsselt wird. Es besteht also das Risiko, dass Daten von Unbefugten abgerufen werden können. Sie sollten den Zugang zum Netzwerk so absichern, dass nur bekannte und befugte Geräte angeschlossen werden können (siehe Abschnitt 16.5).

Ein weiteres Risiko besteht im Einsatz von teilweise sehr alten Netzwerkprotokollen, die von Haus aus nicht sicher sind. Zu diesen Protokollen gehört unter anderem das ARP-Protokoll (ARP, *Adress Resolution Protocol*). Das ARP-Protokoll ist im lokalen Subnetz dafür zuständig, dass die IP-Adresse des Computers in die MAC-Adresse (MAC, *Media Access Control*) übersetzt wird.

In Netzwerken, die auf IPv4 basieren, findet die Kommunikation im lokalen Subnetz auf Grundlage der MAC-Adressen statt. Dazu schickt der Absender der Daten einen Broadcast an alle angeschlossenen Systeme im Subnetz, und zwar in Form eines Broadcast-Pakets. In diesem Paket fragt der Sender nach der MAC-Adresse, die zu der Netzwerkkarte bzw. dem Computersystem gehört, mit dem der Sender kommunizieren möchte. Der Besitzer der MAC-Adresse wird dem fragenden System antworten, und der Absender wird die IP-Adresse und die zugehörige MAC-Adresse im ARP-Cache speichern. Diesen Cache können Sie sich auf einem Windows-System mit dem Befehl `arp -a` anzeigen lassen:

```
C:\>arp -a

Schnittstelle: 192.168.1.71 --- 0x6
  Internetadresse       Physische Adresse     Typ
  192.168.1.1           38-10-d5-b7-3c-1d     dynamisch
  192.168.1.2           02-11-32-2b-5b-fe     dynamisch
  192.168.1.5           00-11-32-94-04-89     dynamisch
  192.168.1.24          98-ee-cb-19-d5-5b     dynamisch
  192.168.1.86          60-6d-3c-22-c2-b9     dynamisch
  192.168.1.100         30-cd-a7-ee-80-b5     dynamisch
  192.168.1.255         ff-ff-ff-ff-ff-ff     statisch
  224.0.0.22            01-00-5e-00-00-16     statisch
```



```
  224.0.0.251           01-00-5e-00-00-fb     statisch
  224.0.0.252           01-00-5e-00-00-fc     statisch
  239.255.255.250       01-00-5e-7f-ff-fa     statisch
  255.255.255.255       ff-ff-ff-ff-ff-ff     statisch
```

Listing 2.1 Ausgabe der gespeicherten MAC-Adressen

Listing 2.1 zeigt die auf dem System gecachten MAC- und IP-Adressen. Sobald ein Computer Kontakt zu einem anderen System im gleichen Subnetz aufbaut, wird diese Tabelle aufgebaut. Die Broadcast-Abfragen zum Aufbau der Tabelle sind in keiner Art und Weise geschützt.

Stellen Sie sich einmal vor, ein Computersystem im Subnetz schickt Ihnen folgende Information: »Übrigens, wenn du mal mit dem Router reden willst, hier ist die MAC-Adresse.« Die MAC-Adresse, die mitübermittelt wird – übrigens ohne, dass das Opfer angefragt hat – ist die MAC-Adresse eines Computers, von dem der Angriff ausgeführt wird. Ein zweites Paket wird an den Router gesendet mit dieser Information: »Übrigens, wenn du mit dem Opfer reden willst, hier ist die MAC-Adresse.« Auch hier wird die MAC-Adresse des Angreifer-PCs verwendet.

Die beiden Systeme speichern diese (gleiche) MAC-Adresse in ihrem Cache, und ab sofort werden jedes Mal, wenn diese beiden Systeme miteinander reden wollen, die Datenpakete an den Angreifer gesendet, der die Pakete dann inspizieren kann und anschließend weiterleitet. Diese Art von Angriff wird als *Man-in-the-Middle-Angriff* bezeichnet. Ein Tool, mit dem dies sehr leicht durchgeführt werden kann, ist *Ettercap*. Ettercap gibt es als separaten Download und es ist auch Teil der *Kali*-Distribution (siehe Abschnitt 3.9).

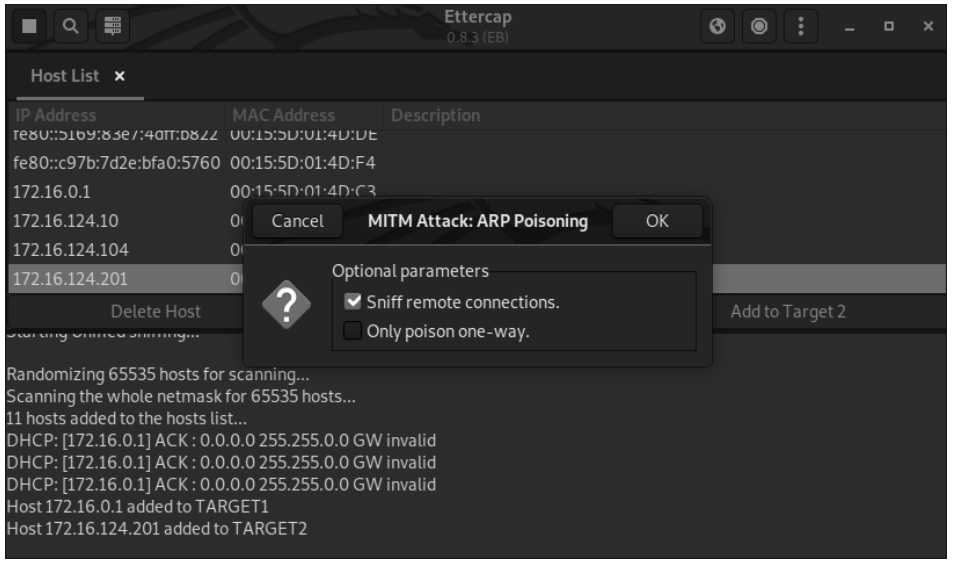


Abbildung 2.9 ARP-Poisioning-Angriff mit Ettercap

Bei Ettercap (siehe Abbildung 2.9) werden die beiden Ziele (*Targets*) ausgewählt und dann wird die MITM-(Man-in-the-Middle-)Attacke gestartet.

Ein MITM-Angriff wäre auch zwischen dem DNS-Server und dem Router sehr effektiv, um die DNS-Antworten zu manipulieren, die an die Clients gesendet werden. So könnte man die Benutzer auf gefälschte oder manipulierte Systeme umleiten und dort z. B. Anmeldeinformationen abgreifen.

Die Protokolle ARP und DNS sind sehr alt und bieten in ihren ursprünglichen Versionen keinerlei Sicherheit. Der effektivste Schutz gegen ARP-Angriffe ist die Definition der kritischen Kern-Komponenten wie der Router und die Verwendung eines IDS (*Intrusion Detection Systems*), das erkennt, wenn ein sogenanntes *ARP-Announcement* (eine ARP-Ankündigung) gesendet wird, obwohl niemand danach gefragt hat.

Zum Absichern von DNS-Informationen können Sie – zumindest für interne Ressourcen – das Protokoll *DNSSec* (DNS-Security) verwenden, bei dem die Anfragen digital signiert werden und somit sichergestellt werden kann, dass die DNS-Informationen von einem vertrauenswürdigen DNS-Server stammen.

2.3.5 Pass the Hash und Pass the Ticket

Bei einem *Pass-the-Hash-Angriff* erbeuten die Angreifer unverschlüsselte Anmeldeinformationen in Form von Hashwerten und verwenden diese, um sich anschließend als derjenige zu authentifizieren, von dem sie die Daten gestohlen haben. Diese Art von Angriff hat in den letzten Jahren rapide zugenommen, da zum einen die Werkzeuge, um solche Angriffe durchzuführen, zugänglich wurden (*Windows Credential Editor*, *Mimikatz*) und zum anderen sehr viele Administratoren (immer) noch keine Schutzmechanismen gegen diese Art von Angriff installiert haben.

Neben dem Einsatz eines Tier-Modells (siehe Kapitel 6) und der Verwendung der Schutzmechanismen von Windows 10 (z. B. Credential Guard, siehe Abschnitt 12.7) können Sie sich einfach und effektiv gegen diese Art von Angriff schützen: Bei diesem Angriff kann der Angreifer – sofern er Anmeldeinformationen eines Domänen-Administrators erbeuten kann oder einen Domänencontroller kompromittieren hat – ein Kerberos-Ticket erstellen, das 10 Jahre gültig ist (siehe Kapitel 4). Bei einigen der verfügbaren Schutzmechanismen, die im Betriebssystem bereitgestellt werden, müssen Sie prüfen, in welchen Editionen die Funktionen verwendbar sind. Einige der Features sind – wie z. B. Credential Guard – nur in der Enterprise-Edition von Windows 10 verfügbar.

Microsoft hat ein Whitepaper veröffentlicht, das eine Vielzahl von weiteren Information bereithält. Sie finden es unter:

https://www.microsoft.com/en-us/download/confirmation.aspx?id=36036

Sie sollten nach Möglichkeit keine Authentifizierungs- bzw. Zugriffsmethoden verwenden, die am Ziel wiederverwertbare Anmeldeinformationen (*Reusable Credentials*) hinterlassen. So sind z. B. eine lokale Anmeldung und das Verbinden eines Netzlaufwerkes Methoden, die ohne Credential Guard wiederverwendbare Anmeldemethoden hinterlassen, die ein Angreifer verwenden kann, wenn er sie erbeutet. Die Verwendung der Remote-PowerShell oder der Zugriff mithilfe von Verwaltungskonsolen hinterlässt keine dieser Anmeldeinformationen am Ziel.

Bei einem *Pass-the-Ticket-Angriff* kompromittiert der Angreifer einen Server, auf den die Anwender zugreifen und bei dem sich die Benutzer authentifizieren. Dies kann ein Anwendungsserver wie etwa ein SharePoint-Server oder ein Webserver sein. Der Angreifer fängt die Anmeldeinformationen der Anwender ab und versucht, mit diesen Informationen auf andere Ressourcen zuzugreifen.

2.3.6 Angriffe auf Cloud-Dienste

Cloudbasierte Dienste sind auf dem Vormarsch, und immer mehr Kunden »gehen in die Cloud«. Eine Herausforderung an die Sicherheit ist die ständige Online-Verfügbarkeit der Cloud-Systeme. Dadurch können Angreifer diese Systeme Tag und Nacht attackieren. Cloud-Anbieter schützen den Zugriff auf die Systeme mithilfe von *Blacklists* (IP-Adressen von Computern, die zu kontrollierten Botnetzen gehören) und blockieren den Zugriff von Systemen, die zu dieser Liste gehören. Alternativ muss – wenn eine Anmeldung von unbekannten Systemen erfolgt oder wenn von anderen geografischen Standorten aus zugegriffen wird – eine zusätzliche Art und Weise der Authentifizierung verwendet werden.

Die Cloud-Dienste müssen aber auch von irgendwo administriert und eingerichtet werden. Hier kann ein mögliches Sicherheitsproblem entstehen. Sie sollten sicherstellen, dass der Computer, von dem aus Sie Ihre Cloud-Dienste verwalten und einrichten, die höchsten Sicherheitsanforderungen erfüllt und entsprechend als gehärtete PAW (*Privilege Admin Workstation*) installiert und betrieben wird (siehe Kapitel 10).

Bei allen möglichen Zugriffen, die auf Kennwörtern basieren, sind *Keylogger* ein mögliches Risiko. Diese Geräte gibt es in unterschiedlichen Bauformen und sie können so verbaut und verwendet werden, dass sie nicht leicht zu erkennen sind. Ein Keylogger kann meist sehr große Datenmengen in Form von Tastatureingaben speichern. Dadurch kann ein Angreifer sehr leicht Zugangsdaten und Kennwörter erbeuten. Hier sollte eine Multi-Faktor-Authentifizierung verwendet werden, um das Risiko zu reduzieren.

Bedenken Sie aber bitte, dass eine Mutli-Faktor-Authentifizierung nicht das Allheilmittel ist: Stellen Sie sich einmal vor, Ihr Computer, mit dem Sie Ihren Cloud-Zugang administrieren, wird kompromittiert und ein Angreifer kann sich dort einnisten. Nun melden Sie sich bei Ihrem Cloud-Anbieter an und verwenden eine Multi-Faktor-

Authentifizierung. Danach ist die Verbindung zwischen Ihrem Computer und dem Cloud-Anbieter »offen« und kann verwendet werden. Damit kann auch ein möglicher Angreifer auf Ihrem System die Verbindung über bekannte Routinen (PowerShell oder andere Schnittstellen) unbemerkt verwenden.

Grundsätzlich ist die Multi-Faktor-Authentifizierung in Verbindung mit einer gehärteten Arbeitsstation (siehe Kapitel 6) aber ein guter Schutz. Eine Multi-Faktor-Authentifizierung verhindert, dass der Angreifer eine erneute unbemerkte Authentifizierung von einem fremden Rechner ausführen kann.

2.4 Offline-Angriffe auf das Active Directory

In den meisten Netzwerken ist das Active Directory nach wie vor der zentrale Anmelde- und Verzeichnisdienst, in dem die Benutzerkonten und die administrativen Konten erstellt und verwaltet werden. Die Daten eines Domänencontrollers sollten besonders geschützt werden. Der Zugriff auf diese Systeme mit administrativen Rechten sollte auf ein Minimum begrenzt werden und die Zugriffe müssen überprüft und protokolliert werden.

Eine Verschlüsselung der Datenträger der Domänencontrollers (z. B. mit *BitLocker*) verhindert bzw. erschwert einen möglichen Datenabfluss durch unbefugten Zugriff auf die physischen Domänencontroller oder das Kopieren einer virtuellen Festplatte eines Domänencontrollers durch einen Virtualisierungsadministrator.

Genauso sensibel sind eventuell vorhandene IFM-Datenträger (*Install From Media*) und Datensicherungen, die die relevanten Anmeldeinformationen (Hashwerte) enthalten.

2.5 Das Ausnutzen sonstiger Schwachstellen

Neben den unsicheren Verwendungsmethoden der Systeme gibt es noch zusätzliche Rahmenbedingungen, die Sie beachten sollten. Verwenden Sie auf Ihren Systemen nach Möglichkeit immer die aktuellen Protokolle, und schalten Sie alte und unsichere Protokolle ab und entfernen Sie diese auch.

So gibt es z. B. im SMB-1.0-Protokoll bekannte Probleme und Sicherheitslücken. Besonders bei Systemen, die schon länger in Betrieb sind, ist es nicht unüblich, dass alte Netzwerkprotokolle aktiviert sind, jedoch niemand sagen kann, ob diese alten Protokolle verwendet werden oder notwendig sind. Hier sollten Sie regelmäßig die Sicherheitsrichtlinien (siehe Abschnitt 11.4.6) der Hersteller prüfen und die Empfehlungen umsetzen, um einen möglichst hohen Sicherheitsstandard der Systeme zu gewährleisten. Dies gilt besonders für die Ziele, die sich für einen Angreifer wirklich lohnen.

Nach Möglichkeit sollten Sie auf den kritischen Systemen (Tier-0) auf den Einsatz von Agenten oder Drittanbietersoftware verzichten. Sollte dies doch notwendig sein, müssen Sie sicherstellen, dass auch diese Pakete regelmäßig auf Schwachstellen geprüft werden und dass die Pakete regelmäßig aktualisiert werden. Hier kann es hilfreich sein, ein *Application Lifecycle Management* (Anwendungs-Lebenszyklus-Verwaltung, siehe Kapitel 13) zu etablieren, mit dem Sie eine Übersicht der verwendeten Software-Versionen auf Ihren Systemen erstellen. So können Sie leicht feststellen, welche Systeme Anwendungen ausführen, die bekannte Schwachstellen haben, oder ob Sie Systeme einsetzen, die vom Hersteller nicht mehr mit Sicherheitsupdates versorgt werden.

Kapitel 4
Authentifizierungsprotokolle

In diesem Kapitel erhalten Sie einen kurzen Überblick über LM, NTLM, Kerberos, SPNs und die Kerberos-Delegierung. Zusätzlich geben wir Empfehlungen, welche Protokolle Sie nach Möglichkeit nicht mehr einsetzen sollten.

Wenn wir mit Kunden über Authentifizierungsprotokolle sprechen, stellen wir häufig fest, dass viele sich nie intensiver mit den Protokollen beschäftigt haben und ganz oft der Meinung sind, dass diese Beschäftigung Zeitverschwendung sei: »Wieso soll ich darum kümmern, die Anmeldung funktioniert doch?«

Die Verwendung sicherer Authentifizierungsmethoden ist aber ein Schlüssel für die Sicherheit der IT-Infrastruktur und der Anmeldeinformationen. Widmen Sie ihnen also die Aufmerksamkeit, die ihnen zusteht.[1] Bevor wir jedoch mit den einzelnen Protokollen beginnen, definieren wir folgende drei Begriffe:

- *Identifikation*: »Ich bin der Peter«. Der Client »behauptet«, ein bestimmter Benutzer zu sein
- *Authentifizierung*: »Ich bin der Peter und ich kann's beweisen«. Der Client beweist, dass er der Benutzer ist – zum Beispiel durch Eingabe eines Kennwortes.
- *Autorisierung*: Die Autorisierung wird durch eine andere Instanz durchgeführt, die die Authentifizierungsinformationen geprüft hat und dem Client die entsprechenden Rechte gewährt.

Im folgenden Abschnitt schauen wir uns die Authentifizierungsprotokolle an.

4.1 Domänenauthentifizierungsprotokolle

Für die Authentifizierung eines Benutzers oder eines Computers an einer Ressource, die zu einer Domäne gehört, stehen unterschiedliche Protokolle zur Verfügung. Um Abwärtskompatibilität zu gewährleisten, sind unter Umständen noch alte Protokolle wie LanManager aktiv und können von Clients oder Applikationen verwendet wer-

1 Dieses Kapitel ist die aktualisierte und leicht erweiterte Fassung des entsprechenden Kapitels aus: Kloep et al: »Windows Server 2019. Das umfassende Handbuch«. Erschienen im Rheinwerk Verlag unter der ISBN 978-3-8362-6657-4.

den. Dadurch können Sicherheitsrisiken entstehen, da viele der alten Protokolle als unsicher angesehen werden müssen.

Aktualisierung der Domänencontroller

Falls Sie mithilfe von Gruppenrichtlinien Anpassungen an den zu verwendenden Authentifizierungsprotokollen vornehmen, werden diese Richtlinien nicht angepasst oder aktualisiert, wenn Sie die Betriebssysteme der Domänencontroller aktualisieren.

Daher empfehlen wir, bei einem Betriebssystemwechsel die bestehenden Gruppenrichtlinien auf Überbleibsel aus früheren Betriebssystemversionen zu prüfen und sie gegebenenfalls zu bereinigen.

In diesem Kapitel legen wir den Schwerpunkt auf das Authentifizierungsprotokoll Kerberos, da es das Protokoll ist, das heute verwendet werden sollte.

4.1.1 LanManager (LM)

Das Authentifizierungsprotokoll LM (LanManager oder LANMAN) wurde um 1990 von IBM und Microsoft entwickelt. Mit ihm werden die Kennwortinformationen gehasht, und dieser Hashwert wird gespeichert und übertragen. Ein Hashwert – oder auch ein Hashingalgorithmus – stellt stellt Folgendes sicher: Wenn die gleiche Eingabe (Text oder Datei) an den Algorithmus übergeben wird, wird am Ende immer der gleiche Hashwert ausgegeben. Ähnliche Eingaben müssen unterschiedliche Hashwerte liefern. Von einem Hashwert kann nicht auf den Eingabetext zurückgeschlossen werden, denn die mathematischen Funktionen bei der Hasherzeugung basieren auf *Falltüralgorithmen*.

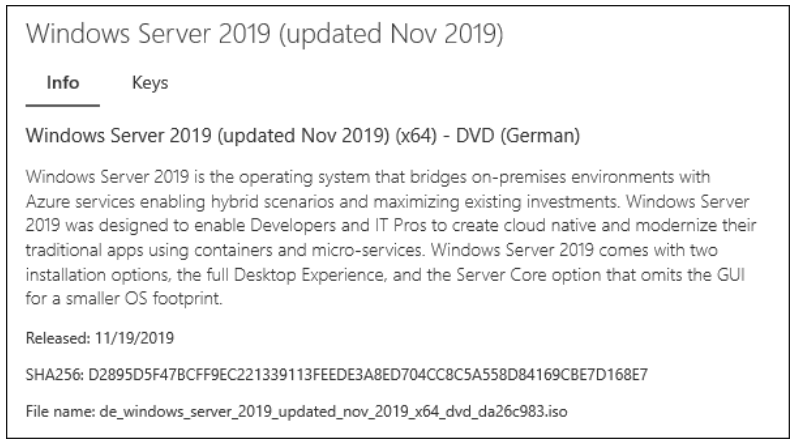


Abbildung 4.1 Der Hashwertes (SHA256) für den Download der ISO-Datei von Windows Server 2019 von my.visualstudio.com

Sie kennen Hashwerte vermutlich von Downloads aus dem Internet, wo Sie eine Prüfsumme für eine Datei finden, die Sie herunterladen möchten. Dadurch können Sie prüfen, ob der Download korrekt ausgeführt wurde (siehe Abbildung 4.1).

Hashwerte kommen unter anderem beim Clean-Source-Prinzip (siehe Abschnitt 12.3.1) zum Tragen.

LM wurde eingeführt, als Windows 3.0 aktuell war. LM hat – in Hinblick auf die Sicherheit – einige Probleme:

- Das eingegebene Kennwort wird in Blöcke mit jeweils 7 Zeichen geteilt. Ist die Länge des Kennwortes kein Vielfaches von 7, wird mit Nullen (0) aufgefüllt.
- Die Kleinbuchstaben im Kennwort werden durch Großbuchstaben ersetzt, wodurch der mögliche verwendbare Zeichensatz für Kennwörter reduziert wird.
- Die einzelnen 7 Zeichen langen Zeichenketten werden mit einer 56-Bit-DES-Verschlüsselung (DES – Data Encryption Standard) verschlüsselt.

Durch das Ändern der Kleinbuchstaben und die (nach heutigem Stand der Technik) veraltete und unsichere Verschlüsselung ist LM als sehr unsicheres Protokoll anzusehen und sollte nicht mehr verwendet werden. Eine Beschreibung, wie Sie das Protokoll abschalten, finden Sie in Abschnitt 4.1.9.

Auch wenn Sie heute (hoffentlich) aktuellere Betriebssysteme einsetzen, kann es trotzdem sein, dass Anwendungen noch alte Protokolle verwenden. Als Beispiel sei hier das SMB-Protokoll für den Dateizugriff genannt. Es kann vorkommen, dass in bestimmten Implementierungen von SMB noch sehr alte Authentifizierungsprotokolle aktiviert sind.

Ab Windows NT 3.5.1 und Windows 2000 wurde als Nachfolger das Protokoll NTLM (New Technology LAN-Manager) unterstützt, das – zumindest zu dieser Zeit – sicherer war.

4.1.2 NTLM

Der Nachfolger den LM-Protokolls ist *New Technology LAN-Manager* (NTLM). NTLM basiert auf einem sogenannten *Challenge und Response*-Verfahren. Dabei sendet der Client den Benutzernamen an das Zielsystem. Der Server sendet nun eine Zufallszahl (Challenge) an den Client. Der Client verschlüsselt die Challenge mit dem Hashwert seines Kennworts und sendet den Wert zurück (Response). Der Server verschlüsselt die Zufallszahl ebenfalls mit dem Hashwert des Kennworts, das lokal oder auf dem authentifizierenden Domänencontroller gespeichert ist. Sind die beiden Ergebnisse identisch, wird die Authentifizierung als erfolgreich betrachtet.

Die erste Version von NTLM war NTLMv1 (Version 1). Sie wurde als Nachfolger von LM verwendet. Da es in ihr auch einige Schwachstellen gab (die teilweise erst durch leistungsfähigere Rechner zum Erstellen von Hashwerten für Bruteforce-Angriffe ausgenutzt werden konnten), wurde die Version 2 des NTLM-Protokolls entwickelt und implementiert.

NTLMv2 ist heute noch im Einsatz, sollte aber – wenn möglich – durch Kerberos abgelöst werden. NTLM-Protokolle bieten das Risiko einer Replay-Attacke, bei der ein Angreifer den initialen Verbindungsaufbau abfängt und die Daten später erneut sendet.

4.1.3 Kerberos

Kerberos ist das aktuelle und bevorzugte Authentifizierungsprotokoll für Domänenumgebungen.

Der Name *Kerberos* leitet sich von Cerberus ab – dem dreiköpfigen Höllenhund aus der griechischen Mythologie. Dabei steht jeder der drei Köpfe für eine Komponente bei der Authentifizierung:

- *Client* – der Computer oder Benutzer, der auf die Zielressource zugreifen will
- *Zielserver* – der Dienst, auf den der Client zugreifen will
- *Schlüsselverteilungscenter* – der Dienst auf einem vertrauenswürdigen Server (Domänencontroller), der die für Kerberos notwendigen Tickets erstellt (*Key Distribution Center*, KDC)

Eine Kerberos-Authentifizierung kann man sehr gut mit dem System in einem Freizeitpark vergleichen: Wenn Sie morgens den Freizeitpark betreten, erwerben Sie an dem Kassenhäuschen ein Armband (*Ticket-Granting Ticket*, TGT), auf dem Ihr Alter, Ihre Größe und der Tag vermerkt werden, für den Sie den Eintritt bezahlt haben. Dieses Armband wird mit einer Plombe versiegelt. Mit ihm können Sie sich nun im Park bewegen.

Gelangen Sie nun zu einem Autoscooter-Fahrgeschäft und möchten Sie eines der Fahrzeuge benutzen, benötigen Sie einen Fahrchip (*Service-Ticket*), den Sie in den Autoscooter stecken müssen, damit das Fahrzeug startet. Diesen Chip erhalten Sie am Häuschen neben dem Fahrgeschäft. Dort zeigen Sie einfach nur Ihr Armband, um einen Chip zu erhalten. Das Armband – das die geprüften Merkmale (Alter, Größe, Datum) enthält, wurde von einer vertrauten Instanz ausgestellt (Plombe). Der Mitarbeiter vertraut daher den Angaben auf dem Armband und händigt Ihnen einen Fahrchip aus. Sie müssen also am (Kassen-)Häuschen des Autoscooters nicht mehr in Form eines Ausweises und Ihrer Kreditkarte den Nachweis erbringen, dass Sie das Mindestalter erfüllen und für heute bezahlt haben.

Auf Kerberos übertragen, fordert der Computer (und der Benutzer) bei der Anmeldung ein *Ticket-Granting Ticket* (ticketgewährendes Ticket) aus, das den Client dazu berechtigt, Service-Tickets (Diensttickets) – oder »Fahrchips« – anzufordern, mit denen der Client auf eine Ressource zugreifen kann.

Beide Tickets werden vom *Schlüsselverteilungscenter* (*Key Distribution Center*) ausgestellt. Dieser Dienst kann auf einem Windows Server ausgeführt werden, auf dem die Domänencontroller-Rolle installiert ist und der zu einem Domänencontroller heraufgestuft wurde.

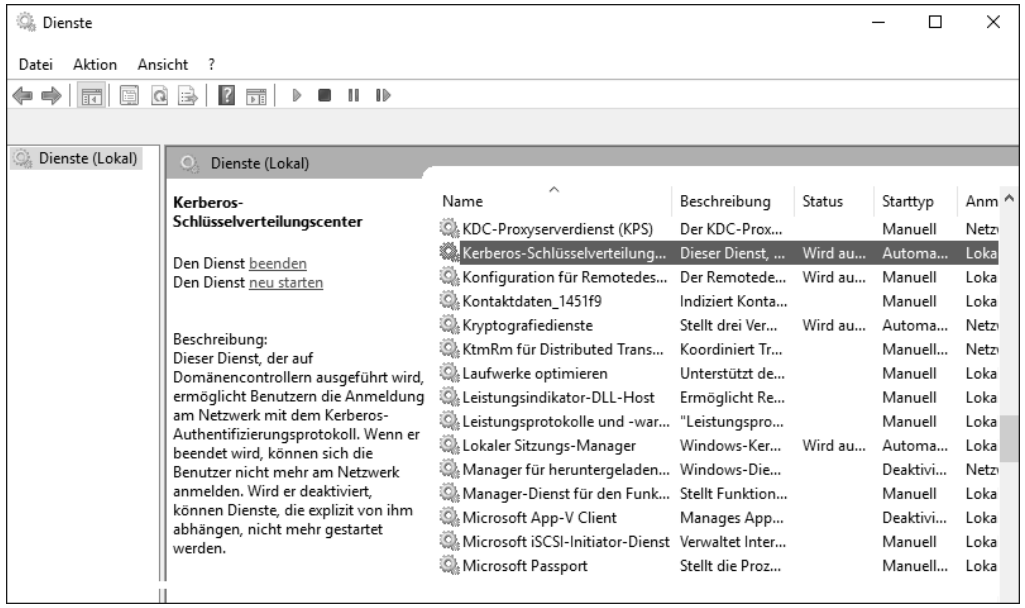


Abbildung 4.2 Der Dienst »Kerberos-Schlüsselverteilungscenter« auf einem Windows-Domänencontroller

Der Dienst *Kerberos-Schlüsselverteilungscenter* (Dienstname: KDC) besteht aus zwei Komponenten:

- *Authentication Service* – Der Authentication Service (AS) stellt die Ticket-Granting Tickets (»Armbänder«) aus.
- *Ticket-Granting Service* – Der Ticket-Granting Service (TGS) stellt die Service Tickets (»Fahrchips«) aus.

Mit dem Befehl `KList` können Sie sich auf einem Windows-Client die dort zwischengespeicherten Kerberos-Tickets anzeigen lassen und auch Kerberos-Tickets löschen (siehe Abbildung 4.3).

Java-Version

Abhängig von der auf dem Computer installierten Java-Version und der damit verbundenen *Path*-Umgebungsvariablen (in dieser Variable wird die Reihenfolge der Suchpfade für ausführbare Dateien definiert) kann es dazu kommen, dass das Java-Tool *KList* gestartet wird. Die Windows-Version befindet sich im Standard-Windows-Ordner *%windir%\System32*.

```
C:\Users\Peter.Kloep>klist

Aktuelle Anmelde-ID ist 0:0x17c37d

Zwischengespeicherte Tickets: (2)

#0>     Client: Peter.Kloep @ INTRANET.RHEINWERK-VERLAG.DE
        Server: krbtgt/INTRANET.RHEINWERK-VERLAG.DE @ INTRANET.RHEINWERK-VERLAG.DE
        KerbTicket (Verschlüsselungstyp): AES-256-CTS-HMAC-SHA1-96
        Ticketkennzeichen 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Startzeit: 7/18/2020 11:19:34 (lokal)
        Endzeit:   7/18/2020 21:19:34 (lokal)
        Erneuerungszeit: 7/25/2020 11:19:34 (lokal)
        Sitzungsschlüsseltyp: AES-256-CTS-HMAC-SHA1-96
        Cachekennzeichen: 0x2 -> DELEGATION
        KDC aufgerufen: PNHN10SDCV00001.intranet.rheinwerk-verlag.de

#1>     Client: Peter.Kloep @ INTRANET.RHEINWERK-VERLAG.DE
        Server: krbtgt/INTRANET.RHEINWERK-VERLAG.DE @ INTRANET.RHEINWERK-VERLAG.DE
        KerbTicket (Verschlüsselungstyp): AES-256-CTS-HMAC-SHA1-96
        Ticketkennzeichen 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Startzeit: 7/18/2020 11:19:19 (lokal)
        Endzeit:   7/18/2020 21:19:34 (lokal)
        Erneuerungszeit: 7/25/2020 11:19:34 (lokal)
        Sitzungsschlüsseltyp: AES-256-CTS-HMAC-SHA1-96
        Cachekennzeichen: 0x1 -> PRIMARY
        KDC aufgerufen: PNHN10SDCV00001.intranet.rheinwerk-verlag.de
```

Abbildung 4.3 (Teil)-Ausgabe der auf einem Client vorhandenen Kerberos-Tickets

Den Zweck und die Art eines Tickets können Sie in der Ausgabe des `KList`-Kommandos über den Wert `Server` identifizieren. Dort ist der `ServicePrincipalName` für den Zieldienst hinterlegt.

Im Beispiel aus Abbildung 4.3 können Sie erkennen, dass die beiden Tickets (`#0` und `#1`) für den Server `krbtgt/INTRANET.RHEINWERK-VERLAG.DE` ausgestellt wurden. `krbtgt` steht dabei für *Kerberos Ticket-Granting Ticket*. Tickets, die für diesen Server ausgestellt wurden, sind Ticket-Granting Tickets (»Armbänder«).

Die Sortierreihenfolge der Tickets zeigt immer zuerst die TGTs und anschließend die Service-Tickets an – die aktuellsten stehen jeweils an erster Stelle.

Ein Ticket-Granting Ticket (TGT), das der Domänencontroller basierend auf einem AS_REQ (*Authentication Service Request*) ausstellt, besteht aus den zwei Teilen, die Sie in Abbildung 4.4 sehen.

Der *Logon Session Key* wird für die Verschlüsselung der Kommunikation zwischen dem Benutzer (oder dem Computer – abhängig davon, für wen das Ticket ausgestellt wurde) und dem KDC verwendet. Dieser Session Key wird zweimal im TGT hinterlegt: Einmal wird der Session Key mit dem *Long Term Session Key* (LTSK) des Benutzers

verschlüsselt – einer Verschlüsselung, die vom Kennwort des Benutzers (oder Computers) abgeleitet wird. Eine weitere Kopie des Session Keys wird mit dem »Kennwort« des *krbtgt*-Benutzers verschlüsselt. In der zusätzlichen Kopie wird zudem das *Privilege Access Certificate* (PAC) hinzugefügt. Das PAC beinhaltet die Gruppenmitgliedschaften und Privilegien des Benutzers (oder Computers).

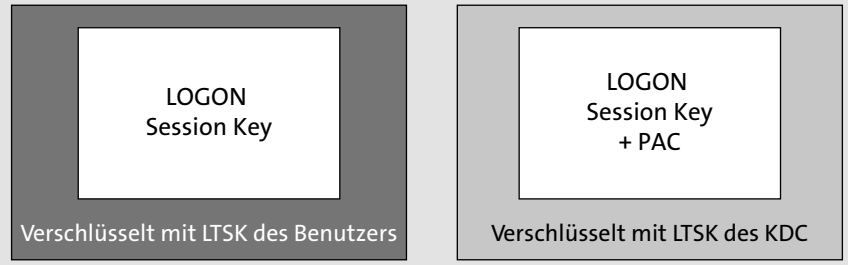


Abbildung 4.4 Inhalt eines TGT

Das *krbtgt*-Konto befindet sich im *Users*-Container der Domänenpartition des Active Directory des Benutzers oder Computers und ist deaktiviert (siehe Abbildung 4.5). Um sich das Konto mit dem Tool Active Directory-Benutzer und -Computer anzeigen zu lassen, müssen Sie die »Erwachsenen-Ansicht« aktivieren, indem Sie Ansicht • Erweiterte Features auswählen.

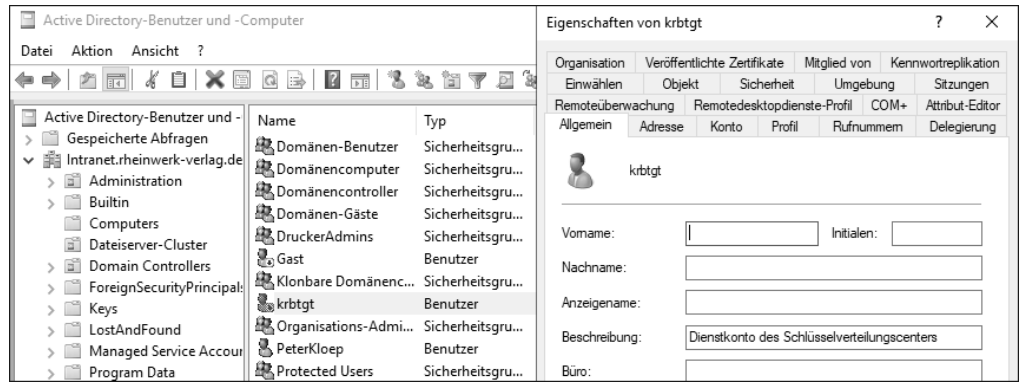


Abbildung 4.5 Anzeige des »krbtgt«-Kontos

Der zweite Teil des TGT wird basierend auf dem Kennwort dieses Kontos verschlüsselt, sodass Sie mit dem TGT bei einem anderen Domänencontroller der Domäne weitere Tickets anfordern können, ohne sich erneut durch Eingabe von Benutzername und Kennwort (oder einer anderen Authentifizierungsmethode) anmelden zu müssen. Das *krbtgt*-Konto wird auf alle Domänencontroller der Domäne repliziert,

wodurch jeder Domänencontroller der Domäne den zweiten Teil des TGTs entschlüsseln kann.

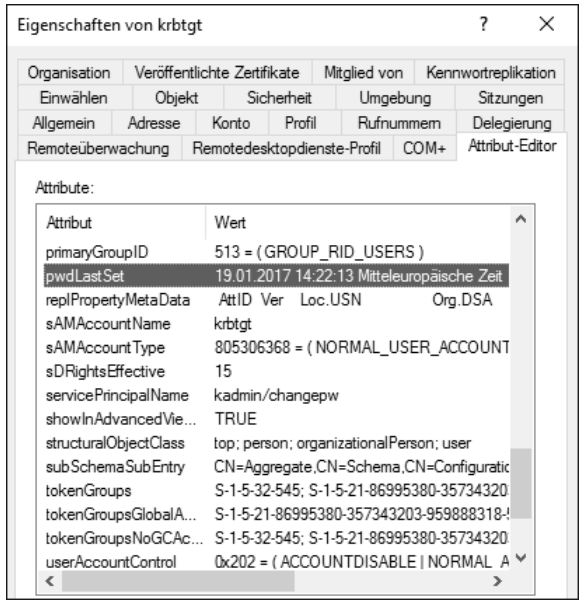


Abbildung 4.6 Kennwortänderungsdatum des »krbtgt«-Kontos

Das Kennwort dieses Kontos – das zur Verschlüsselung der TGTs verwendet wird – wird nicht automatisch geändert. Das System verwendet ein komplexes und über 120 Zeichen langes Kennwort. Microsoft empfiehlt, das Kennwort des Kontos in regelmäßigen Abständen zu ändern. Dadurch werden eventuell existierende Golden Tickets, die das unbegrenzte Erstellen weiterer Tickets ermöglichen, ungültig (siehe Abschnitt 3.2.3).

Die Empfehlung und eine Beschreibung des PowerShell-Skripts zum Durchführen der Änderung finden Sie unter *https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51* und den Download unter *https://github.com/microsoft/New-KrbtgtKeys.ps1*.

Das Reset-Script funktioniert nur auf englischsprachigen Betriebssystemen

In der aktuellen Version (Stand: Sommer 2020) funktioniert das Skript nur mit Domänencontrollern, die ein englischsprachiges Betriebssystem ausführen. Sie können es aber bei Bedarf anpassen.

Basierend auf dem ausgestellten TGT kann der Client Service-Tickets beim TGS (Ticket-Granting Service) anfordern. Dazu sendet der Client einen *TGS Request* an den Domänencontroller (siehe Abbildung 4.7). Dieser Request beinhaltet einen Authenticator, der die Zielressource beschreibt. Dieser Authenticator wird mit dem Session Key des TGT verschlüsselt. Zusätzlich wird der zweite Teil des TGT (der Teil, der mit dem *krbtgt*-Kennwort verschlüsselt wurde) mit an den Domänencontroller gesendet.

Der Domänencontroller sucht nun nach dem *Service Principal Name* (SPN), der Zielressource. Dieser SPN wird bei `KList` unter dem Punkt `Server` angezeigt. SPNs müssen im Active Directory eindeutig zuzuordnen sein. Sollte ein Domänencontroller keinen oder mehrere SPNs für ein Ziel finden, kann der Domänencontroller kein Service-Ticket ausstellen.

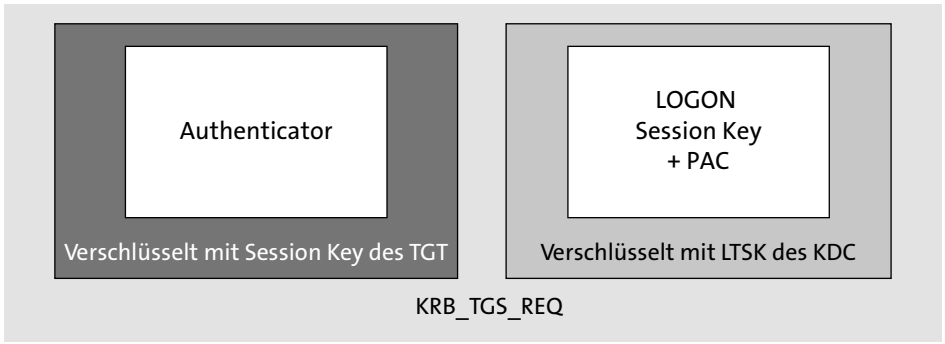


Abbildung 4.7 Inhalt des »TGS Request«

Sowohl das TGT als auch das Service-Ticket wird verschlüsselt. Dabei handeln Client und Server das bestmögliche Protokoll aus. Abhängig vom verwendeten Betriebssystem oder den konfigurierten Einstellungen können hier durchaus alte und unsichere Protokolle zum Einsatz kommen, z. B. DES mit einer 56-Bit-Verschlüsselung. Aktuelle Betriebssysteme verwenden den aktuellen AES-Standard (*Advanced Encryption Standard*) mit 128 oder 256 Bit. AES ist deutlich robuster gegen Angriffe als das deutlich ältere DES-Protokoll.

Das vom Domänencontroller ausgestellte TGS wird an den Client übermittelt. Auch dieses Ticket besteht aus zwei Teilen (siehe Abbildung 4.8).

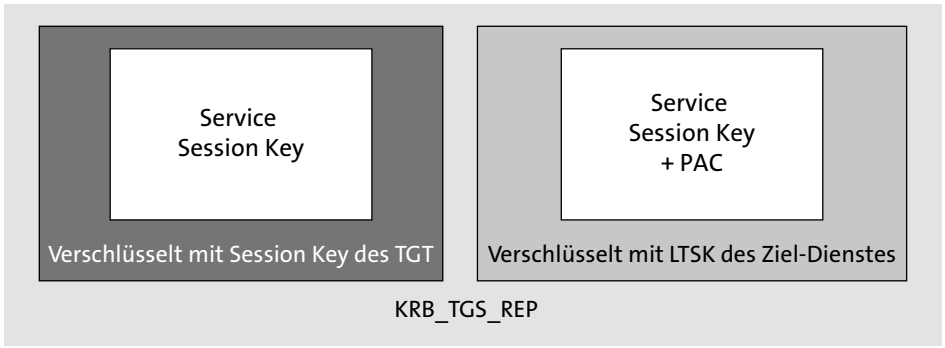


Abbildung 4.8 Inhalt des »TGS Reply«

Dazu berechnet der Domänencontroller einen *Service Session Key*, der an den Client übertragen wird. Einmal wird der Key auf Basis des Session-Keys aus dem Ticket-Granting Ticket verschlüsselt, damit der Client den Inhalt entschlüsseln kann. Zusätzlich wird zum Session-Key ein PAC angefügt und mit dem Kennwort des Zieldienstes verschlüsselt. Dieses Kennwort ist entweder das Computerkennwort (sofern der Zieldienst unter dem Computerkonto ausgeführt wird) oder basiert auf dem Kennwort des Dienstkontos, das auf dem Zieldienst eingerichtet wurde. Den zweiten Teil des TGS (mit dem PAC) übermittelt der Client an das Zielsystem, wo es entschlüsselt werden kann.

Die ausgestellten TGS werden auf dem Client ebenfalls mit dem `KList`-Kommando angezeigt (siehe Abbildung 4.9). Eine Zuordnung zum Ziel erfolgt über den `Server`-Wert, der zurückgegeben wird. Hier wird der Service Principal Name des Zieldienstes angezeigt.

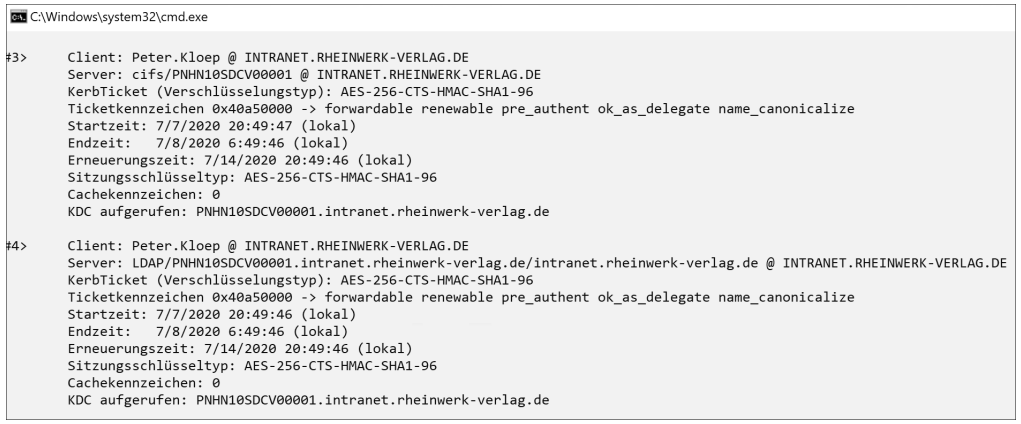


Abbildung 4.9 Für den Benuzter ausgestellte Service-Tickets

Kerberos-Tickets sind standardmäßig 10 Stunden lang gültig. Dieser Wert kann innerhalb der Domäne über Gruppenrichtlinien angepasst werden.

Kann ein Client keine Authentifizierung mittels Kerberos durchführen, wird der (Windows)-Client ein *Failback* zu älteren Authentifizierungsprotokollen (NTLM oder LM) versuchen.

Damit die Kerberos-Authentifizierung richtig funktioniert, muss in der Domänenumgebung eine »saubere« Zeitsynchronisierung vorhanden sein oder eingerichtet werden. Der PDC-Emulator der Stammdomäne sollte mit einer externen Zeitquelle synchronisiert werden. Diese Konfiguration muss manuell erfolgen. Die anderen Domänencontroller beziehen die Zeit dann vom PDC-Emulator der Domäne über das NT5DS-Protokoll. Alle anderen Domänenmitglieder beziehen die Systemzeit von ihrem Anmeldeserver.

NT5DS ist das Standardprotokoll zur Zeitsynchronisierung auf domänenbasierten Systemen. Andere Systeme verwenden das NTP-Protokoll.

Sie können die Zeitquelle bei den Systemen mithilfe von `W32TM /query /status` abfragen.

Die Ausgabe könnte für einen Nicht-Domänencontroller so wie in Listing 4.1 aussehen:

```
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\1Peter.Kloep>w32tm /query /status
Sprungindikator: 0(keine Warnung)
Stratum: 4 (Sekundärreferenz - synchr. über (S)NTP)
Präzision: -23 (119.209ns pro Tick)
Stammverzögerung: 0.0002500s
Stammabweichung: 0.0100002s
Referenz-ID: 0x564D5450 (Quell-IP:  86.77.84.80)
Letzte erfolgr. Synchronisierungszeit: 24.02.2020 13:21:18
Quelle: VM IC Time Synchronization Provider
Abrufintervall: 6 (64s)
```

Listing 4.1 Abfrage des Zeitservers bei einem virtuellen Fileserver der Domäne

Bei virtuellen Maschinen ist standardmäßig die Zeitsynchronisierung zwischen dem Host (Blech) und dem Gast (virtuelle Maschine) aktiviert. Diese kann in den Eigenschaften der virtuellen Maschinen angepasst werden. Alternativ können Sie mithilfe einer Gruppenrichtlinie den Dienst, der in der virtuellen Maschine läuft, abschalten, sodass eine Anpassung der Eigenschaften der virtuellen Maschinen nicht mehr notwendig ist. Setzen Sie dazu den Wert für `Enabled` unter *Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\VMICTimeProvider* auf `0`. Nach einem Neustart des Windows-Zeitgebers oder nach einem Neustart des Systems sind die Änderungen sichtbar (einen Auszug aus der Ausgabe sehen Sie in Listing 4.2):

```
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\1Peter.Kloep>w32tm /query /status
Referenz-ID: 0xAC10C8C9 (Quell-IP:  172.16.200.201)
Letzte erfolgr. Synchronisierungszeit: 24.02.2020 13:24:55
Quelle: PNHN10SDCV00001.Intranet.rheinwerk-verlag.de
```

Listing 4.2 Ausgabe von »W32tm« bei deaktiviertem »VMICTimeProvider«

4.1.4 Service Principal Names (SPN)

Dienstprinzipalnamen (*Service Principal Names*, SPN) werden benötigt, damit der Domänencontroller die Diensttickets (Service-Tickets) mit einem Geheimnis verschlüsseln können, das dem Zieldienst bekannt ist. SPNs werden entweder auf Active Directory-Computer- oder -Benutzerkonten registriert – abhängig davon, in welchem Kontext der Zieldienst ausgeführt wird.

Vereinfachte Namen zur leichteren Erklärung

Im folgenden Abschnitt bin ich vom definierten Namenskonzept abgewichen und habe weniger komplexe und damit für Sie leichter lesbarere und verständlichere Namen verwendet, um die Kerberos-Delegierung zu erklären.

Damit eine korrekte Zuordnung durch den Domänencontroller erfolgen kann, müssen SPNs in der Gesamtstruktur eindeutig sein. Sollten mehrere gleiche SPNs vorhanden sein, werden für dieses Ziel keine Kerberos-Tickets ausgestellt. Ein Service Principal Name hat meist die Form `<Dienst>/<Ziel>`, also z. B. `CIFS/W2K19-FS01` oder `LDAP/PNHN10SDCV00001`. Wird jetzt ein Dienstticket für einen Zieldienst angefordert, sucht der Domänencontroller über das gesamte Active Directory nach dem SPN, um festzustellen, welchem Konto (Benutzer oder Computer) dieser zugeordnet ist. Wird genau ein Konto gefunden, wird der Session Key des TGS mit dem Kennwort des Zieldienstes verschlüsselt (bzw. mit einem *Long-Term Session Key*, der vom Kennwort gebildet wird). Wird kein SPN oder werden mehrere gleiche SPNs gefunden, stellt der Domänencontroller gar kein Ticket aus: Stellen Sie sich vor, Sie kommen an eine Rezeption und möchten Frau Müller besuchen. Nun prüft die Person an der Rezeption, ob Frau Müller anwesend ist. Wenn es aber mehrere Frau Müllers im Unternehmen gibt und Sie weder den Vornamen noch die Abteilung wissen, werden Sie nicht durchgelassen. Der Domänencontroller agiert genauso wie eine sicherheitsbewusste Rezeptionistin: Obwohl die Rezeptionistin nacheinander alle Frauen namens Müller kontaktieren könnte, tut sie es nicht, sondern hält Sie für verdächtig. Analog wird der Domänencontroller, wenn er mehrere SPNs erkennt, die Erstellung des Kerberos-Tickets verweigern.

Die SPN werden im Attribut SERVICEPRINCIPALNAME (siehe Abbildung 4.10) gespeichert und können hier auch geändert werden. Fordert nun ein Client ein Kerberos-Ticket für einen Zieldienst an und findet der Domänencontroller mehrere Computer (oder Benutzer), die den gleichen SPN registriert haben, wird der Domänencontroller in der Ereignisanzeige einen Fehler protokollieren, der besagt, dass ein doppelter SPN gefunden wurde (siehe Abbildung 4.11).

Den Eintrag finden Sie im System-Protokoll von der Quelle *Kerberos-Key-Distribution-Center* (Kerberos-Schlüsselverteilzentrum).

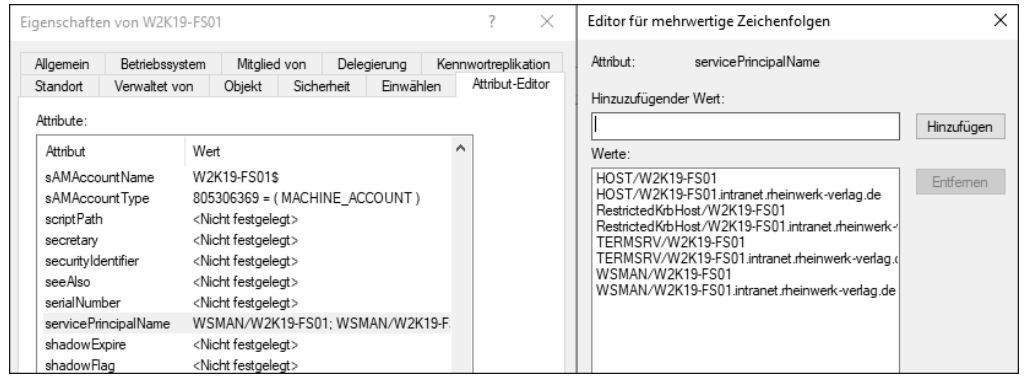


Abbildung 4.10 »servicePrincipalName«-Attribut eines Computerkontos

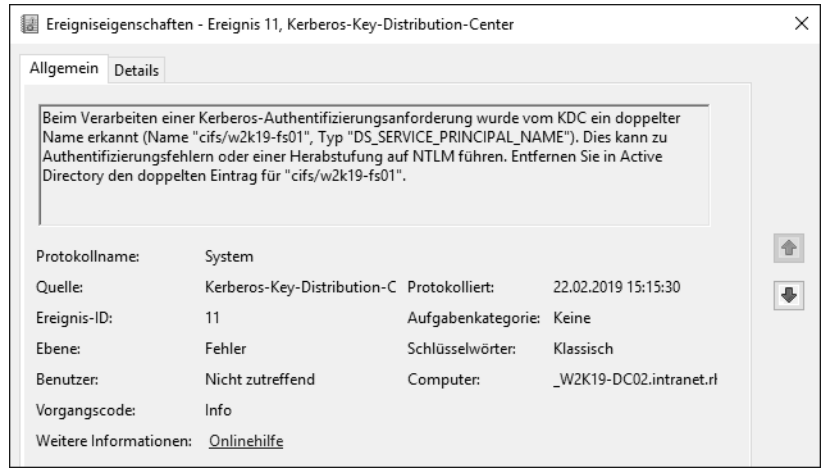


Abbildung 4.11 Ereignisprotokolleintrag mit einem doppelten SPN für »cifs/w2k19-fs01«

Seit Windows Server 2012 verhindern die von Microsoft bereitgestellten Tools das Anlegen doppelter SPNs. Wurden jedoch vorher bereits solche Einträge erstellt, bleiben sie auch bei einem Domänen-Upgrade erhalten. Auch wenn doppelte SPNs vorhanden sind und die Fehler in der Ereignisanzeige protokolliert werden, merken Benutzer eventuell nichts von den Problemen, da das System automatisch ein Failback zu NTLMv2 durchführt und der Zugriff darüber autorisiert wird.

Sie können das sehr einfach mit einem `KList` testen. Nach dem Zugriff sollte ein Kerberos-Ticket angezeigt werden.

Die Verwaltung der SPNs kann über jeden LDAP-Browser oder über die Active Directory-Tools erfolgen. Alternativ steht das Kommandozeilentool `SetSPN` zur Verfügung, mit dem Sie SPNs erstellen und löschen können. Zusätzlich können Sie mit dem Tool nach doppelten SPNs in der Umgebung suchen:

```
C:\Users\Administrator.INTRANET>setspn -x
Die Domäne "DC=intranet,DC=rheinwerk-verlag,DC=de" wird überprüft.
Eintrag 0 wird verarbeitet.
HOST/W2K19-FS01 wird auf diesen Konten registriert:
        CN=W2K19-FS02,CN=Computers,DC=intranet,DC=rheinwerk-verlag,DC=de
        CN=W2K19-FS01,CN=Computers,DC=intranet,DC=rheinwerk-verlag,DC=de

1 Gruppe von doppelten SPNs gefunden.
```

Listing 4.3 Suche nach doppelten SPNs mit »SetSPN«

In Listing 4.3 können Sie sehen, dass der SPN `HOST/W2K19-FS01` auf zwei Computerkonten registriert ist. Dies kann durch manuelle Fehlkonfiguration passiert sein oder durch das Anpassen von Diensten. Wenn Sie zum Beispiel einen SQL-Server installieren und diesen bei der ersten Einrichtung als *Lokales System* laufen lassen, dann würde der SPN auf dem Computerkonto registriert. Ändern Sie nun nachträglich das Konto, mit dem der SQL ausgeführt wird, in ein Benutzerkonto, dann wird das System eventuell den SPN (zusätzlich) am Benutzerkonto registrieren und nicht aus dem Computerkonto entfernen.

Das manuelle Setzen eines SPN über die Kommandozeile erfolgt mit dem Aufruf `setspn -S host/W2K19-FS01 W10-PAW01` wie in Listing 4.4:

```
C:\Windows\system32>setspn -S host/W2K19-FS01 W10-PAW01
Die Domäne "DC=Intranet,DC=rheinwerk-verlag,DC=de" wird überprüft.
CN=W2K19-FS01,CN=Computers,DC=Intranet,DC=rheinwerk-verlag,DC=de
        RestrictedKrbHost/W2K19-FS01
        HOST/W2K19-FS01
        RestrictedKrbHost/W2K19-FS01.Intranet.rheinwerk-verlag.de
        HOST/W2K19-FS01.Intranet.rheinwerk-verlag.de

Doppelter SPN gefunden, Vorgang wird abgebrochen.
```

Listing 4.4 Das Anlegen wird abgebrochen, wenn der SPN bereits auf einem anderen Konto registriert ist.

Mit `SetSPN` wird automatisch eine Prüfung auf doppelte SPNs beim Erstellen durchgeführt. Den Parameter `-A`, den es in früheren Versionen noch gab, wird durch `-S` ersetzt. Mit dem Parameter `-A` war es möglich, die Überprüfung auf doppelte SPN zu überspringen.

Wenn Sie sich nun die ausgestellten Kerberos-Tickets anschauen, werden Sie Tickets für `LDAP/`, `CIFS/` und andere Dienste finden. Sie werden jedoch keine SPNs finden, die für diese Dienste registriert sind. Hinter dem SPN `Host/` verbergen sich zahlreiche unterschiedliche Dienste. Die Liste kann über einen Eintrag im Konfigurations-

container des Active Directory angepasst werden. Für diese Änderung benötigen Sie Organisationsadministrator-Rechte.

Hinter dem Parameter `Host` verbergen sich die SPNs aus Listing 4.5, die über die Eigenschaften von `Directory Service` im Active Directory zentral festgelegt werden können (siehe Abbildung 4.12).

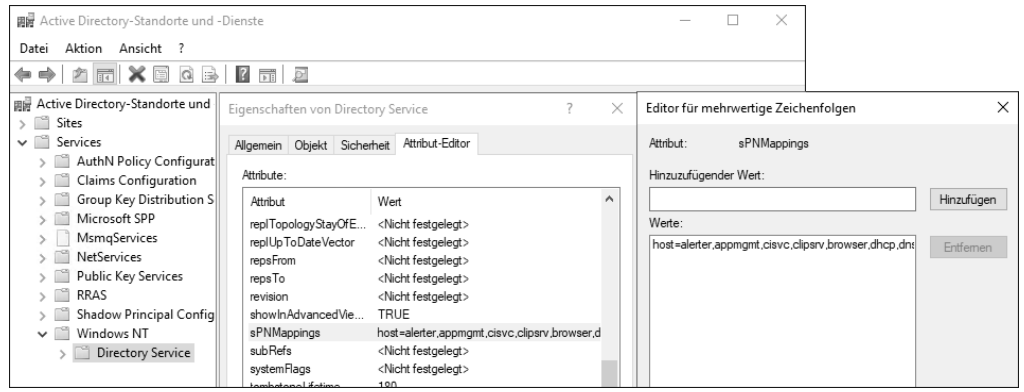


Abbildung 4.12 Übersicht der »sPNMappings«

```
host=alerter,appmgmt,cisvc,clipsrv,browser,dhcp,dnscache,replicator,eventlog,
eventsystem,policyagent,oakley,dmserver,dns,mcsvc,fax,msiserver,ias,messenger,
netlogon,netman,netdde,netddedsm,nmagent,plugplay,protectedstorage,rasman,
rpclocator,rpc,rpcss,remoteaccess,rsvp,samss,scardsvr,scesrv,seclogon,scm,
dcom,cifs,spooler,snmp,schedule,tapisrv,trksvr,trkwks,ups,time,wins,www,http,
w3svc,iisadmin,msdtc
```

Listing 4.5 Liste der SPNs, die sich hinter »Host/« verbergen

Sie sollten Ihre Umgebung auf das Vorhandensein von doppelten SPNs überwachen und/oder eine Überwachung des Systemereignisprotokolls auf das Vorhandensein der Ereignis-ID `11` einrichten.

4.1.5 Kerberos-Delegierung

Von einer Kerberos-Delegierung spricht man, wenn Anmeldeinformationen im Namen eines anderen an Systeme weitergegeben werden. Stellen Sie sich vor, Sie möchten über einen Webserver auf Daten eines Datenbankservers zugreifen. In Hinblick auf die Sicherheit ist es durchaus sinnvoll, den Datenbankserver gegen einen direkten Zugriff durch die Clients abzuschotten und den Server in ein separates Netzwerksegment zu bringen, auf das nur der Webserver (Frontend-Server) Zugriff hat. Der Datenbankserver benötigt außerdem Zugriff auf einen Domänencontroller und eventuell weitere unterstützende Dienste (Updates, Virenscanner).

Damit nun ein Benutzer über die Webseite auf die Daten des SQL-Servers zugreifen kann, muss auf dem Webserver ein sogenannter *Kontextwechsel* (*Impersonation*) stattfinden. Dabei wird der Zugriff auf den Datenbankinhalt durch ein hinterlegtes Konto durchgeführt. Dieses Konto hat keine Beziehung zu dem Benutzer, der gerade auf den Webserver zugegriffen hat. Eine Filterung der Daten basierend auf dem Benutzer, der über den Webserver zugreift, ist somit auf Datenbankebene nicht möglich und muss durch den Entwickler des Webdienstes geregelt werden. Dort muss sichergestellt sein, dass dem Benutzer nur die Daten zur Verfügung gestellt werden, die der Benutzer sehen soll.

Damit eine Sicherheitsfilterung auf der Quelle der Daten, also dem Datenbankserver, durchgeführt werden kann, sollte eine Kerberos-Delegierung eingerichtet werden. Dabei wird dem Webserver erlaubt, die ihm präsentierten Anmeldeinformationen an den SQL-Server weiterzugeben. Dies ist natürlich ein sehr sensibles Recht, das nur auf die gewünschten Zieldienste beschränkt werden sollte.

Diese Kerberos-Delegierung funktioniert nur, wenn Kerberos läuft, und muss auf dem System eingerichtet werden, das das Recht zum Delegieren bekommen soll .

Delegierung

Damit die Registerkarte Delegierung (siehe Abbildung 4.13) verfügbar ist, muss auf dem Konto (Benutzer oder Computer) ein SPN registriert sein. Ist kein SPN registriert, kann keine Delegierung eingerichtet werden.

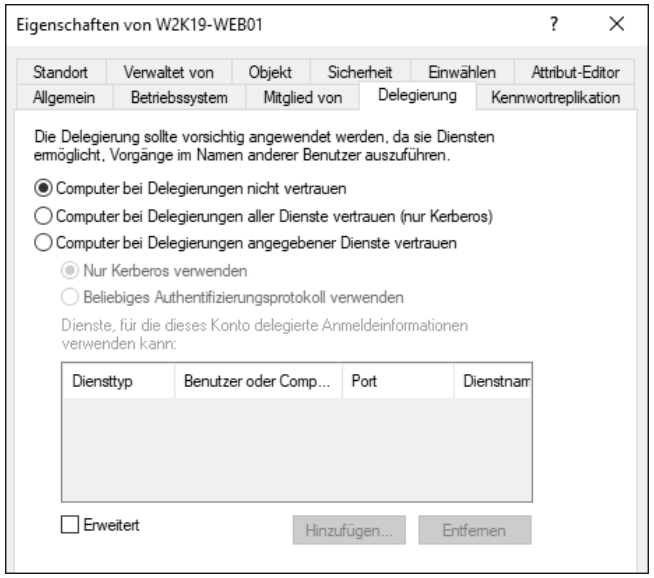


Abbildung 4.13 Die Registerkarte »Delegierung« eines Server-Kontos

In den Eigenschaften des Computers oder des Benutzers stehen folgende Optionen zur Verfügung:

- Computer bei Delegierungen nicht vertrauen – Dies ist die Standardeinstellung. Dabei darf dieses System keine Anmeldeinformationen an andere Systeme weiterleiten.
- Computer bei Delegierungen aller Dienste vertrauen (nur Kerberos) – Diese Option wird als *Unconstrained Delegation* bezeichnet. Das bedeutet, dass es für die Kerberos-Delegierung keine Beschränkung gibt. Damit darf das System die Anmeldeinformationen an jedes andere System weiterleiten und eventuell Zugriff auf Ressourcen darüber erhalten. Hierbei besteht das Risiko, dass die Anmeldeinformationen missbraucht werden können, wenn das System kompromittiert wurde oder durch den Systemverwalter (lokaler Administrator) falsch konfiguriert wurde.
- Computer bei Delegierungen angegebener Dienste vertrauen – Bei dieser »eingeschränkten Delegierung« (*Constrained Delegation*) darf das System die Anmeldeinformationen nur an vordefinierte Systeme weiterleiten. Dadurch wird das Risiko des Missbrauchs reduziert.

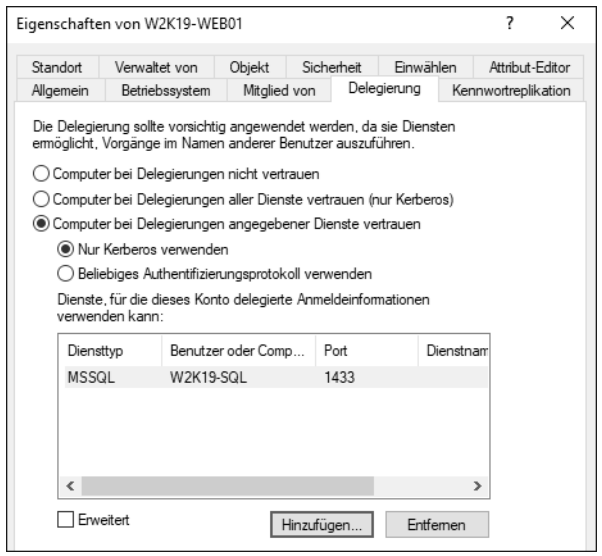


Abbildung 4.14 Konfiguration der eingeschränkten Delegierung

Die Auswahl in Abbildung 4.14 gestattet es dem Webserver, die Anmeldeinformationen, die dem Webserver präsentiert werden, an den Datenbankserver weiterzuleiten.

Ein weiterer Schutz vor Missbrauch der Delegierung sind die Einstellungen bei den Benutzerkonten. Hier können Sie – besonders bei administrativen Konten – konfigu-

rieren, dass eine Weitergabe von Anmeldeinformationen für diese Konten gar nicht möglich ist. Wählen Sie dazu in den Eigenschaften des Kontos die Option KONTO IST VERTRAULICH UND KANN NICHT DELEGIERT WERDEN.

4.1.6 Kerberos-Richtlinien

Mithilfe von Kerberos-Richtlinien können Sie die Gültigkeit der Kerberos-Tickets konfigurieren.

Dies erfolgt über COMPUTERKONFIGURATION • RICHTLINIEN • WINDOWS-EINSTELLUNGEN • SICHERHEITSEINSTELLUNGEN • KONTORICHTLINIEN • KERBEROS-RICHTLINIE. Hier können Sie unter anderem die maximale Gültigkeit für Benutzer- und Diensttickets hinterlegen (siehe Abbildung 4.15).

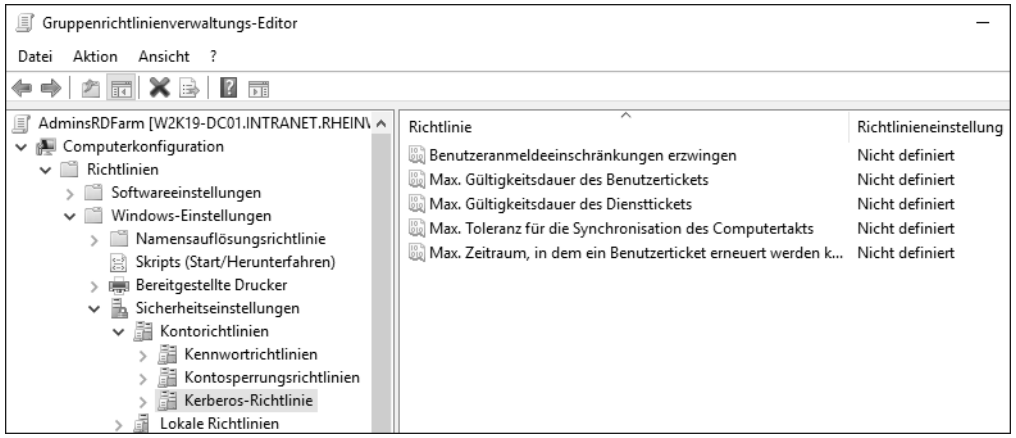


Abbildung 4.15 Konfigurationsmöglichkeit der Kerberos-Richtlinien

Zusätzlich kann per Gruppenrichtlinie die maximale Zeitabweichung hinterlegt werden, die für die Verwendung von Kerberos zulässig ist. Dieser Wert beträgt standardmäßig 5 Minuten.

Eine weitere wichtige Richtlinie ist die Konfiguration der möglichen Verschlüsselungsalgorithmen für die Kerberos-Tickets. Welche Algorithmen Sie verwenden können, hängt vom verwendeten Betriebssystem ab. Dabei spielen sowohl die Kerberos-Clients als auch die Domänencontroller eine Rolle und müssen entsprechend konfiguriert werden.

Die Richtlinie finden Sie unter COMPUTERKONFIGURATION • RICHTLINIEN • WINDOWS-EINSTELLUNGEN • SICHERHEITSRICHTLINIEN • LOKALE RICHTLINIEN • SICHERHEITOPTIONEN. Dort finden Sie die Option NETZWERKSICHERHEIT: FÜR KERBEROS ZULÄSSIGE VERSCHLÜSSELUNGSTYPEN KONFIGURIEREN (siehe Abbildung 4.16). Im Listenfeld darunter können Sie die für Kerberos möglichen Verschlüsselungsproto-

kolle konfigurieren. Der Client wird beim Anfordern des Ticket-Granting Tickets eine Liste seiner möglichen Protokolle verschicken, die der Domänencontroller dann gegen die Liste der Protokolle prüft, die er unterstützt. Dann wählt er aus den beiden Listen das beste Protokoll aus. Findet der Domänencontroller kein passendes Protokoll, wird es keine Kerberos-Tickets geben und es wird eventuell ein Failback auf NTLM durchgeführt.

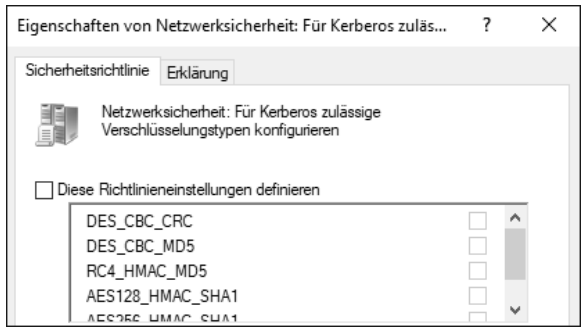


Abbildung 4.16 Konfiguration der Verschlüsselungstypen für Kerberos

Diese Richtlinie sollte so konfiguriert werden, dass Clients und Domänencontroller mindestens ein gemeinsames Protokoll finden. Hierauf ist besonders bei Umstellungen der Betriebssysteme bzw. der Aktualisierung von Betriebssystemen zu achten und nach erfolgter Konfiguration sollte getestet werden, ob gültige Kerberos-Tickets ausgestellt werden.

4.1.7 Kerberos und Vertrauensstellungen

Bei der Einrichtung einer Vertrauensstellung (siehe Abschnitt 14.2.2) können Sie zwischen unterschiedlichen Vertrauensstellungstypen auswählen. Sie können eine *externe Vertrauensstellung* oder eine *Gesamtstrukturvertrauensstellung* zwischen Windows-Domänen bzw. Windows-Gesamtstrukturen erstellen. Die externen Vertrauensstellungen werden als *Legacy-Trust* (veraltete Vertrauensstellung) bezeichnet und sollten nicht mehr verwendet werden. Heutzutage sollten Sie eine Gesamtstrukturvertrauensstellung verwenden, damit Sie Kerberos sicher zwischen den beiden Umgebungen einsetzen können. Bei einem Legacy-Trust kann nicht garantiert werden, dass die Kerberos-Authentifizierung zuverlässig funktioniert.

Haben Sie nun eine Gesamtstrukturvertrauensstellung eingerichtet und möchten Sie auf eine Ressource in der anderen Gesamtstruktur zugreifen, so bekommen Sie von »Ihrem« Domänencontroller ein sogenanntes *Kerberos-Referral-Ticket*. Dieses Weiterleitungsticket wird mit dem Kennwort des *Trusted Domain Object* (TDO, *Vertraute Domäne*-Objekt) verschlüsselt. Die Trusted Domain Objects befinden sich

jeweils im System-Container der vertrauenden Domäne (siehe Abbildung 4.17). Der *PDC* (primäre Domänencontroller) der vertrauten Domäne wird dieses Kennwort alle 30 Tage automatisch ändern und übertragen.

Mit dem Referral-Ticket wenden Sie sich nun an einen Domänencontroller der »anderen« Domäne. Da dieser das Referral-Ticket entschlüsseln kann, wird er dann ein Service-Ticket für das Ziel ausstellen und Ihnen zurückschicken.

Auf den Freizeitpark übertragen, bedeutet das: Habe ich in »meinem« Freizeitpark (in meiner Domäne) ein Armband (ein Ticket-Grantig Ticket) erhalten und gehe ich damit in einen anderen Freizeitpark, der mit »meinem« Freizeitpark kooperiert, dann kann ich in dem zweiten Park basierend auf dem vertrauten Armband Fahrchips erhalten, ohne dort erneut meinen Ausweis und zusätzliche Unterlagen vorzuweisen.

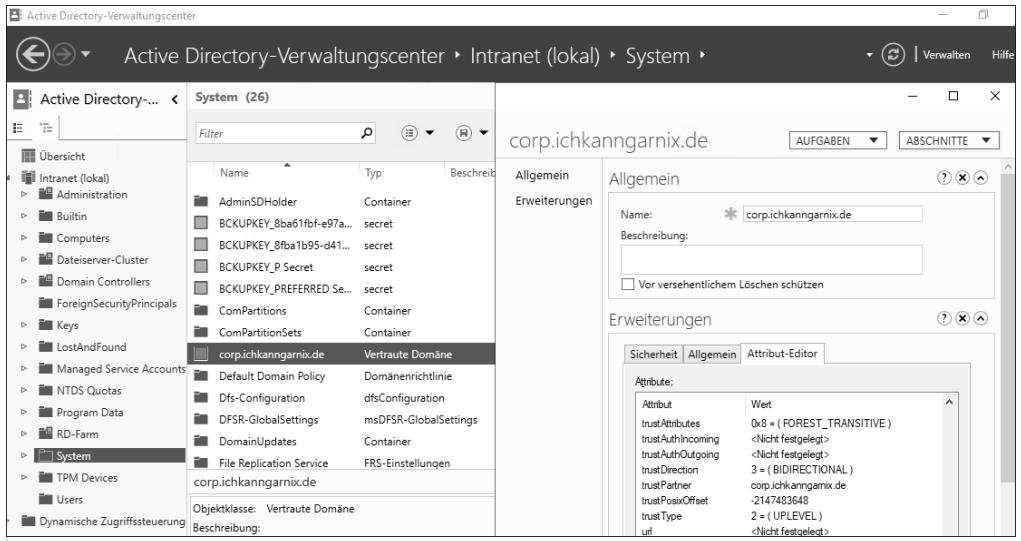


Abbildung 4.17 Das »Trusted Domain Object« für die Gesamtstruktur »corp.ichkanngarnix.de«

Bei der Konfiguration der Vertrauensstellungen müssen Sie nachträglich die Einstellungen der gerade erstellten Vertrauensstellung überprüfen. Dort gibt es ein unscheinbares Feld, in dem Sie die AES-Verschlüsselung für die Kerberos-Tickets aktivieren können. Diese Option ist standardmäßig nicht aktiviert. Ist nun jedoch in einer der beiden Umgebungen eine Gruppenrichtlinie konfiguriert, die ausschließlich Kerberos mit einer AES-Verschlüsselung erlaubt (siehe Abbildung 4.18), wird zwischen den beiden Umgebungen keine Authentifizierung mittels Kerberos möglich sein und es wird vermutlich NTLM verwendet.

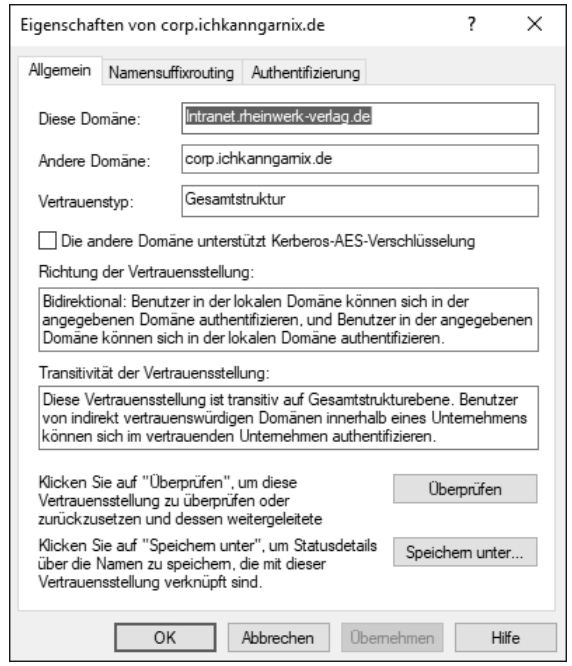


Abbildung 4.18 Konfiguration der Vertrauensstellungsoptionen zum Aktivieren der AES-Verschlüsselung

4.1.8 Ansprüche (Claims) und Armoring

Ansprüche (*Claims*) können für Authentifizierungs-Silos und die dynamische Zugriffssteuerung (*Dynamic Access Control*, DAC) verwendet werden. Zusätzlich wird so bei Clients ab Windows 8 und DCs ab Windows Server 2012 *Kerberos Armoring* vorgenommen, eine Härtung des Kerberos-Protokolls.

Ansprüche können beispielsweise von einen Dateiserver ausgewertet werden, sodass Sie die Berechtigungen auf Dateien so festlegen können, dass ein Benutzer mit einem bestimmten Attribut im Active Directory (z. B. Department = Geschäftsleitung) nur auf einem Computer mit einem entsprechenden AD-Attribut (z. B. Department = Geschäftsleitung) auf die Dateien zugreifen kann. Ist eines der beiden Attribute nicht vorhanden, wird der Zugriff verweigert. Damit diese Informationen von einem Domänencontroller geliefert werden, muss der Client »danach fragen« und der Domänencontroller diese Ansprüche liefern können. Diese Einstellungen können mithilfe von Gruppenrichtlinien aktiviert werden.

Die Einrichtung der Dynamischen Zugriffssteuerung (Dynamic Access Control, DAC), die Ansprüche für den Dateizugriff verwendet, erfolgt über das Active Directory-Verwaltungscenter (siehe Abbildung 4.19).

Abbildung 4.19 Möglichkeit zur Einrichtung der »Dynamischen Zugriffssteuerung«

Hier stehen fünf Objekte bzw. Container zur Verfügung:

- Central Access Policies (zentrale Zugriffsrichtlinie) – Eine zentrale Zugriffsrichtlinie enthält mehrere *zentrale Zugriffsregeln* (*Central Access Rules*), in denen festgelegt wird, wer Zugriff auf Ressourcen wie Dateien und Ordner hat. Die Richtlinie kann veröffentlicht und dann auf eine Ressource angewendet werden, um den Zugriff auf diese Ressource zu steuern.
- Central Access Rules (zentrale Zugriffsregel) – In einer zentralen Zugriffsregel wird definiert, welche Berechtigungen einer Ressource zugewiesen werden.
- Claim Types (Anspruchstyp) – Ein Anspruchstyp kann für einen Benutzer und/oder einen Computer definiert werden. Im Anspruchstyp wird das Active Directory-Attribut definiert, das als Anspruch bei der Anmeldung in das Kerberos-Ticket übernommen wird.
- Resource Properties (Ressourceneigenschaft) – Eine Ressourceneigenschaft beschreibt ein Merkmal einer Ressource (z. B. Datei oder Ordner). Sie wird beim Erstellen zentraler Zugriffsregeln verwendet, um Zielressourcen und Berechtigungen zu definieren, und dient auch zum Klassifizieren von Ressourcen.
- Resource Property Lists (Ressourceneigenschaftenliste) – Eine Ressourceneigenschaftenliste wird verwendet, um Ressourcen zu kategorisieren.

Diese Ansprüche werden nach dem Ausstellen im Kerberos-Ticket hinterlegt und belegen dort Speicher. Ein Kerberos-Ticket darf maximal 64.000 Bytes groß sein. Wenn alle Ihre Clients Windows 8 oder höher ausführen, können Sie die sogenannte *SID-Compression* aktivieren. Dabei werden die Sicherheitskennungen *(Security Identifiers*, SID) komprimiert, sodass mehr Informationen im Ticket hinterlegt werden können.

Kerberos Armoring (bzw. *Flexible Authentication Secure Tunneling*, FAST) ist ein neues Feature, das eine Replay-Attacke auf das Kerberos-Protokoll erschwert bzw. unmöglich macht. FAST bietet ein neues Framework zum Schutz der (Kerberos)-Präauthentifizierung und kann von Clients ab Windows 8 und Domänencontrollern ab Windows Server 2012 verwendet werden. Die Aktivierung erfolgt automatisch, sofern Sie die Unterstützung für Ansprüche aktiviert haben.

Sie können mithilfe von `KList` prüfen, ob FAST aktiviert ist:

```
C:\Users\Peter.Kloep>klist
Aktuelle Anmelde-ID ist 0:0x367af
Zwischengespeicherte Tickets: (2)

#0>     Client: Peter.Kloep @ INTRANET.RHEINWERK-VERLAG.DE
        Server: krbtgt/INTRANET.RHEINWERK-VERLAG.DE @ INTRANET.RHEINWERK-
                VERLAG.DE
        KerbTicket (Verschlüsselungstyp): AES-256-CTS-HMAC-SHA1-96
        Ticketkennzeichen 0x40e10000 -> forwardable renewable initial
                                        pre_authent name_canonicalize
        Startzeit: 2/22/2020 18:18:48 (lokal)
        Endzeit:   2/23/2020 4:18:48 (lokal)
        Erneuerungszeit: 3/1/2020 18:18:48 (lokal)
        Sitzungsschlüsseltyp: AES-256-CTS-HMAC-SHA1-96
        Cachekennzeichen: 0x41 -> PRIMARY FAST
        KDC aufgerufen: PNHN10SDCV00001

#1>     Client: Peter.Kloep @ INTRANET.RHEINWERK-VERLAG.DE
        Server: LDAP/ PNHN10SDCV00001.Intranet.rheinwerk-
                verlag.de/Intranet.rheinwerk-
                verlag.de @ INTRANET.RHEINWERK-VERLAG.DE
        KerbTicket (Verschlüsselungstyp): AES-256-CTS-HMAC-SHA1-96
        Ticketkennzeichen 0x40a50000 -> forwardable renewable pre_authent
                                        ok_as_delegate name_canonicalize
        Startzeit: 2/22/2020 18:18:49 (lokal)
        Endzeit:   2/23/2020 4:18:48 (lokal)
        Erneuerungszeit: 3/1/2020 18:18:48 (lokal)
        Sitzungsschlüsseltyp: AES-256-CTS-HMAC-SHA1-96
        Cachekennzeichen: 0x40 -> FAST
        KDC aufgerufen: PNHN10SDCV00001.Intranet.rheinwerk-verlag.de
```

Listing 4.6 Ausgabe von »KList« mit dem Hinweis, dass FAST verwendet wurde

Der Eintrag unter `Cachekennzeichen` in der Ausgabe von `KList` ist ein Nachweis dafür, dass FAST verwendet wurde.

4.1.9 Sicherheitsrichtlinien

Über Gruppenrichtlinien (für Windows-Clients und -Server) können Sie konfigurieren, welche Authentifizierungsmethoden im Netzwerk verwendet werden sollen (siehe Abbildung 4.20).

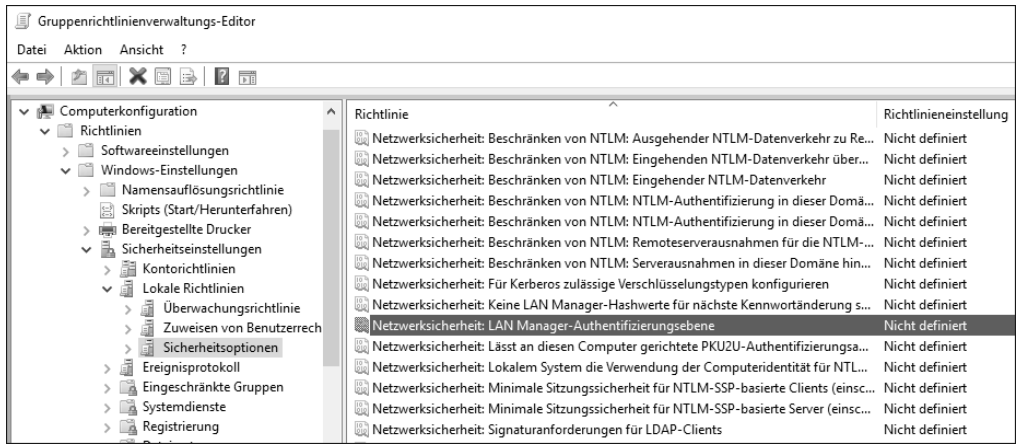


Abbildung 4.20 Konfiguration der »LAN Manager-Authentifizierungsebene«

Microsoft empfiehlt für aktuelle Betriebssysteme die Option NUR NTLMV2-ANTWORTEN SENDEN. LM & NTLM VERWEIGERN (siehe Abbildung 4.21). Diese Einstellung muss bei älteren Clients (vor Windows XP) und bei Drittanbieter-Betriebssystemen und Netzwerkgeräten, die sich an der Domäne anmelden, geprüft werden.

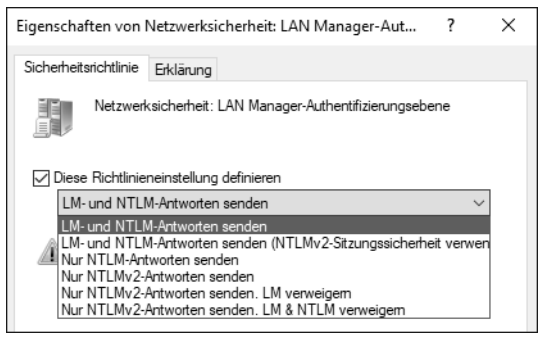


Abbildung 4.21 Auswahlmöglichkeit der »LAN Manager-Authentifizierungsebene«

Die Richtlinie muss für die Domänencontroller und Authentifizierungsclients gesetzt werden, damit alle Systeme die Einstellung erhalten.

Detaillierte Informationen zur Windows-Anmeldung und zur Kerberos-Authentifizierung werden unter anderem auf folgenden Microsoft-Webseiten zur Verfügung gestellt:

- How Interactive Logon Works: *https://technet.microsoft.com/en-us/library/cc780332(WS.10).aspx*
- How Kerberos Works: *https://technet.microsoft.com/en-us/library/cc772815(v=ws.10).aspx*

4.2 Remotezugriffsprotokolle

Remotezugriffsprotokolle werden beim Zugriff über VPN oder WLAN verwendet. Hier stehen meist keine Domänenauthentifizierungsprotokolle zur Verfügung, da in aller Regel kein Domänencontroller über ein öffentliches und unsicheres Netzwerk zur Verfügung steht.

4.2.1 MS-CHAP

MS-Chap ist die Microsoft-Adaption des *Challenge Handshake Authentication Protocol* (CHAP). Die erste Version des MS-CHAP-Protokolls stammt aus Zeiten von Windows NT und Windows 95. MS-CHAP v1 ist eine Umsetzung des Standardprotokolls für DFÜ-Verbindungen (*Einwahl per Modem*), wogegen MS-CHAP v2 für VPN-Verbindungen angepasst wurde. Mit dem Protokoll wird ein *Drei-Wege-Handshake* durchgeführt und eine gegenseitige Authentifizierung (*Mutual Authentication*) durchgeführt.

4.2.2 Password Authentication Protocol (PAP)

Das *Password Authentication Protocol* (Kennwortauthentifizierungsprotokoll) ist ein unsicheres Protokoll, da mit ihm Benutzername und Kennwort unverschlüsselt an den Zielserver übertragen werden. PAP ist vergleichbar mit der Basis-Authentifizierung bei Webserver-Zugriffen. Wenn die Verbindung vor der Authentifizierung nicht verschlüsselt ist, sollte dieses Protokoll nicht verwendet werden, da ein Angreifer die Daten sehr einfach mitlesen könnte.

4.2.3 Extensible Authentication Protocol (EAP)

Das *Extensible Authentication Protocol* ist ein von der Internet Engineering Task Force entwickeltes Authentifizierungsprotokoll, das in den Windows-Betriebssystemen für eine Remotezugriffsauthentifizierung verwendet werden kann. Hierbei stehen in den Windows-Betriebssystemen zwei Varianten zur Verfügung:

- Authentifizierung über Benutzername und Kennwort des Benutzers oder Computers (*Protected EAP*)
- Authentifizierung über Zertifikate (*EAP-TLS*, *Extensible Authentication Protocol – Transport Layer Security*)

4.3 Webzugriffsprotokolle

Für den Zugriff auf Webserver können Sie aus einer Liste von möglichen Authentifizierungsprotokollen wählen. Hier müssen Sie entscheiden, ob Sie eine hohe Kompatibilität zu den verwendeten Browsern haben wollen und bereit sind, eventuell Benutzernamen und Kennwort im Klartext zu übertragen, oder ob Sie sichere Authentifizierungsprotokolle verwenden wollen und dadurch die Verwendung bestimmter Browser ausschließen.

Drei Protokolle möchten wir an dieser Stelle noch erwähnen, die beim Zugriff auf Webdienste – besonders außerhalb der eigenen Umgebung – eine Rolle spielen:

- *SAML* – Das Protokoll *Security Assertion Markup Language* ist ein XML-basiertes Protokoll, mit dem Single Sign-On bei Webdiensten eingerichtet werden kann, auch wenn die Webdienste zu unterschiedlichen Umgebungen gehören. Dabei werden von der ausstellenden Instanz »Aussagen« (*Assertions*) erstellt, die auf Active Directory-Attributen beruhen können. Diese Aussagen werden vom Zielsystem überprüft, bevor das Konto berechtigt wird. Durch die Verwendung des XML-Formats kann SAML plattformübergreifend eingesetzt werden.
- *OAuth2 – Open Authorization 2.0* ist ein Standardprotokoll zur Authentifizierung, das von der Internet Engineering Task Force entwickelt wurde. Die Version 2.0 ersetzt dabei die ältere Version. OAuth wird gerne bei Webdiensten verwendet, die über eine API angesprochen werden können. Hierdurch können Anwendungen (auch Apps auf Mobilgeräten) gesichert auf die Webdienste zugreifen.
- *OpenID Connect* – OpenID Connect ist ein Authentifizierungs-Framework, das aus *OpenID* hervorgegangen ist, einem offenen Protokoll bzw. einer Spezifikation für das Single Sign-On aus dem Jahre 2005. OpenID Connect wurde 2014 veröffentlicht und zeichnet sich durch eine einfachere Umsetzung und Verwendung aus als sein Vorgänger (OpenID). OpenID Connect basiert auf dem Framework von OAuth 2.0 und bietet eine Authentifizierung für eine große Zahl an Webclients.

Kapitel 10

Planung und Konfiguration der Verwaltungssysteme (PAWs)

In diesem Kapitel gehen wir näher auf die Planung und Konfiguration der Verwaltungssysteme ein. Dabei geht es um die Fragen, wo ein Verwaltungssystem stehen soll, welche Ausprägung es haben soll und wie es technisch umgesetzt werden kann.

Eine *Privileged Access Workstation* (PAW) ist ein spezielles Verwaltungssystem, mit dem Sie Ihre Infrastruktur administrieren. Vereinfacht gesagt, ist eine PAW eine gesicherte und gesperrte Arbeitsstation mit privilegiertem Zugriff, die ein Höchstmaß an Sicherheit für sensible Konten und Aufgaben bietet. PAWs empfehlen sich für die Verwaltung von Identitätssystemen und Cloud-Diensten ebenso wie für vertrauliche Geschäftsfunktionen.

Eine PAW darf keinesfalls für »Alltagsaufgaben« im normalen Geschäftsbetrieb Ihres Unternehmens eingesetzt werden, und selbstverständlich ist es auch verboten, damit im Internet den letzten Promiklatsch oder die Bundesliga-Ergebnisse abzurufen. Stattdessen sind PAWs spezielle Arbeitsplätze, die mit großer Sorgfalt gepflegt und eingerichtet werden müssen.

Bei allen Varianten der Absicherung, die wir Ihnen in diesem Kapitel vorstellen wollen, müssen Sie immer zwischen der maximalen Sicherheit und der Umsetzbarkeit in Ihrem Unternehmen abwägen und einen geeigneten Mittelweg finden. Wenn Sie immer die maximale Sicherheit umsetzen wollen, riskieren Sie, dass die Admins nicht mehr richtig oder nur sehr erschwert arbeiten können. Das ist natürlich genauso wenig der richtige Weg wie maximaler Komfort.

Auch während des Betriebs sollten Sie kontinuierlich den sichersten machbaren Weg ermitteln und Ihre Infrastruktur dahin optimieren. Diese Optimierung kann auch mal zulasten der Sicherheit gehen, wenn dadurch die Umsetzung der Verwaltungsaufgaben stark vereinfacht wird. Hier gibt es leider keine allgemeingültige Empfehlung: Schauen Sie, welcher Kompromiss für Ihre Umgebung und die Bedrohungsszenarien, denen Ihr Unternehmen ausgesetzt ist, der richtige ist.

10.1 Wo sollten die Verwaltungssysteme (PAWs) eingesetzt werden?

Generell empfiehlt es sich, so wenige Verwaltungssysteme wie möglich, aber so viele wie nötig zu nutzen. Auf jeder PAW müssen alle notwendigen Verwaltungstools sowie das System aktuell gehalten werden, was bei einer großen Anzahl von Verwaltungssystemen schnell sehr komplex und aufwendig werden kann. In der Praxis haben sich eine Terminalserver-Farm und die Bereitstellung von RemoteApps bewährt. Durch die Verwendung der Terminalserver-Farm können Sie die Verwaltungstools auf wenigen Systemen bereitstellen (natürlich nach Tier-Leveln getrennt), wodurch die Aktualisierung der Tools weniger komplex wird. Ein Beispiel für so eine Terminalserver-Umgebung mit RemoteApps zeigen wir Ihnen in Abschnitt 10.7.

10.1.1 Tier-Level 0 (Domainadministration)

Die administrativen Kennungen des Tier-Levels 0 sind Ihr höchstes Gut und müssen besonders geschützt werden. Daher ist im Tier-Level 0 ein Verwaltungssystem unumgänglich und muss in jedem Fall eingeplant werden, denn es darf keine Anmeldung mit einer Kennung aus dem Tier-Level 0 an einem normalen Arbeitsplatz möglich sein. Im Tier-Level 0 kommen Sie daher nicht um die Implementierung eines Verwaltungssystems herum, außer Sie administrieren Ihre Umgebung mit Tools, die direkt auf den Domänencontrollern bereitgestellt werden. Dies kann aber nur in kleinen Umgebungen umgesetzt werden, da je Windows-Server maximal zwei gleichzeitige Anmeldungen möglich sind. Und wenn Sie Verwaltungswerkzeuge von Drittanbietern benötigen, brauchen Sie auf jeden Fall ein Verwaltungssystem, weil Microsoft die klare Empfehlung ausspricht, keine weitere Software (wie z. B. Virenscanner) außer den bereitgestellten Serververwaltungstools für die Administration der Domäne und unterstützenden Diensten auf den Domänencontrollern zu installieren. Falls Sie doch Software von Drittanbietern auf den Domänencontrollern installieren, erhalten Sie im Fehlerfall eventuell keinen Support mehr durch den Hersteller.

Ob Sie die Verwaltungstools auf einem Terminalserver oder auf einer PAW bereitstellen, bleibt Ihnen überlassen und ist von Ihrer Umgebung abhängig. Haben Sie z. B. Standorte, von denen aus die Terminalserver zeitweise nicht erreichbar sind, an denen aber Sie trotzdem administrative Tätigkeiten ausführen müssen, können Sie die Verwaltungstools nur lokal auf dem Verwaltungssystem verfügbar halten.

Die Verwaltungssysteme des Tier-Levels 0 sollten niemals Zugriff auf das Internet haben. Selbst wenn Sie das Active Directory zusammen mit einem Azure-AD synchronisieren, sollten für die Verwaltungssysteme des Azure-AD eigene *Cloud-PAWs* bereitgestellt werden. Darauf gehen wir in Abschnitt 10.5 in »PAW für Azure AD« noch genauer ein.

10.1.2 Tier-Level 1 (zugewiesene Rechte auf den DCs am Standort)

Im Tier-Level 1 brauchen Sie aufgrund des Aufgabenbereiches nicht zwingend ein Verwaltungssystem. Die administrativen Kennungen werden zur Installation der Windows-Updates, zum Neustart der Domänencontroller, zur Datensicherung sowie zum Beheben von kleinen Fehlern verwendet. Diese Schritte können alle direkt auf dem Domänencontroller ausgeführt werden.

Nur wenn Sie in großen Umgebungen die Logs der Ereignisanzeige durch die Administratoren des Tier-Levels 1 auswerten lassen wollen, benötigen Sie ein Verwaltungssystem, auf dem sich der jeweilige Benutzer anmelden und dann auf die Logs zugreifen kann. Eine Alternative dazu ist das zentrale Sammeln der Logs auf einer Netzwerkfreigabe, da dann z. B. auch eine Kennung aus dem Tier-Level 2 mit lesenden Rechten ausgestattet und ein Verwaltungssystem des Tier-Levels 2 genutzt werden könnte.

10.1.3 Tier-Level 2 (Serversysteme und Serveranwendungen)

Im Tier-Level 2 ist nicht für jede Arbeit ein Verwaltungssystem notwendig. Hier sollten Sie genau planen und sich eine Übersicht erstellen, für welche administrativen Tätigkeiten der Umweg über ein Verwaltungssystem nötig oder sinnvoll ist.

Tabelle 10.1 zeigt Ihnen ein mögliches Beispiel für eine solche Planung, die wir sinnvoll finden. Auf dieser Basis könnten Sie sich eine eigene Übersicht über die benötigen Verwaltungssysteme und Tools erstellen.

Anwendung	PAW (ja/nicht zwingend)	Tools	Begründung
Exchange	Ja	AD-Benutzer und -Computer, Verwaltungskonsole des Exchange-Servers	Verwaltung der Rechte von vielen Benutzerobjekten
Datenbanken	Ja	SQL-Server Management-studio, Datenbank-entwicklungstools	Verwaltung von Datenbanken, mit teils kritischen Unternehmens-daten
Serveradminis-trator (Support Betriebssysteme)	Nicht zwingend		Administration der Server direkt über das Betriebssystem

Tabelle 10.1 Die benötigten Verwaltungssysteme im Tier-Level 2

Anwendung	PAW (ja/nicht zwingend)	Tools	Begründung
DHCP, Druck-Server, WSUS	Nicht zwingend, kann per RDS erfolgen	Verwaltungs-konsolen der Serverdienste	Die Administration kann je nach Größe lokal auf dem Server oder per RDS erfolgen.

Tabelle 10.1 Die benötigten Verwaltungssysteme im Tier-Level 2 (Forts.)

Wenn Sie nur eine kleine Umgebung administrieren, benötigen Sie für die Serveradministration nicht zwingend ein Verwaltungssystem. In größeren Umgebungen ist es jedoch empfehlenswert, Verwaltungssysteme zu implementieren, weil dort weitreichendere administrative Zugänge benötigt werden. Die Administration wäre sonst sehr erschwert und das Netzwerk könnte nicht gut geschützt werden, da die Server aus zu vielen Subnetzen mit zu vielen offenen Ports erreichbar sein müssten.

10.1.4 Tier-Level 3 (Administration der normalen Arbeitsplatzcomputer)

Im Tier-Level 3 wird grundsätzlich kein PAW benötigt, denn im Tier-Level 3 befinden sich die Administratoren der normalen Arbeitsplatzcomputer. Diese haben sowieso lokale Adminrechte. Wenn die Administratoren des Tier-Levels 3 Tools für ihre administrativen Arbeiten benötigen, können diese über einen Terminalserver im genannten Tier-Level bereitgestellt werden. In sehr kleinen Umgebungen können die Verwaltungstools auch direkt auf dem Arbeitsplatzcomputer des Administrators installiert und über die Funktion AUSFÜHREN ALS gestartet werden.

Dieser Vorschlag gilt aber wirklich nur für sehr kleine Umgebungen. Ansonsten sollte immer die Bereitstellung der RemoteApps genutzt werden, die wir Ihnen in Abschnitt 10.7 vorstellen – vorausgesetzt, die Anbindung an die Terminalserver ist immer gewährleistet. Das ist der einfachste Weg, mit dem Sie immer die aktuellen Verwaltungstools mit der gleichen Konfiguration nutzen können.

LAPS

Für die Administration der normalen Arbeitsplatzcomputer und die lokale Anmeldung an diesen sollte immer die von LAPS verwaltete administrative Kennung genutzt werden, die wir Ihnen in Abschnitt 11.1 vorstellen werden. Die von LAPS verwaltete Kennung hat auf jedem Arbeitsplatz ein anderes Kennwort und kann sehr schnell zurückgesetzt werden. Hier ist das Ausspähen des Kennwortes für die anderen Systeme des gleichen Tier-Levels weniger problematisch, da die Kennwörter zeitnah gewechselt werden.

10.2 Dokumentation der ausgebrachten Verwaltungssysteme

Ein weiterer sehr wichtiger Aspekt, dem Sie genauso viel Aufmerksamkeit und Sorgfalt wie der Einrichtung widmen sollten, ist die Dokumentation Ihrer Verwaltungssysteme. Sie sollten mindestens die folgenden Punkte in einer Liste nachhalten. Die genauen Angaben können bei Ihnen natürlich variieren und müssen an Ihre Umgebung angepasst werden.

- Welche PAWs gibt es in welchen Tier-Leveln?
- Von wem werden diese genutzt?
- Welche Dienste werden damit administriert?
- Wie sieht die Netzwerkkartenkonfiguration mit den verwendeten VLANs aus?
- Wie wurden die Firewalls für die Verwaltungssysteme implementiert, und welche Freigaben gibt es?
- Welche Verwaltungstools sind freigegeben und installiert?
- In welchen externen Systemen wurden die Verwaltungssysteme freigegeben?

10.3 Wie werden die Verwaltungssysteme bereitgestellt?

Falls Ihre Umgebung komplex ist und sich über viele Standorte erstreckt und daher viele Verwaltungssysteme vorhanden sind und eine Terminalserver-Umgebung nicht genutzt werden kann, dann sollten die Verwaltungssysteme über ein automatisches Deployment z. B. per *Microsoft Deployment Toolkit* (MDT) bereitgestellt werden. Wenn Sie die Verwaltungssysteme über ein solches Deployment bereitstellen, haben alle Systeme immer den gleichen Stand und können turnusgemäß immer wieder aktualisiert werden. Außerdem besteht im Fehlerfall der Vorteil, dass die Verwaltungssysteme automatisiert neu installiert werden können und mit den notwendigen administrativen Tools schnell wieder verfügbar sind.

Wenn die Verwaltungssysteme virtuell bereitgestellt werden, sollte immer eine Vorlage der virtuellen Maschine mit den notwendigen Verwaltungstools in der aktuellen Version vorhanden sein. Über diese Vorlage kann die neue virtuelle Maschine in Minuten neu bereitgestellt werden. Die Virtualisierungsplattform sollte redundant und ausfallsicher konfiguriert sein.

Falls Sie die Verwaltungstools per *RemoteApps* auf einer Terminalserver-Umgebung bereitstellen, sollten auch diese redundant und ausfallsicher sein. Denken Sie immer daran: Wenn Ihre Terminalserver-Umgebung nicht erreichbar ist, dann sind die zentral bereitgestellten Verwaltungstools nicht mehr verfügbar. Die Redundanz einer Terminalserver-Umgebung kann entweder auf einer hoch verfügbaren Virtualisierungsplattform oder über eine Terminalserver-Farm bereitgestellt werden.

Eine Terminalserver-Farm besteht dann aus mehreren Terminalservern, die auf unterschiedliche Standorte verteilt sind.

10.4 Zugriff auf die Verwaltungssysteme

Auch der Zugriff auf die PAWs bedarf einiger Sicherheits- und Schutzmaßnahmen, um die vorhandenen Verwaltungssysteme abzusichern. Die von uns genannten Maßnahmen sind auch in kleinen Umgebungen einfach zu implementieren und somit schnell einsetzbar.

10.4.1 Restricted Adminmode (eingeschränkter Admin-Modus)

Der *Restricted Adminmode* wurde bereits mit Windows Server 2012 eingeführt. Er bietet eine Methode zur interaktiven Anmeldung bei einem Remote-Host-Server, ohne dass Ihre Anmeldedaten an den Server übertragen werden müssen. Dadurch wird verhindert, dass Ihre Anmeldedaten während des Anmeldeprozesses gesammelt werden können, falls das Zielsystem kompromittiert wurde. In diesem Modus werden zu keinem Zeitpunkt Klartextpasswörter oder andere wiederverwendbare Formen von Anmeldeinformationen an das Zielsystem gesendet.

Bei Verwendung dieses Modus versucht der Remote-Desktop-Client sich interaktiv bei einem Host anzumelden, der diesen Modus ebenfalls unterstützt, ohne Ihre Berechtigungsnachweise zu senden. Wenn das Zielsystem überprüft, dass das administrative Konto, das sich mit ihm verbindet, Administratorrechte besitzt und den Modus *Restricted Adminmode* unterstützt, ist die Verbindung erfolgreich. Andernfalls schlägt der Verbindungsversuch fehl.

Der *Restricted Adminmode* hat den klaren Nachteil, dass die verwendete administrative Kennung, die für die Anmeldung genutzt wird, über Adminrechte auf dem Zielsystem verfügen muss. Aufgrund unserer Empfehlung, dass die administrativen Kennungen keine administrativen Rechte auf dem Zielsystem haben sollen, können wir diese Maßnahme nur dann empfehlen, wenn die administrativen Kennungen aufgrund der notwendigen Verwaltungstools sowieso administrative Rechte auf dem Zielsystem haben.

Aktivierung des Restricted Adminmode auf einem Zielsystem

Die Aktivierung des Restricted Adminmode bei den Zielsystemen erfolgt über eine Einstellung in der Registry:

1. Öffnen Sie den Registrierungs-Editor.
2. Im Registrierungs-Editor wechseln in den Schlüssel *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa* (siehe Abbildung 10.1).

3. Falls es noch nicht vorhanden ist, erstellen Sie das REG-DWORD `DisableRestrictedAdmin`.
4. Weisen Sie durch einen Doppelklick auf `DisableRestrictedAdmin` dem REG-DWORD den Wert `0` zu. Der Restricted Adminmode wird so aktiviert.

Der Restricted Adminmode ist direkt aktiv, das Zielsystem muss nicht neu gestartet werden. Wenn Sie die Unterstützung deaktivieren wollen, müssen Sie dem REG-DWORD `DisableRestrictedAdmin` den Wert `1` zuweisen.

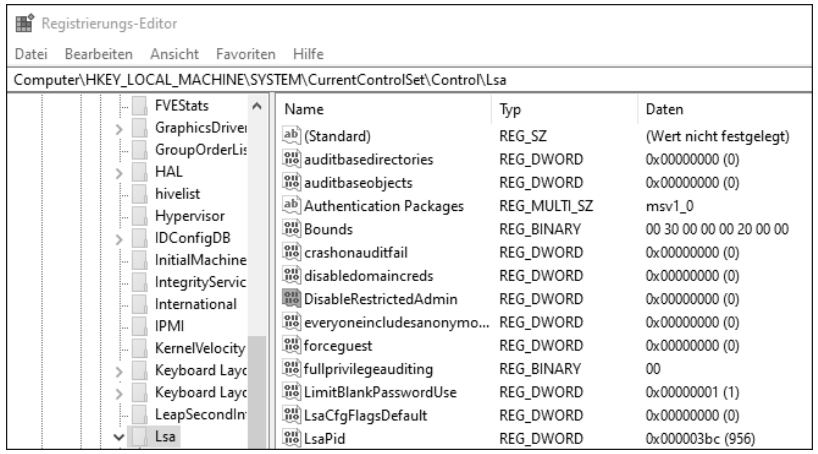


Abbildung 10.1 Der Registrierungs-Editor mit dem REG_DWORD »DisableRestrictedAdmin«

Den Restricted Adminmode für alle ausgehenden Remotedesktopverbindungen festlegen

Über die Gruppenrichtlinieneinstellung können Sie die Verwendung des Restricted Adminmode für alle ausgehenden Verbindungen festlegen:

1. Öffnen Sie die Gruppenrichtlinienverwaltungskonsole, indem Sie auf Start klicken. Geben Sie *gpmc.msc* ein, und klicken Sie dann auf das angezeigte Suchergebnis.
2. Wählen Sie unter den Gruppenrichtlinienobjekten diejenige Gruppenrichtlinie aus, die mit der Organisationseinheit verknüpft ist, in der die Systeme vorhanden sind, von denen aus Sie die Remotedesktopverbindungen initiieren wollen. Ist noch keine Gruppenrichtlinie vorhanden, muss diese neu erstellt werden.
3. Klicken Sie mit der rechten Maustaste auf die Gruppenrichtlinie, und wählen Sie Bearbeiten aus.
4. Navigieren Sie zu dem Punkt Computerkonfiguration • Richtlinien • Administrative Vorlagen • System • Delegierung von Anmeldeinformationen.
5. Stellen Sie den Status von Delegierung von Anmeldeinformationen an Remoteserver einschränken auf Aktiviert, und ändern Sie die Option auf Eingeschränkte Verwaltung anfordern.

Die neue Einstellung der Gruppenrichtlinie wird erst wirksam, wenn die Gruppenrichtlinie übernommen wird. Damit die Gruppenrichtlinie sofort übernommen wird, öffnen Sie eine administrative Eingabeaufforderung und geben folgenden Befehl ein:

```
gpupdate /force /target:Computer
```

Wenn Sie nun im Restricted Adminmode eine Verbindung zum Zielsystem aufbauen, verwenden Sie hinter dem Befehl `mstsc.exe` den Schalter `/RestrictedAdmin`. Sie können, wenn Sie eine Verbindung immer im Restricted Adminmode starten wollen, z. B. auf dem Desktop eine Verknüpfung mit den Eigenschaften speichern.

Restricted Adminmode und Remotedesktopverbindung

Auch bei einer Remotedesktopverbindung im Restricted Adminmode ist es möglich, über die Funktion Ausführen als den Nutzer zu wechseln.

10.4.2 Windows Defender Remote Credential Guard

Der *Windows Defender Remote Credential Guard* ist der Nachfolger des Restricted Adminmode. Für diese Variante sind keine administrativen Berechtigungen mehr auf dem Zielsystem notwendig, und deswegen ist unsere klare Empfehlung, ihn zu nutzen.

Allerdings gibt es auch einen kleinen Nachteil: Beim Windows Defender Remote Credential Guard gibt es keine Möglichkeit mehr, die Funktion Ausführen als zu nutzen. Es wird immer die lokale Anmeldung des Quellsystems genutzt und direkt an das Zielsystem übergeben, also ein *Single Sign-On* durchgeführt. Das bedeutet auch, dass diese Variante immer nur von einem Verwaltungssystem aus dem gleichen Tier-Level genutzt werden kann, da Sie sonst nicht über ausreichende Berechtigungen verfügen.

Voraussetzungen für den Windows Defender Remote Credential Guard

Der Remotedesktopclient muss folgende Voraussetzungen erfüllen:

- Sie brauchen mindestens Windows 10 in der Version 1703.
- Es muss der klassische RDP-Client genutzt werden; die universelle Windows-App unterstützt diesen noch nicht.
- Die Kerberos-Authentifizierung muss genutzt werden: Erreicht der RDP-Client keinen DC, wird dieser einen Verbindungsversuch mit NTLM starten. NTLM wird vom Windows Defender Remote Credential Guard aber nicht unterstützt.

Der Remotedesktop-Host muss folgende Voraussetzungen erfüllen:

- Sie brauchen mindestens Windows 10 in der Version 1607 oder Windows Server 2016.

- Der Restricted Adminmode muss unterstützt werden.
- Das administrative Benutzerkonto muss über Anmelderechte auf dem Zielsystem verfügen.
- Das Zielsystem muss die Delegierung von nicht exportierbaren Anmeldeinformationen zulassen.

Der Windows Defender Remote Credential Guard kann sowohl On-Premise als auch in Azure genutzt werden. Wie der Restricted Adminmode aktiviert wird, haben wir Ihnen bereits im vorigen Abschnitt erläutert. Die Aktivierung des Credential Guards erfolgt vergleichbar.

Den Windows Defender Remote Credential Guard für alle ausgehenden Remotedesktopverbindungen festlegen

Mit der folgenden Gruppenrichtlinieneinstellung können Sie die Verwendung des *Windows Defender Remote Credential Guard* für alle ausgehenden Verbindungen festlegen:

1. Öffnen Sie die Gruppenrichtlinienverwaltungskonsole, indem Sie auf Start klicken. Geben Sie *gpmc.msc* ein, und klicken Sie dann auf das angezeigte Suchergebnis.
2. Wählen Sie unter den Gruppenrichtlinienobjekten die Gruppenrichtlinie aus, die mit der Organisationseinheit verknüpft ist, in der die Systeme vorhanden sind, von denen aus Sie die Remotedesktopverbindungen initiieren wollen. Ist noch keine Gruppenrichtlinie vorhanden, müssen Sie diese neu erstellen.
3. Klicken Sie mit der rechten Maustaste auf die Gruppenrichtlinie, und wählen Sie Bearbeiten aus.
4. Navigieren Sie zum Punkt Computerkonfiguration • Richtlinien • Administrative Vorlagen • System • Delegierung von Anmeldeinformationen.
5. Stellen Sie den Status der Option Delegierung von Anmeldeinformationen an Remoteserver einschränken auf Aktiviert, und ändern Sie den Wert auf Remote Credential Guard anfordern.

Die neue Einstellung der Gruppenrichtlinie wird erst wirksam, wenn die Gruppenrichtlinie übernommen wurde. Damit die Gruppenrichtlinie sofort übernommen wird, öffnen Sie eine administrative Eingabeaufforderung und geben den folgenden Befehl ein:

```
gpupdate /force /target:Computer
```

Wenn Sie nun mithilfe des Windows Defender Remote Credential Guard eine Verbindung zum Zielsystem aufbauen, verwenden Sie hinter dem Befehl `mstsc.exe` den Schalter `/remoteguard`. Sie können, wenn Sie eine Verbindung immer mithilfe des

Windows Defender Remote Credential Guard starten wollen, z. B. auf dem Desktop eine Verknüpfung mit den Eigenschaften speichern.

Beim Verbindungsaufbau zum Zielsystem werden die Anmeldedaten direkt übergeben und können während der aktiven Verbindung auch bei einem Zugriff auf weitere Systeme genutzt werden. Wird die RDP-Verbindung beendet, sind die Anmeldeinformationen auf dem RDP-Host nicht mehr verfügbar.

Wenn Sie eine RDP-Verbindung zu einem Zielsystem aufbauen, auf dem der Restricted Adminmode nicht aktiviert ist, wird die Fehlermeldung aus Abbildung 10.2 angezeigt.

Abbildung 10.2 Diese Fehlermeldung erscheint beim Versuch, eine Remote-Credential-Guard-RDP-Verbindung zu einem Zielsystem aufzubauen, auf dem der Restricted Adminmode nicht aktiv ist.

10.5 Design der Verwaltungssysteme

Beim Einsatz von PAWs empfiehlt Microsoft, immer das aktuellste und sicherste verfügbare Betriebssystem in der Edition *Enterprise* zu nutzen, denn in der Enterprise-Edition sind mehrere zusätzliche Sicherheitsfeatures enthalten, die in anderen Editionen fehlen, z. B. der *Credential Guard* und der *Device Guard*. Falls in Ihrem Unternehmen keine Windows-10-Enterprise-Lizenzen vorhanden sind, sollte *Windows 10 Pro* zum Einsatz kommen. Diese Edition enthält viele der wichtigen grundlegenden Technologien, z. B. vertrauenswürdiger Start, BitLocker und Remotedesktop.

Bei der Einrichtung der PAWs müssen Sie eine Entscheidung treffen: Soll der Arbeitsplatz auf dedizierter Hardware oder virtuell auf einem vorhandenen Arbeitsplatzcomputer bereitgestellt werden? Mit *dedizierter Hardware* meinen wir ein separates Gerät, das dann ausschließlich für die administrativen Aufgaben genutzt wird. Alternativ können Sie auch einen Rechner gleichzeitig als Arbeitsplatzcomputer und als PAW verwenden. Dann wird die PAW auf dem physikalischen Gerät installiert und der Arbeitsplatzcomputer virtualisiert.

Beide Varianten haben ihre Vor- und Nachteile, die wir in Tabelle 10.2 und Tabelle 10.3 kurz darstellen wollen.

Vorteile einer dedizierten Hardware	Nachteile einer dedizierten Hardware
Strikteste Trennung aus Sicherheitssicht	Zusätzliche Kosten für die Hardware und Lizenzen sowie für Zugriffslizenzen
Die Vertraulichkeit der Aufgaben wird als sehr hoch eingeschätzt.	Zusätzliches Gewicht und erhöhter Platzbedarf bei der Remotearbeit: Sie tragen im Zweifelsfall zwei Laptops mit sich herum.

Tabelle 10.2 Vor- und Nachteile der dedizierten Hardware

Vorteile gleichzeitiger Verwendung	Nachteile gleichzeitiger Verwendung
Geringere Kosten für die Hardware	Die gleiche Peripherie birgt eine erhöhte Gefahr (z. B. Keylogger).
Es wird nur ein Gerät benötigt.	
Das Verwaltungssystem ist immer verfügbar.	

Tabelle 10.3 Vor- und Nachteile der gleichzeitigen Verwendung

Es gibt noch eine dritte Variante, bei der der Arbeitsplatzcomputer virtuell auf einem Hyper-V-Server bereitgestellt wird. Dabei ist aber kein Offlinebetrieb möglich. Alle drei Varianten werden wir in den folgenden Abschnitten etwas näher erläutern.

Dedizierte PAW für die Verwaltungsaufgaben

Sie können eine dedizierte PAW nutzen. Bei dieser Variante werden Rechner als PAWs für alle Verwaltungsaufgaben in dem jeweiligen Tier-Level benötigt. Alle normalen Aufgaben, wie E-Mail- und die Dokumentenbearbeitung, müssen auf anderen Rechnern durchgeführt werden.

Durch diese Variante können die Netzwerksegmente am einfachsten voneinander getrennt werden und Sie können die Firewallregeln so strikt wie möglich definieren. Außerdem hat diese Variante einen besonderen psychologischen Vorteil: Wir haben schon oft die Erfahrung gemacht, dass auf diese Weise schnell die Wichtigkeit der Verwaltungsaufgaben erkennbar wird. Wenn der Arbeitsplatz gewechselt werden muss und ein anderer Rechner genutzt wird, auf dem es keine Ablenkung durch Mails und Social Media gibt, werden komplizierte Aufgaben mit höherer Konzentration angegangen.

Im Tier-Level 0 sollten Sie, wenn Ihre Umgebung keine andere sichere Variante zulässt, immer auf eine dedizierte PAW setzen und diese für die Administratoren bereitstellen, da sich dort ja die unternehmenskritischsten Systeme befinden, die vor jeder Angriffsart mit der höchstmöglichen Sicherheitsvariante geschützt werden sollten.

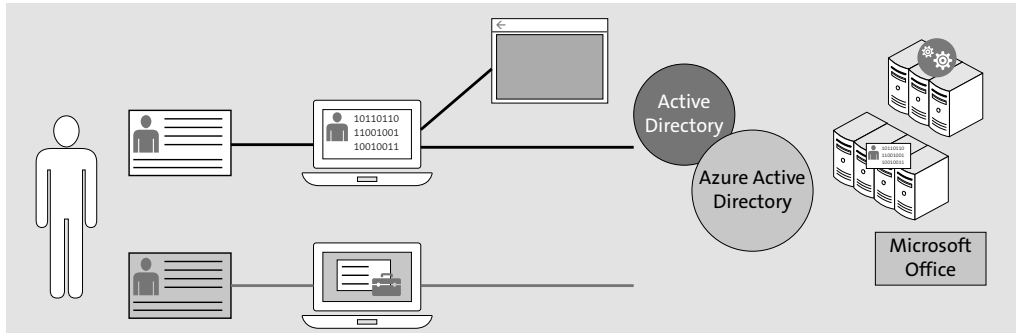


Abbildung 10.3 Dedizierte Hardware für einen Nutzer

Gleichzeitige Verwendung auf einer Hardware

Bei der gleichzeitigen Verwendung einer Hardware wird die PAW direkt auf der Hardware installiert und der normale Arbeitsplatzcomputer wird dann virtualisiert über beispielsweise Hyper-V zur Verfügung gestellt. Die normalen Aufgaben wie Dokumentbearbeitung oder E-Mail-Kommunikation werden in der virtuellen Maschine erledigt. Die Verwaltungsaufgaben werden ausschließlich auf dem physikalisch installierten Betriebssystem durchgeführt.

Die virtuelle Maschine kann direkt mit einem Unternehmensimage installiert werden und unterliegt nicht den Einschränkungen der PAW. Diese Möglichkeit hat den großen Vorteil, dass beide Umgebungen immer offline verfügbar sind. Sie kann, wenn der mobile Einsatz berücksichtigt wurde, jederzeit genutzt werden.

Wenn Sie auf Ihrem Rechner nur eine Netzwerkschnittstelle zur Verfügung haben, sollte auf dem Switch eine dynamische VLAN-Steuerung (z. B. mit einem RADIUS-Server) implementiert werden. Wie das funktioniert, erläutern wir in Abschnitt 16.6.1.

Ist die dynamische VLAN-Steuerung nicht möglich, sollte dieses Szenario nur auf einem Computer mit mehreren Netzwerkkarten bzw. auf mobilen Geräten mit externen Netzwerkadaptern angewendet werden. Nur so können die empfohlenen Firewalleinstellungen angewendet werden.

Nutzen Sie keine virtualisierten PAWs!

Der Ansatz, dass der Arbeitsplatzcomputer auf dem physikalischen Gerät und die PAW als VM bereitgestellt wird, weist eine bedenkliche Sicherheitslücke auf und sollte daher nicht genutzt werden.

Die Sicherheit einer virtuellen PAW ist vom installierten Betriebssystem des Arbeitsplatzcomputers abhängig. In einer sicheren PAW-Architektur ist es nicht zu empfehlen, einen virtuellen Verwaltungscomputer auf einem Arbeitsplatzcomputer zu hosten. Auf einer physischen PAW kann aber ein virtueller Arbeitsplatzcomputer mit einem standardmäßigen Unternehmensimage gehostet werden, um für die Mitarbeiter nur einen Computer für alle Aufgaben bereitstellen zu können.

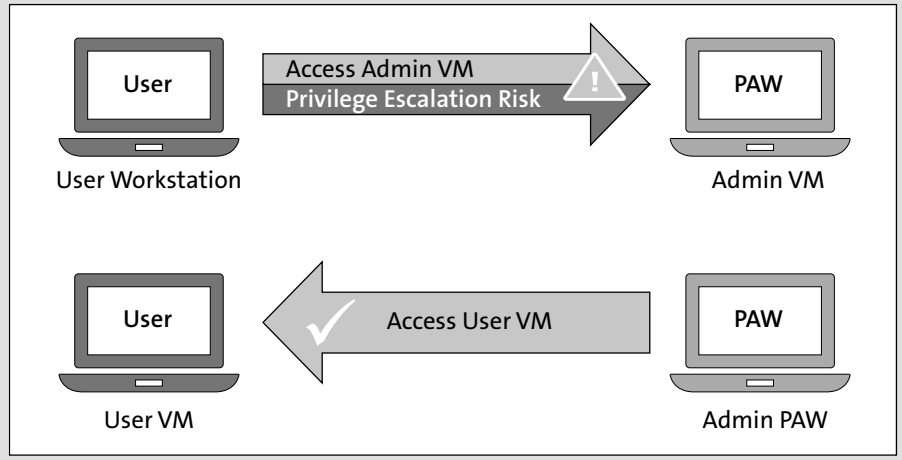


Abbildung 10.4 Sicherheitslücke bei einer virtualisierten PAW

PAW- und Terminalserver-Lösung mit virtuellen Arbeitsplatzcomputern

Wenn Sie über eine Terminalserver-Infrastruktur verfügen, bietet sich die Möglichkeit, einen einzigen Computer sowohl für die Verwaltungsaufgaben als auch für allgemeine Aktivitäten zu verwenden.

Bei dieser Variante werden die Arbeitsplatzcomputer zentral (z. B. in einem Rechenzentrum) bereitgestellt und verwaltet, sind aber offline nicht verfügbar. Auf der physischen Hardware wird das PAW-Betriebssystem für die Verwaltungsaufgaben installiert und genutzt. Für die allgemeinen Aufgaben (wie E-Mail und Dokumentbearbeitung) wird eine Remotedesktopverbindung zu einer virtuellen Maschine her-

gestellt, die auf einem Terminalserver bereitgestellt wird. In den Remotebetriebssystemen unterliegen die Anwendungen dann nicht den Einschränkungen des PAW-Hosts.

Arbeitsplatzcomputer und RemoteApps für die Verwaltungsaufgaben

Wenn Sie eine große Umgebung administrieren und außer im Tier-Level 0 keine dedizierten PAWs bereitstellen müssen und nur einheitliche Arbeitsplatzcomputer beschaffen wollen, dann hat sich in der Praxis die Bereitstellung der administrativen Werkzeuge per RemoteApps auf einem Terminalserver durchgesetzt.

Der normale Arbeitsplatzcomputer kann immer gleich ausgestattet sein – es ist keine leistungsfähige Hardware notwendig. Sie können außerdem das Image nutzen, das auch sonst in Ihrem Unternehmen verwendet wird, und müssen keine besondere Konfiguration pflegen. Alle administrativen Werkzeuge können über eine Terminalserver-Umgebung bereitgestellt werden. Eine Administration ist dann aber immer nur online möglich und kann bei einem Offline-Szenario nicht umgesetzt werden. Dies sollten Sie bei dieser Variante immer bedenken. Spielen Sie gegebenenfalls Notfallszenarien durch, in denen ein Ausfall des Netzwerks vorkommt.

Azure-Administration mit PAW

Falls Sie in Ihrer Umgebung eine PAW für die Verwaltung der in Azure bereitgestellten Dienste, z. B. Azure AD, benötigen, dann sollten Sie diese automatisiert installieren, aber nicht in die Domäne aufnehmen. Dazu können Sie z. B. *MDT* oder *Intune* nutzen.

Dieser PAW muss der Zugriff auf das Internet ermöglicht werden. Durch den direkten Internetzugriff sind die PAWs dann angreifbarer als alle anderen Verwaltungssysteme und sollten von der Domäne und dem sonstigen Netzwerk getrennt administriert werden. Von diesen PAWs aus sollte auch kein Zugriff auf die virtuellen Arbeitsplatzcomputer oder sonstige Komponenten im internen Netzwerk möglich sein.

10.6 Anbindung der Verwaltungssysteme

Bei der Auswahl der Anbindung der PAWs kommt es darauf an, welche Variante Sie angewendet haben. Wir werden Ihnen für jede in Abschnitt 10.5 beschriebene Möglichkeit eine Anbindungsvariante aufzeigen und kurz erläutern. Ins Detail können wir aufgrund der unterschiedlichen Firewallsysteme, Switches und Router natürlich nicht gehen, und wir werden die unterschiedlichen Absicherungsvarianten auch nur allgemein beschreiben. Wie diese dann umgesetzt werden, kommt auf das jeweils genutzte System und auf Ihre Netzwerkkomponenten an. Hier gilt mal wieder, dass

gute Planung sehr wichtig ist und dem Kopfzerbrechen bei der Umsetzung vorbeugen kann.

Bei allen Möglichkeiten sollten Sie auf jeden Fall den Remotedesktop-Zugriff aus allen Nicht-Verwaltungsnetzen sperren, und zwar nach Tier-Leveln getrennt. So kann kein Arbeitsplatzcomputer einen Remotedesktopzugriff erfolgreich aufbauen und sich somit nicht mit einer eventuell kompromittierten Kennung an einem Server anmelden. Die Absicherung der unterschiedlichen Tier-Level wird bei allen Varianten natürlich vorausgesetzt und sollte immer als Erstes umgesetzt werden.

Dedizierte PAW für die Verwaltungsaufgaben

Bei der dedizierten PAW kann die Netzwerksicherheit am einfachsten umgesetzt werden. In jeden Tier-Level sollte es für die PAWs immer mindestens einen getrennten Netzbereich (*VLAN*) geben. Wenn Sie die Sicherheit erhöhen wollen, können Sie für den Administrationsbereich ein getrenntes Netz konfigurieren. Alle Firewallsysteme können auch sehr einfach konfiguriert werden, da genau bekannt ist, welche Netze und Ports ein- und ausgehend freigegeben werden müssen. Ein Zugriff auf die PAWs kann bereits an der ersten Firewallkomponente unterbunden werden. So sind die Systeme sehr gut geschützt und ein Zugriff von außen wird erschwert.

Eine weitere Steigerung der Sicherheit ist der Einsatz eines RADIUS-Servers, der die Verbindung in das Subnetz nur dann zulässt, wenn das System sich an ihm authentifizieren kann. Ist die Authentifizierung nicht erfolgreich, wird die PAW in ein Quarantänenetzwerk umgeleitet, und der Zugriff ist somit gesperrt.

Gleichzeitige Verwendung auf einem Rechner

Bei einer gleichzeitigen Verwendung der Hardware kommt es darauf an, ob Sie eine zweite Netzwerkkarte bereitstellen können. Falls eine weitere Netzwerkkarte vorhanden ist, können Sie dem virtuellen Arbeitsplatzcomputer im Hypervisor eine eigene Netzwerkkarte zuweisen und somit die Netzwerksicherheit erhöhen. Für das physische System (also die PAW) gelten dann die gleichen Regeln wie für eine dedizierte PAW.

Kann keine weitere Netzwerkkarte bereitgestellt werden, ist der Einsatz dieser Variante im Tier-Level 0 nicht empfehlenswert. Beide Systeme würden dann im selben Subnetz arbeiten, sodass sich ein Angreifer sehr schnell Zugang zu den Komponenten im Tier-Level 0 verschaffen könnte.

In den restlichen Tier-Leveln könnten Sie ebenfalls eine RADIUS-Authentifizierung und die dynamische VLAN-Steuerung umsetzen. Das bedeutet: Wenn sich die PAW am RADIUS-Server authentifiziert, wird das VLAN des Verwaltungsnetzwerks zugewiesen. Demensprechend wird, wenn der virtuelle Arbeitsplatzcomputer denselben Vorgang durchführt, diesem das Netzwerk für Arbeitsplatzcomputer zugewiesen.

Wie Sie dynamische VLAN-Steuerung an einem RADIUS-Server konfigurieren, erläutern wir in Abschnitt 16.6. Für die Implementierung der virtuellen VLAN-Steuerung muss der Hypervisor die VLAN-IDs an die Netzwerkschnittstellen der virtuellen Systeme übergeben können.

PAW- und Terminalserver-Lösung mit virtuellen Arbeitsplatzcomputern

Bei dieser Möglichkeit können Sie ebenfalls wie in Abschnitt »Dedizierte PAW für die Verwaltungsaufgaben« verfahren, müssen aber den Zugriff auf den virtuell bereitgestellten Arbeitsplatzcomputer ermöglichen. Ein Zugriff auf die PAW muss in jedem Fall unterbunden werden.

Denken Sie hier immer daran, dass der Offlinezugriff auf den Arbeitsplatzcomputer nicht ermöglicht werden kann. Außerdem muss eine Anmeldung mit der administrativen Kennung am Hypervisor ebenfalls unterbunden werden.

Arbeitsplatzcomputer und RemoteApps für die Verwaltungsaufgaben

Wenn Sie nur normale Arbeitsplatzcomputer in Ihrem Unternehmen einsetzen, kann das gesamte Netzwerk gleich gesichert werden und Sie müssen keine speziellen erweiterten Sicherheitsmaßnahmen umsetzen. Das gesamte Netzwerk wird über mindestens eine Firewall geschützt, und alle Systeme können auf alle notwendigen Komponenten zugreifen. Die Terminalserver-Umgebung wird getrennt betrachtet und extra geschützt.

Ein Zugriff auf die RemoteApps, die auf getrennten Servern für jeden Tier-Level bereitgehalten werden, wird immer nur den Systemen gewährt, die diese auch für die Verwaltungsaufgaben benötigen. Allen anderen Systemen wird der Zugriff verboten. Eine Speicherung der Kennung, die sich an dem Terminalserver anmeldet, sollte nicht möglich sein und bei jeder Verbindung neu abgefragt werden. Ebenfalls sollte die aktive Sitzung nach einer definierten inaktiven Zeitspanne gesperrt werden.

PAW für Azure AD

Die PAWs, die für die Verwaltung der in Azure bereitgestellten Dienste genutzt werden, sollten immer von den anderen Komponenten im Unternehmensnetzwerk getrennt werden. Hier sollten eigene VLANs – wenn möglich sogar dedizierte Netzwerkkomponenten – bis zum Internetzugang genutzt werden. Eine VLAN-Trennung auf derselben Netzwerkkomponente kann im Angriffsfall ausgenutzt werden. Der Zugriff auf die anderen Komponenten im Netzwerk kann dann nicht mehr geschützt werden.

10.7 Bereitstellung von RemoteApps über eine Terminalserver-Farm im Tier-Level 0

In diesem Abschnitt zeigen wir Ihnen an einem Beispiel, wie Sie eine RemoteApp auf einer vorhandenen Terminalserver-Umgebung bereitstellen. Für die Bereitstellung wird eine funktionstüchtige Terminalserver-Umgebung vorausgesetzt. Diese sollte hochverfügbar und redundant ausgeführt werden, da Sie Ihre Verwaltungsaufgaben nur durchführen können, wenn eine Verbindung zum Terminalserver besteht. Achten Sie darauf, dass kein Single Point of Failure entsteht, über den Sie potenziell angreifbar sein könnten.

10.7.1 Bereitstellung einer RemoteApp in einer Terminalserver-Umgebung

Um eine RemoteApp in einer Terminalserver-Umgebung bereitzustellen, starten Sie den *Server-Manager*, klicken auf der linken Seite auf Remotedesktopdienste und wechseln in den Unterpunkt Sammlungen. Wenn Sie noch keine Sammlung erstellt haben, müssen Sie dies jetzt nachholen.

Eine Sitzungssammlung als Grundlage der RemoteApp-Programme erstellen

Klicken Sie dafür auf Aufgaben, und wählen Sie Sitzungssammlung erstellen aus (siehe Abbildung 10.5).

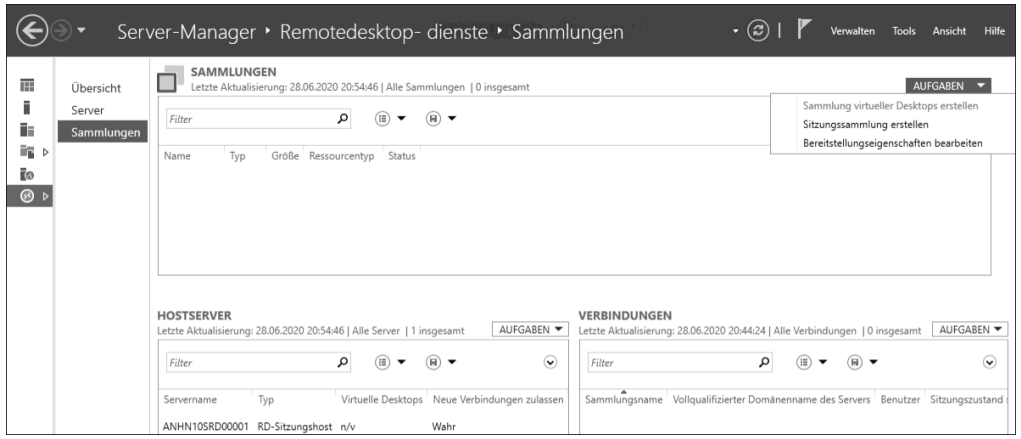


Abbildung 10.5 »Sitzungssammlung erstellen« in den Remotedesktopdiensten

Nun startet der Assistent mit der Seite Vorbemerkungen, die Sie einfach mit Weiter überspringen (siehe Abbildung 10.6).

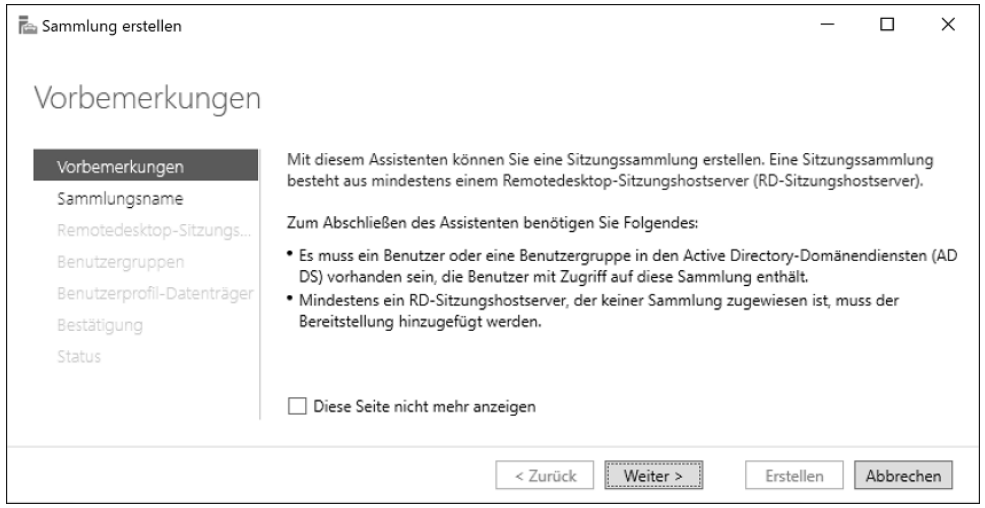


Abbildung 10.6 Der Assistent zur Erstellung der Sitzungssammlung – »Vorbemerkungen«

Auf der zweiten Seite müssen Sie einen Namen für die Sitzungssammlung festlegen und können optional eine Beschreibung hinterlegen (siehe Abbildung 10.7).

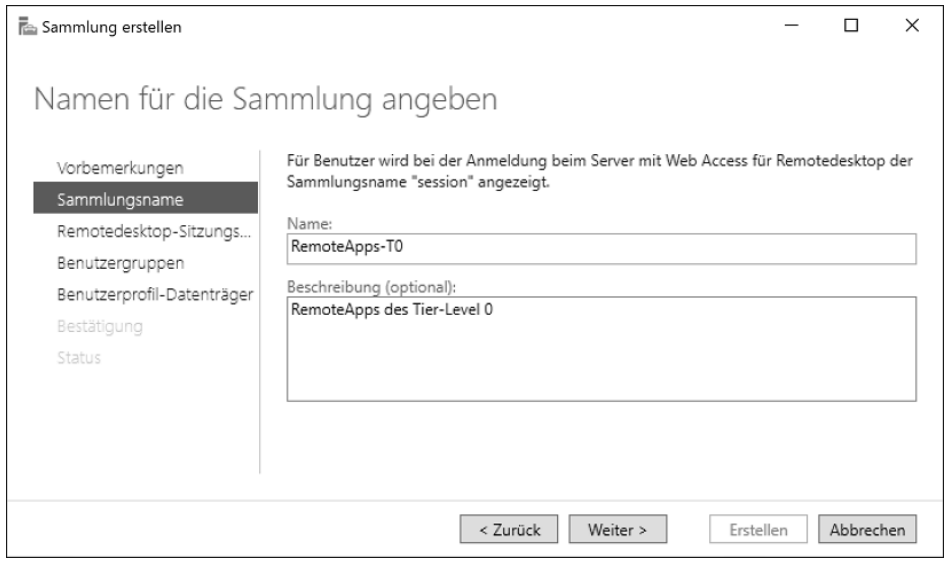


Abbildung 10.7 Der Assistent zur Erstellung der Sitzungssammlung – »Sammlungsname«

Auf der folgenden Seite müssen Sie den oder die Remotedesktop-Sitzungshostserver zum Serverpool hinzufügen (siehe Abbildung 10.8). In unserem Beispiel gibt es nur einen solchen Server und dieser wurde dem Serverpool hinzugefügt.

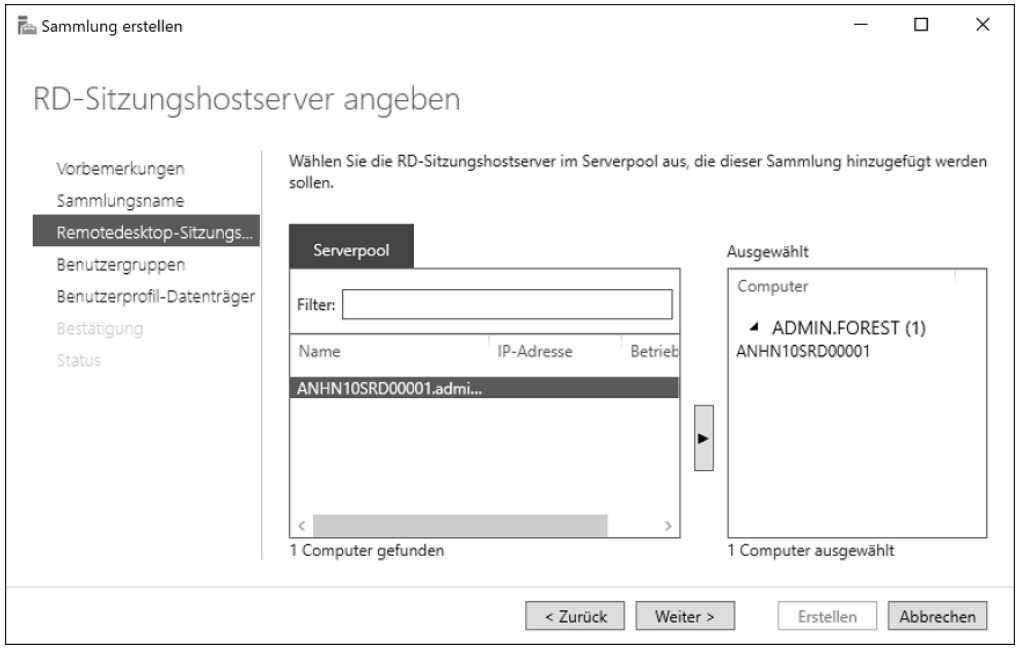


Abbildung 10.8 Der Assistent zur Erstellung der Sitzungssammlung – »Serverpool«

Als nächsten Schritt müssen Sie die Benutzergruppen festlegen, die auf die Anwendungen zugreifen dürfen (siehe Abbildung 10.9). Standardmäßig ist die Gruppe der *Domänenbenutzer* eingetragen, die wir entfernt haben, da wir nur Anwendungen für den Tier-Level 0 bereitstellen wollen. Stattdessen haben wir die Sicherheitsgruppe der *Domänen-Admins* aufgenommen.

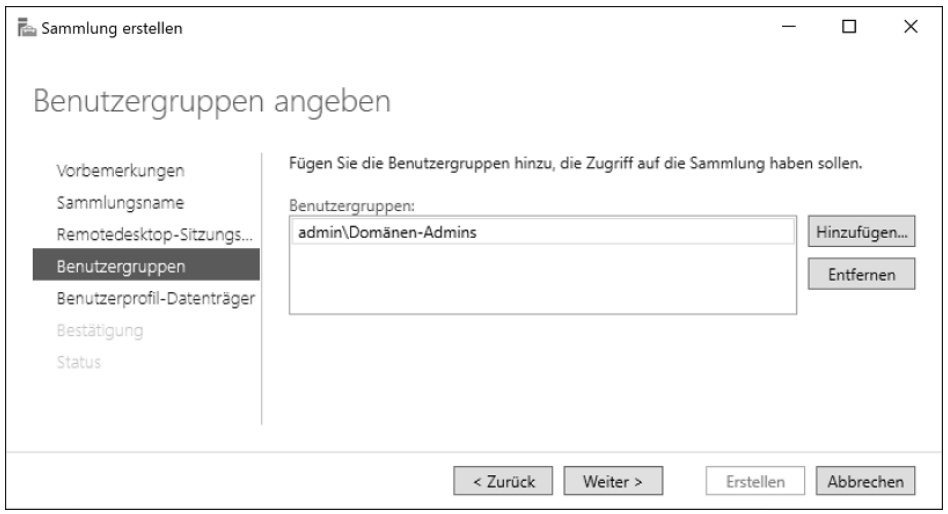


Abbildung 10.9 Der Assistent zur Erstellung der Sitzungssammlung – »Benutzergruppen«

Im vorletzten Fenster müssen Sie noch den Ordner für die Benutzerprofil-Datenträger festlegen (siehe Abbildung 10.10).

Zugriff auf die Sammlung

Alle Server in der Sammlung müssen Vollzugriff auf diesen Ordner haben. Außerdem muss die aktuelle Benutzerkennung, mit der Sie gerade die Einrichtung vornehmen, lokale Adminrechte auf dem Server haben,

Wir haben in unserem Beispiel kein UNC verwendet, da der Serverpool in unserer Testumgebung nur aus einem Server besteht. In Produktionsumgebungen sieht das sicherlich anders aus.

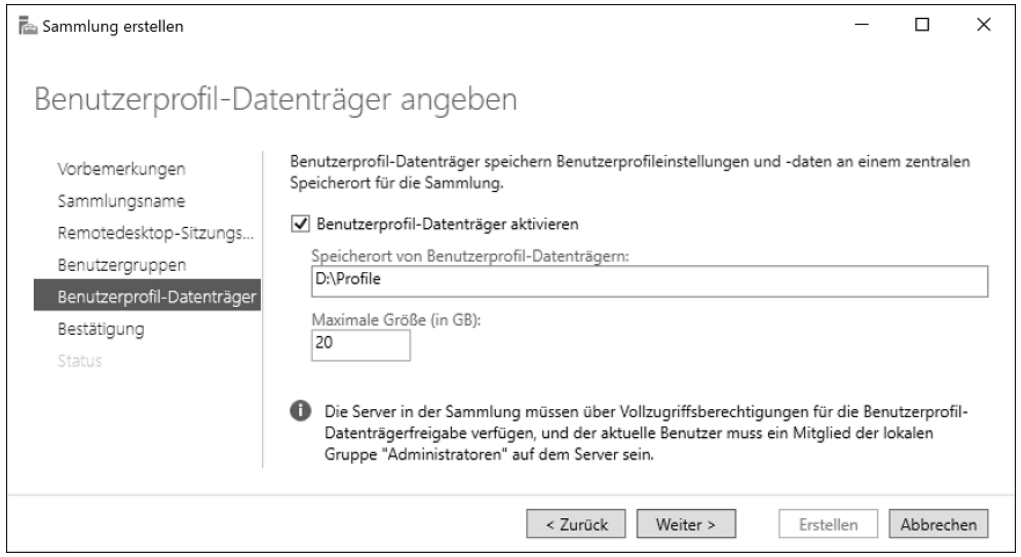


Abbildung 10.10 Der Assistent zur Erstellung der Sitzungssammlung – »Benutzerprofil-Datenträger«

Auf der letzten Seite des Assistenten werden noch einmal alle festgelegten Einstellungen angezeigt (siehe Abbildung 10.11). Klicken Sie auf ERSTELLEN, damit der ausgewählte Server dem Serverpool hinzugefügt wird und mit dem Anlegen der Sammlung begonnen werden kann.

In der neu geöffneten Seite (siehe Abbildung 10.12) können Sie den Fortschritt der Erstellung beobachten.

Sobald Sie alle Schritte erfolgreich durchgeführt haben, können Sie den Assistenten beenden. Nun haben Sie eine Sammlung erstellt und können mit dem Veröffentlichen der RemoteApp beginnen.

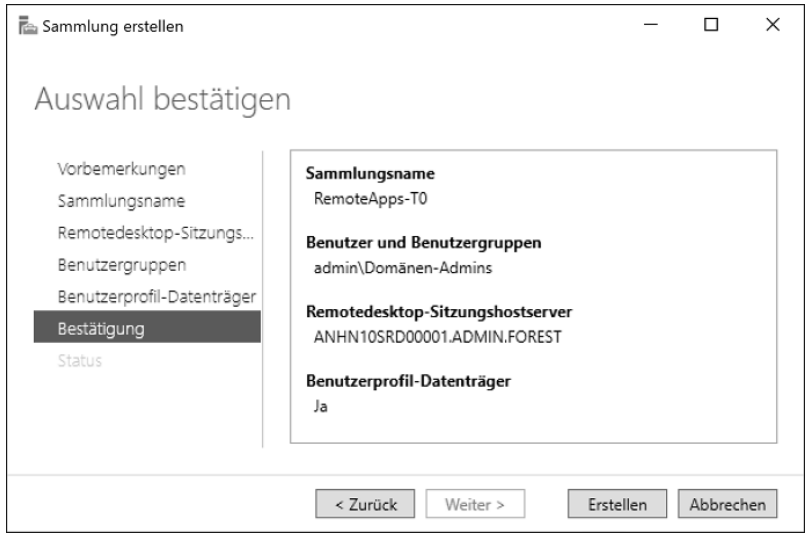


Abbildung 10.11 Der Assistent zur Erstellung der Sitzungssammlung – »Zusammenfassung«

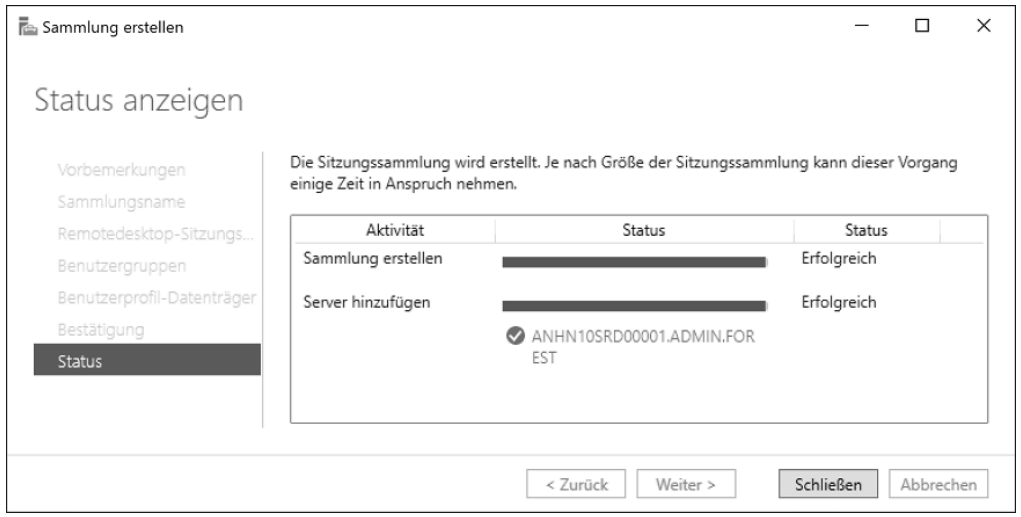


Abbildung 10.12 Der Assistent zur Erstellung der Sitzungssammlung – »Statusanzeige«

Veröffentlichung von RemoteApp-Programmen

Zum Veröffentlichen der RemoteApp-Programme klicken Sie im Server-Manager im Unterpunkt REMOTEDESKTOPDIENSTE • SAMMLUNGEN • REMOTEAPPS-T0 auf REMOTEAPP-PROGRAMME VERÖFFENTLICHEN. Daraufhin startet der Assistent, mit dem Sie die erwünschten RemoteApps bereitstellen können (siehe Abbildung 10.13).

Abbildung 10.13 Veröffentlichung eines RemoteApp-Programms in der Sitzungssammlung »RemoteApps-T0«

Direkt auf der ersten Seite des Assistenten können Sie die Programme auswählen, die Sie als RemoteApp-Programm veröffentlichen wollen (siehe Abbildung 10.14).

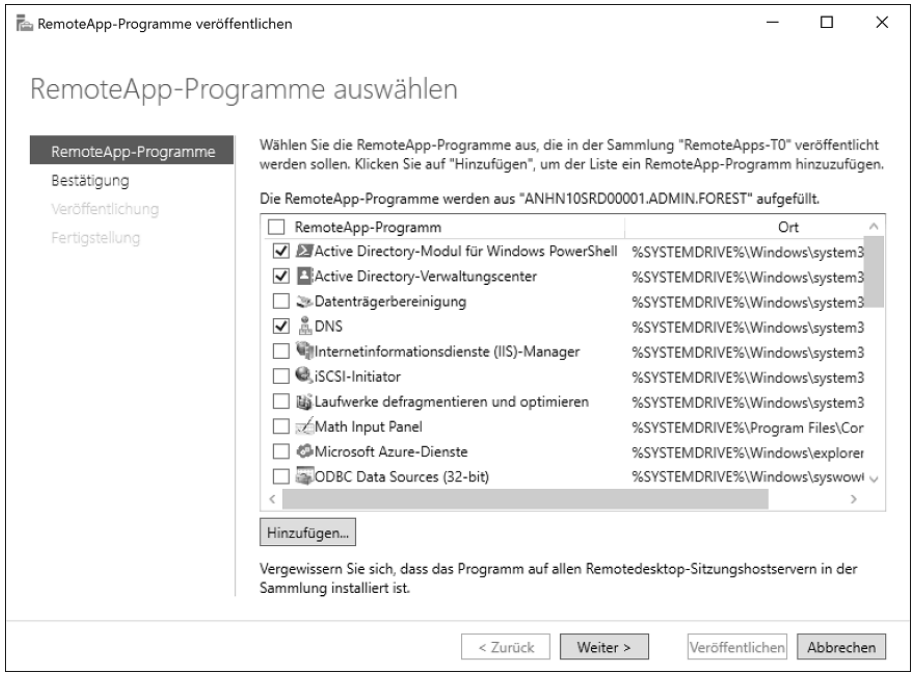


Abbildung 10.14 Auswahl der RemoteApp-Programme

Wir haben uns in unserem Beispiel für folgende Programme entschieden:

- Active Directory-Modul für Windows PowerShell
- Active Directory-Verwaltungscenter
- DNS

Wenn Sie weitere Programme der Liste hinzufügen wollen, klicken Sie auf HINZUFÜGEN. Sie können dann jedes beliebige Programm der Liste anfügen. Durch Klicken auf WEITER kommen Sie auf die nächste Seite (siehe Abbildung 10.15), auf der Sie die getroffene Auswahl bestätigen müssen.

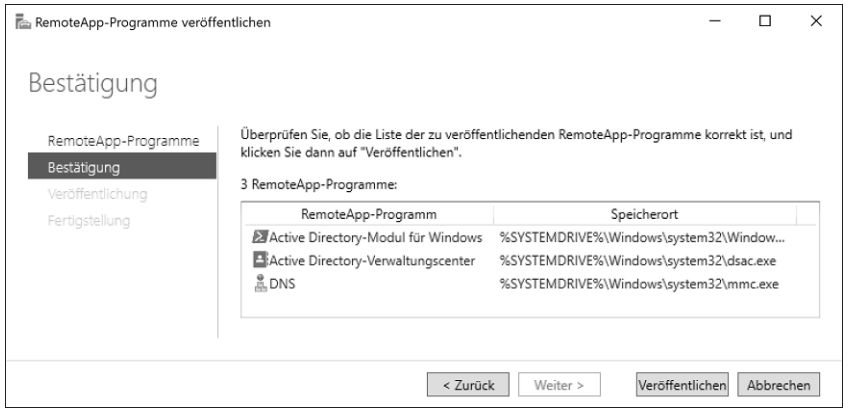


Abbildung 10.15 Bestätigung der RemoteApp-Programme

Wenn Sie auf VERÖFFENTLICHEN klicken, werden die RemoteApp-Programme veröffentlicht und sind nun für die Mitglieder der Sicherheitsgruppen *Domänen-Admins* über die URL des Terminalservers erreichbar. Auf der letzten Seite (siehe Abbildung 10.16) meldet der Assistent, dass die RemoteApp-Programme veröffentlicht wurden.

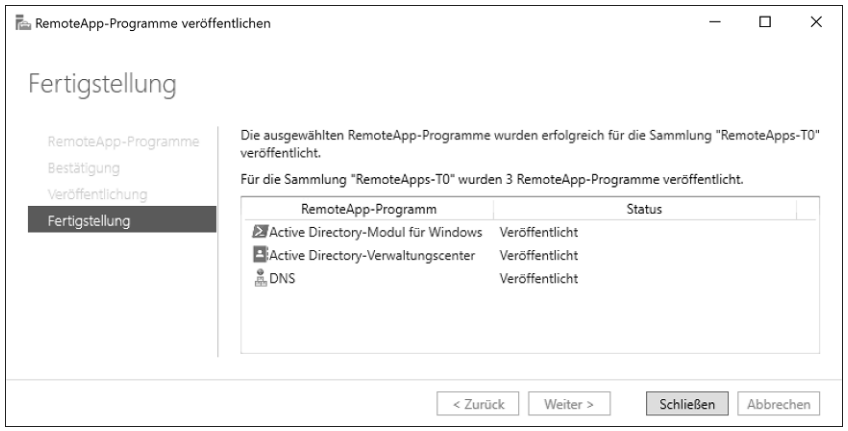


Abbildung 10.16 Die RemoteApp-Programme wurden veröffentlicht.

Zugriff von einem Client auf die veröffentlichten RemoteApp-Programme

Wenn Sie nun von einem Client auf die veröffentlichten RemoteApp-Programme zugreifen wollen, öffnen Sie einen Browser und geben die URL des Terminalservers ein, der die RemoteApp-Programme bereitstellt.

In unserem Beispiel ist es die URL *https://anhn10srd00001/rdweb*. Sobald Sie diese URL im Browser eingegeben haben, öffnet sich das Fenster aus Abbildung 10.17, in dem Sie sich mit Ihrer berechtigten administrativen Kennung anmelden müssen.

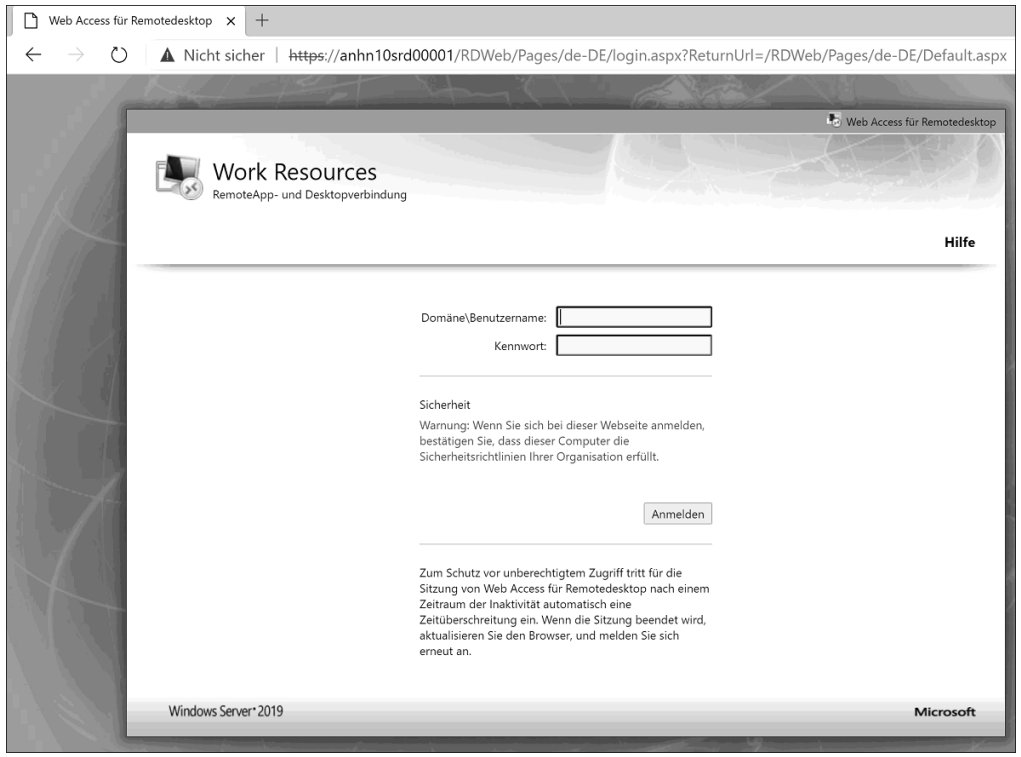


Abbildung 10.17 Zugriff auf die veröffentlichten RemoteApp-Programme – die Anmeldeseite des Terminalservers

Nach der Anmeldung an der Seite werden Ihnen die bereitgestellten RemoteApp-Programme angezeigt (siehe Abbildung 10.18).

Mit einem Klick auf das Icon des Programms wird dieses entweder direkt geöffnet oder es wird die notwendige RDP-Datei heruntergeladen. Hier kommt es darauf an, welchen Browser Sie für den Zugriff nutzen. In unserem Beispiel wurde die RDP-Datei heruntergeladen (siehe Abbildung 10.19) und wir mussten sie nach dem Download starten.

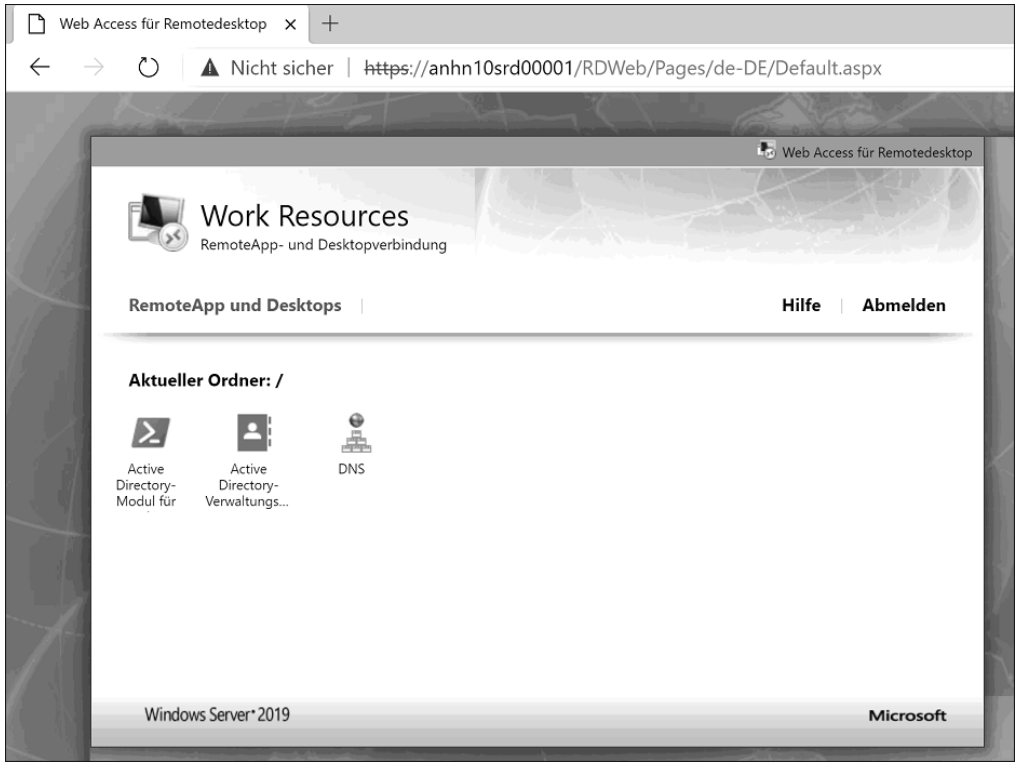


Abbildung 10.18 Zugriff auf die veröffentlichten RemoteApp-Programme – Liste der veröffentlichten RemoteApp-Programme

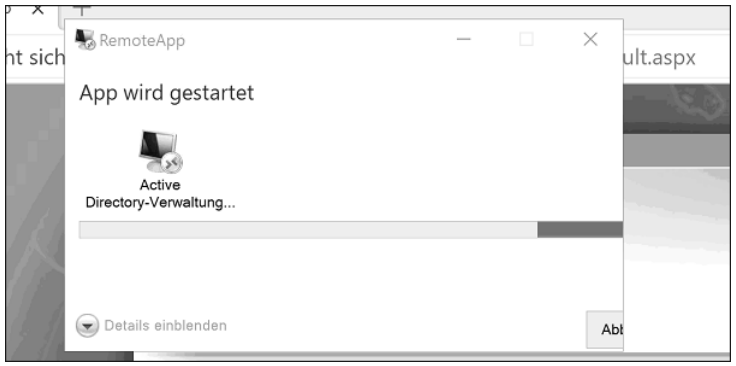


Abbildung 10.19 Zugriff auf die veröffentlichten RemoteApp-Programme – Start des ausgewählten RemoteApp-Programms

Im Hintergrund wird dann eine Remotedesktopsitzung zum Server aufgebaut und das RemoteApp-Programm gestartet.

Beim ersten Start einer Anwendung auf dem Server, wenn noch keine aktive Anmeldung besteht oder es die erste Anmeldung des Tages ist, müssen Sie Ihre Anmeldedaten erneut eingeben (siehe Abbildung 10.20). Hierbei handelt es sich aber jetzt nicht mehr um die Anmeldung am Terminalserver, sondern um die Anmeldung an der Remotedesktopsitzung auf dem Zielserver, auf dem die Anwendung gehostet wird. Der Zielserver muss nicht derselbe Server sein, der auch die Webseite des Terminalservers hostet.

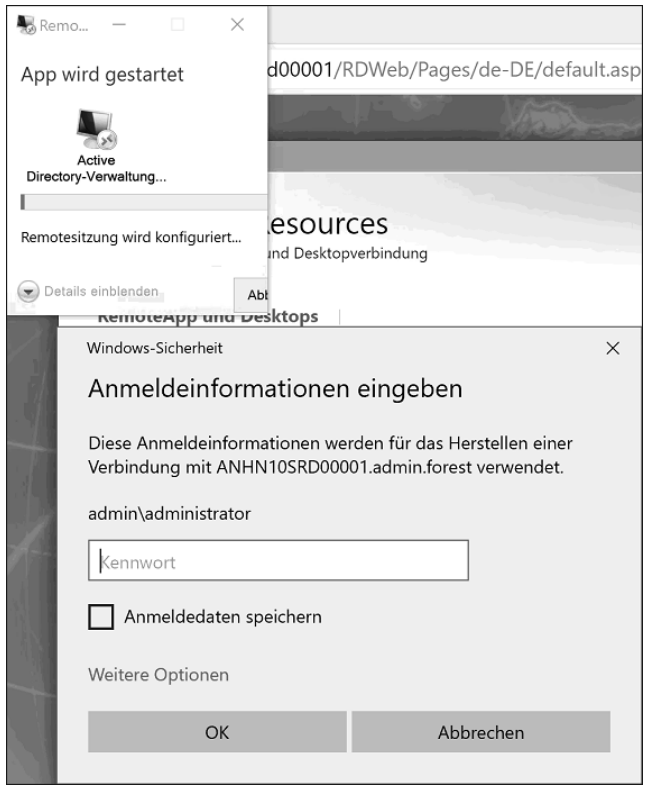


Abbildung 10.20 Zugriff auf die veröffentlichten RemoteApp-Programme – Eingabe der Anmeldedaten für die Remotedesktopsitzung auf dem Zielsystem

Haben Sie Ihre Anmeldedaten erfolgreich eingegeben, dauert es noch einen kleinen Moment, bis die Anwendung startet. Sobald die Anwendung gestartet wurde, wird diese auf dem Client nur angezeigt, aber eigentlich auf dem Server ausgeführt. Wenn Ihre Anbindung zum Server unterbrochen wird, wird auch der Zugriff auf das RemoteApp-Programm unterbrochen.

10.8 Zentralisierte Logs der Verwaltungssysteme

Alle Eventlogs sollten von allen Systemen immer zentral abgelegt werden, wobei eine Staffelung nach Tier-Leveln sinnvoll ist. Die zentrale Ablage der Eventlogs kann mithilfe des Windows Event Forwardings erfolgen. Wie Sie die Weiterleitung der Eventlogs einrichten, zeigen wir Ihnen in Kapitel 19.

Durch die zentralisierte Ablage der Eventlogs kann auch bei einem Ausfall der WAN-Strecke die Fehleranalyse mit den bereits vorhandenen Logs durchgeführt werden. Außerdem kann eine schlechte Anbindung entlastet werden, da der Zugriff auf die Log-Dateien nicht mehr online, sondern vom zentralen Speicherort aus erfolgt. Ein weiterer Vorteil ist, dass die Log-Dateien auf einem performanten Speicher abgelegt werden. Mit den richtigen Filtern sorgt eine Suche dann sehr schnell für Ergebnisse. Wenn Sie hingegen über die WAN-Strecke Eventlog-Dateien durchsuchen, die auf langsamen Speichern liegen, werden Sie mit sehr langen Wartezeiten kämpfen müssen.

10.9 Empfehlung zu Verwendung von Verwaltungssystemen

Zum Schluss möchten wir Ihnen eine Empfehlung mit auf den Weg geben: Ist Ihre Umgebung wenig komplex und überschaubar, sollten Sie dedizierte Verwaltungssysteme einsetzen. Eine Implementierung einer hochverfügbaren Terminalserver-Umgebung ergibt hier keinen Sinn, denn der zusätzliche Aufwand ist einfach zu groß. Wenn Ihre Umgebung jedoch komplex und auf mehrere Standorte verteilt ist, sollten Sie prüfen, ob der Online-Ansatz umsetzbar ist. Dann empfehlen wir die Bereitstellung aller Verwaltungswerkzeuge über eine Terminalserver-Umgebung. Durch diese müssen Sie keine weitere Hardware für Ihre Administratoren beschaffen, können von überall administrieren und müssen die Verwaltungstools nur an einer Stelle aktualisieren.

Auf einen Blick

Inhalt