semperis

2021

Active Directory Security *Halftime Report*

Erhalten Sie Einsichten und Ressourcen zur Verbesserung der Sicherheit hybrider Identitäten

CEO PERSPEKTIVE
MIT MICKEY BRESMAN

Grundlegende Maßnahmen zur Identitätssicherheit müssen ernsthaft angegangen werden, um Cyberangriffe einzudämmen

Nach einem halben Jahr mit weltweit eskalierenden Cyberangriffen in nahezu jeder Branche macht sich CEO Mickey Bresman Gedanken über Trends in der Cybersicherheit, die den Kampf gegen böswillige Angriffe auf Unternehmen sowie auf die öffentliche und nationale Sicherheit in nächster Zeit ausmachen werden

Warum tun sich Unternehmen nach wie vor schwer damit, fundamentale Active Directory-Sicherheitsmaßnahmen zu implementieren?

Zum einen gibt es Active Directory schon seit 20 Jahren und anfangs war Sicherheit bei der AD-Konfiguration kein allzu wichtiges Thema. Hinzu kommt, dass AD inzwischen erheblich komplizierter geworden ist: In jeder Umgebung gibt es zahlreiche unterschiedliche Berechtigungsebenen.

Nach wie vor steht AD im Mittelpunkt jeder Identitätsverwaltung – es ist in den meisten Unternehmen das Herzstück der Identitätsplattform –, jedoch hat sich das Umfeld radikal verändert. Grundlegende AD-Hygiene hat vor 15 Jahren noch keine große Rolle gespielt und aus vielen der damals begangenen Konfigurationen sind die Probleme geworden, die Sie heute beheben müssen. Ich möchte auch auf die Kompetenzlücken eingehen: Möglicherweise kennen sich Ihre Mitarbeiter mit AD extrem gut aus, denken aber eher von den Betriebsabläufen her. Oder Ihre Mitarbeiter sind mit Red-Teaming und Sicherheit umfassend vertraut, aber keine AD-Experten. Es ist nicht einfach, Personen zu finden, die über Kompetenzen in beiden Bereichen verfügen.

Wie können Unternehmen Kompetenzen erweitern oder Organisationsstrukturen anpassen, um IT- und Sicherheitsteams stärker zu integrieren?

Das Thema Identität muss integraler Bestandteil der Cybersicherheitsstrategie eines Unternehmen sein. Wer für Identitäten verantwortlich ist, kommt am Thema Cybersicherheit nicht vorbei. Wir wissen bereits, dass in vielen Unternehmen die Wiederaufnahme des IT-Betriebs nach einem Cyberangriff vom Active Directory abhängig ist. Wie lässt sich nun gewährleisten, dass diese Funktionalität im schlimmsten Fall möglichst schnell wiederhergestellt werden kann? Derzeit wird in Unternehmen die Verantwortung für Identitäten verstärkt in die Sicherheitsbereiche verlagert und selbst bei Unternehmen, die Identitäten nach wie vor dem operativen Bereich zuordnen, beobachten wir ein wachsendes Sicherheitsbewusstsein bei den IT-Experten sowie eine verstärkte Zusammenarbeit zwischen Sicherheits- und IT-Teams – vor allem in Bezug auf Identitätsverwaltung und Active Directory.

Ich halte das für einen durchaus positiven Trend: Jeder Mitarbeiter, der eine Position in identitätsrelevanten Bereichen innehat, muss sicherheitsorientiert denken.

Welche Sicherheitsherausforderungen bringt die Verwaltung einer hybriden Identitätsumgebung mit sich?

Wenn es um die Verwaltung von hybriden Identitätsumgebungen geht, fallen viele unterschiedliche Herausforderungen auf, angefangen bei der Tatsache, dass Active Directory und Azure Active Directory – außer dem Namen – wenig gemeinsam haben. Azure AD umfasst völlig andere Protokolle, die einen unterschiedlichen Verwaltungsansatz erfordern – auch beim Schutz des Identitätssystems vor Cyberangriffen. Wenn ich beispielsweise Änderungen an den Identitäten in der Cloud vornehme, wirkt sich das auf die Gesamtsicherheit im lokalen Rechenzentrum aus? In einem Hybrid-Szenario bietet sich Kriminellen eine größere potenzielle Angriffsfläche. Es kommt relativ häufig vor, dass Angriffe lokal beginnen und sich auf die Cloud ausweiten oder umgekehrt. Unternehmen müssen sich jetzt überlegen, welche Änderungen an den Identitätssystemen in jeder Umgebung vorgenommen werden und wie die Vernetzung zwischen beiden ein Einfallstor für Angreifer schaffen kann.

Bei der Sicherheitsverwaltung in einer Hybrid-Umgebung rückt auch das gemeinsame Verantwortlichkeitsmodell in den Vordergrund: Microsoft hat dafür zu sorgen, dass der Service kontinuierlich verfügbar ist. Was Sie mit Ihrer Umgebung tun – und wie Sie sie absichern – liegt in Ihrer Verantwortung.

Wie lange ist die Hybrid-Umgebung in den meisten Unternehmen relevant?

Die meisten unserer Kunden werden ihre Rechenzentren niemals vollständig aufgeben. Daher dürfte das Hybrid-Modell niemals an Relevanz verlieren. Unternehmen müssen sich überlegen, wofür das Rechenzentrum in Zukunft verwendet werden soll und bei welchen Services das Outsourcing an Microsoft, AWS, Google oder einen anderen Anbieter sinnvoller ist. So lässt sich eine optimale Lösung ganz nach aktuellen Anforderungen und Szenarien beliebig zusammenstellen. Die Cloud ist keine Universallösung.

Unabhängig davon, welche Systeme und Assets Sie lokal betreiben und welche in der Cloud, müssen Sie die Identitätsspeicher schützen. Identität wird beim Schutz vor Angreifern auch weiterhin die entscheidende Rolle spielen. Angesichts der zunehmenden Digitalisierung und des Cloud-Umstiegs müssen Sie zudem davon ausgehen, dass der Schutz von Identitäten für die operative und Sicherheitsstrategie Ihres Unternehmens immer wichtiger wird.

UNLEASH PURPLE KNIGHT

Purple Knight unterstützt IT- und Sicherheitsteams bei der Erkennung von Active Directory-Sicherheitslücken

Das kostenlose Tool zur AD-Sicherheitsbewertung, das bereits tausendfach heruntergeladen wurde, hilft Unternehmen Sicherheitslücken, die immer wieder für Cyberangriffe ausgenutzt werden, zu identifizieren und zu beseitigen.

Durch die Veröffentlichung des Sicherheitsbewertungstools Purple Knight im März 2021 wurde ein bis dato ungedeckter Bedarf erfüllt—Sicherheitslücken in Active Directory identifizieren und beseitigen zu können. Tausende von IT- und Sicherheitsexperten haben das kostenlose, von Semperis entwickelte Tool bereits heruntergeladen, das die Active Directory-Umgebung nach über 60 Risikofaktoren und Gefährdungen durchsucht.

„Bei uns hat niemand mit einer derart hohen Akzeptanz von Purple Knight auf dem Markt gerechnet“, sagt Mickey Bresman, Semperis CEO. „Aber wir sind angenehm überrascht, denn Unternehmen sind jetzt in der Lage, einen direkten Bezug zwischen den Angriffen, die sich in freier Wildbahn beobachten lassen, und den Sicherheitsschwachstellen in Active Directory herzustellen. Unternehmen fordern Purple Knight an, um ihre AD-Umgebungen zuverlässig auf diese Art von Angriffen vorzubereiten.“

Bresman sagt, Kundenfeedback weise darauf hin, dass Purple Knight Schwachstellen aufdeckt, die selbst Beratungsunternehmen entgehen. Er führt dies auf das umfassende Know-how des Semperis Teams in Bezug auf Active Directory zurück – und darauf, wie Unternehmen dieses Know-how nutzen.

„Wir haben festgestellt, dass viele Unternehmen unzureichend mit den Active Directory-Schwachstellen vertraut sind, die Angreifer ausnutzen“, sagt Bresman. „Wir wollten Sicherheitsteams mit geringer AD-Expertise eine Möglichkeit geben, ihren AD-Sicherheitsstatus zu verstehen – und dann vorhandene Lücken zu schließen, um die Umgebung vor Angriffen zu schützen.“

Purple Knight scannt die AD-Umgebung, um Sicherheitslücken aufgrund von böswilligen Aktivitäten oder Konfigurationsfehlern zu identifizieren, die sich vielleicht schon seit Jahren im System verbergen. Ran Harel, Semperis Senior Security Product Manager, sagt, viele der Konfigurationsfehler, die er in Active Directory-Installationen beobachte, seien entweder auf ein mangelndes Verständnis des Sicherheitsmodells insgesamt zurückzuführen oder auf die Implementierung von Notlösungen, die dann später weitere Schwachstellen verursachten.

„Das sind die Szenarien, auf die Angreifer sich bevorzugt konzentrieren – vor allem fehlerhafte Konfigurationen bei Kerberos und Gruppenrichtlinien“, sagt Harel.

Zu den häufigsten von Purple Knight aufgedeckten Schwachstellen zählen folgende:

- Kennwörter, die selten geändert werden und daher das Unternehmen für Brute-Force-Angriffe verwundbar machen
- Konten mit erhöhten Rechten, die nicht angemessen überprüft wurden – beispielsweise für die Gruppe „Unternehmensschlüsseladministratoren“
- Exchange-Konten mit erhöhten AD-Rechten, die mit der Zeit stark zugenommen haben
- Kerberos-Delegierung, die als „unbeschränkt“ konfiguriert ist und leicht missbraucht oder versehentlich unbefugten Benutzern offengelegt werden kann
- Schwache Konfiguration von Gruppenrichtlinien, wobei durch deren Verknüpfung mit Active Directory auf Domänenebene Sicherheitsschwachstellen entstehen können

„Wir wollten Sicherheitsteams mit geringer AD-Expertise eine Möglichkeit geben, ihren AD-Sicherheitsstatus zu verstehen – und dann vorhandene Lücken zu schließen, um die Umgebung vor Angriffen zu schützen.“

Mickey Bresman, *Semperis* CEO

Purple Knight sorgt für eine höhere AD-Sicherheit insgesamt, aber auch in Einzelkategorien, wie etwa AD-Delegierung, Kontensicherheit, AD-Infrastruktursicherheit, Gruppenrichtliniensicherheit und Kerberos-Sicherheit. In Erstberichten von Purple Knight meldeten Unternehmen durchschnittliche Werte von 61 % – das ist nur knapp bestanden. Dabei schnitt die Kerberos-Sicherheit am schlechtesten ab:

Durchschnittliche Werte aus Erstbewertungen

GESAMTBEWERTUNG	61%
AD-Delegierung	**68%**
Kontensicherheit	**59%**
AD-Infrastruktursicherheit	**77%**
Gruppenrichtliniensicherheit	**58%**
Kerberos-Sicherheit	**43%**

„Für Cyberkriminelle sind nachlässige Admin-Berechtigungen leichte Beute“, sagt Darren Mar-Elia, Semperis VP of Products. „Angreifern wird dadurch die Arbeit deutlich erleichtert. Sie nehmen den kürzesten Weg zum Domänenadministratorkonto und sobald Sie dieses unter Kontrolle gebracht haben, ist das Spiel vorbei.“

„Wer ständig vor AD-Sicherheitsschwachstellen auf der Hut sein will, muss sich intensiv um die Kontenhygiene kümmern“, sagt Ran Harel, leitender Security Product Manager bei Semperis.

„Das ist jedoch bekanntermaßen äußerst schwierig. Ein Benutzer kann 20 unterschiedlichen Gruppen angehören, die wiederum Untergruppen mit delegierten Rechten enthalten. Das ist wie Spaghetti: Man muss die Kontoberechtigungen regelmäßig aussortieren, sonst fällt die Kontenverwaltung nach und nach durchs Raster, und die Probleme nehmen immer weiter zu.“

Anhand der Berichte von Purple Knights wird die Ironie deutlich, dass die größten Organisationen mit den meisten Ressourcen wegen der enormen Größe und Komplexität ihrer Umgebungen besonders anfällig dafür sind, mit der Absicherung ihrer kritischen Identitätssysteme ins Hintertreffen zu geraden – und SolarWinds-ähnlichen Angriffen zum Opfer zu fallen.

"Since Active Directory is a prime target for attackers attempting to steal credentials and deploy ransomware across the network, it's worth considering the repercussions of an Active Directory attack even if you're not directly responsible for its daily operation."

MICKEY BRESMAN
Semperis CEO

ACTIVE DIRECTORY IS THE ACHILLES' HEEL OF ENTERPRISE SECURITY

Semperis CEO drängt auf bessere Verteidigung von Active Directory

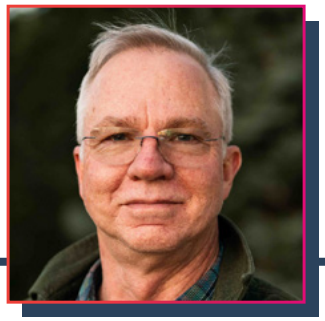
Manche halten Active Directory für einen von vielen Diensten, die nach einem Cyberangriff wiederhergestellt werden müssen. Realistisch gesehen ist AD jedoch Dreh- und Angelpunkt. Wenn AD einem Angriff zum Opfer fällt, ist die gesamte Umgebung gefährdet.

Fast die Hälfte (47 %) aller Unternehmen nutzen Active Directory als primären Identitätsspeicher. Bei 51 % kommt es mit unterschiedlicher Gewichtung parallel zu anderen Identitätsspeichern zum Einsatz, aber nur 1 % der Unternehmen nutzen AD entweder überhaupt nicht oder stellen derzeit auf ein anderes System um.

Viele Unternehmen verfolgen in Bezug auf Identitäten einen Hybrid-Ansatz und konzentrieren sich zunehmend auf die Cloud mit ihren Abhängigkeiten und ihrer Komplexität – dabei ignorieren sie jedoch die Tatsache, dass ihre Cloud-Identitäten nach wie vor mit einem lokalen Active Directory synchronisiert werden. AD wird als Quellsystem für die Synchronisierung mit anderen Identitätsspeichern genutzt, sodass ein erfolgreicher Angriff auf AD auch sämtliche verknüpften Cloud-Anwendungen beeinträchtigen kann. Diese potenziell problematische Vernetzung von cloudbasierten und lokalen Assets wird dadurch verschärft, dass viele Unternehmen während der Pandemie gezwungen waren, in kürzester Zeit die Unterstützung von Mobilgeräten im Homeoffice umzusetzen.

In seinem Artikel „Rethinking Active Directory Security" (Überdenken der Sicherheit von Active Directory) auf Help Net Security, befasst sich Semperis CEO Mickey Bresman damit, wie wichtig es für Unternehmen ist, über einen erprobten Plan zur Wiederherstellung von Active Directory (AD) im Falle eines Cyberangriffs zu verfügen. In diesem Artikel erfahren Sie, welche Schritte unternommen werden können, um beispielsweise durch AD-spezifische Überwachung den Schutz vor Cyberangriffen auf die AD-Infrastruktur zu verstärken.

ACTIVE DIRECTORY-EXPERTEN HABEN MIT SICHERHEIT EINE AUSSICHTSREICHE ZUKUNFT



VON **GIL KIRKPATRICK,** *Chief Architect bei Semperis*

Angesichts der immer größeren Verbreitung von Cloud-Anwendungen und einer sich wandelnden Bedrohungslandschaft hat sich der Aufgabenbereich von Experten für Microsoft Active Directory (AD) über die vergangenen mehr als 20 Jahre deutlich verändert.

Wie in jedem anderen IT-Bereich kommt es auch bei AD-Ingenieuren und -Architekten im Wesentlichen darauf an, mit wie viel Engagement und Interesse sie daran arbeiten, mit den neuesten Technologien Schritt zu halten.

Zwei Jahrzehnte lang lag der Schwerpunkt auf lokalen Systemen, Benutzern und Anwendungen. Heute sind die meisten AD-Experten verantwortlich für die Cloud-Integration und die verlässliche Absicherung von Umgebungen, in denen der herkömmliche Netzwerkperimeter nicht mehr relevant ist. Dabei sind sie ständigen Angriffen mit immer ausgefeilteren Methoden und Tools ausgesetzt, die AD, Konfigurationsfehler und Schwachstellen von Windows ausnutzen, Anmeldedaten von Benutzern ausspionieren und versuchen, sich auf den lokalen Systemen permanent einzunisten.

Angesichts dieser Entwicklung setzen IT-Führungskräfte verstärkt auf die Zusammenarbeit von Teams aus Sicherheits- und Identity-Experten, um dadurch im Zeitalter von Cloud-Computing und Homeoffice für einen sicheren Benutzerzugriff zu sorgen.

In Zukunft müssen AD-Experten damit rechnen, in Bezug auf Sicherheitsfragen eine aktivere Rolle zu spielen. Bisher ist das noch eher ungewöhnlich, aber da AD auch weiterhin die bevorzugte Angriffsfläche für Cyberkriminelle ist, können AD-Profis bei der Unterstützung der Sicherheitsbemühungen ihres Unternehmens mit ihrer Expertise glänzen. Bei unternehmensinternen Sicherheitsstrategien steht immer häufiger die Identität im Mittelpunkt, sodass AD-Administratoren verstärkt in Sicherheitsdiskussionen einbezogen werden. Wenn sie zudem in der Lage sind, ihr Wissen und ihre Kompetenz kontinuierlich zu erweitern, stellen sie einen erheblichen Mehrwert für das Unternehmen dar.

Veränderungen in der Bedrohungslandschaft als Chance für Active Directory-Profis

Bei der Konzeption von AD spielten die heutigen Sicherheitsherausforderungen noch keine Rolle – und damit sind nicht nur die Schwachstellen gemeint, die letztes Jahr u.a. von den Zerologon-Angriffen ausgenutzt wurden. Heutzutage fallen auch in Windows integrierte Protokolle sowie AD selbst solchen Angriffen zum Opfer.

Hinzu kommt das Problem von Ransomware. In vergangenen Jahren wurden immer wieder Ransomware-Angriffe beobachtet, bei denen APT-Methoden (Advanced Persistent Threats) für das Ausspähen und den Diebstahl von Anmeldedaten zum Einsatz kamen, beispielsweise über Tools wie BloodHound und Mimikatz. Bei einem Fall aus dem Jahr 2020 übernahm eine Ransomware die SYSVOL-Freigabe auf AD-Domänencontrollern, um Schadsoftware in der gesamten Zielumgebung zu verbreiten.

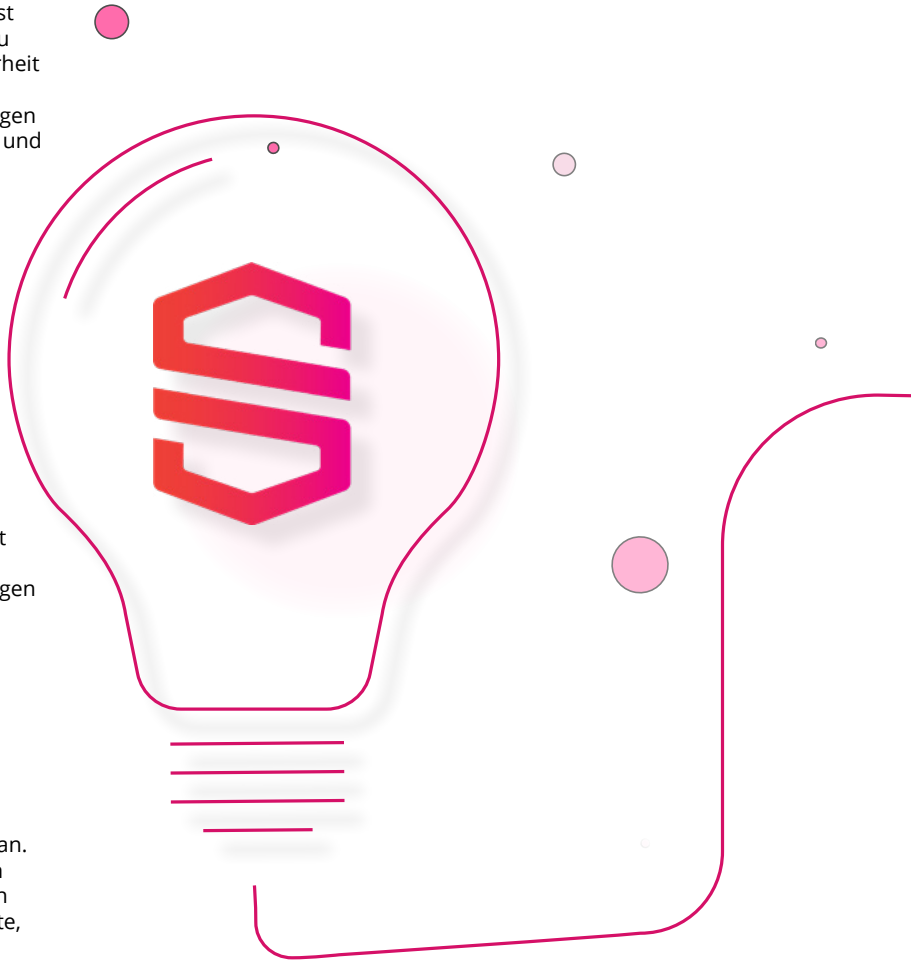
Früher konzentrierten sich AD-Wiederherstellungspläne in erster Linie auf Naturkatastrophen, Stromausfälle, Administrationsfehler und ähnliche Ereignisse. Heute müssen sich Unternehmen angesichts des wachsenden Risikos, dass Ransomware die gesamte IT-Umgebung lahmlegen könnte, auf ein Szenario vorbereiten, das deutlich wahrscheinlicher ist: ein Cyberangriff, der eine AD-Komplettwiederherstellung erforderlich macht.

Identität im Fokus

Mobile Benutzer und Cloud-Computing haben die herkömmlichen Netzwerkabgrenzungen aufgeweicht: Der einzige Kontrollpunkt für Benutzer, Anwendungen und Netzwerk-Assets ist die Benutzeridentität. Die digitale Identität spielt in allen Bereichen eines modernen Unternehmens eine Rolle. Jeder Benutzer muss Zugriff auf die relevanten Systeme und Anwendungen haben, um seine Arbeit machen zu können. Allerdings ist eine sichere Zugriffskontrolle weit mehr als nur eine Frage der Produktivität. Zu großzügige Berechtigungen, schwache Kennwörter und zahlreiche weitere potenzielle Probleme ziehen neben Datenschutzverletzungen, Infektionen mit Schadsoftware, erhebliche finanzielle Schäden nicht zuletzt lange Nächte für IT-Mitarbeiter und -Führungskräfte und vor allem teilweise erhebliche Produktionsausfälle nach sich.

Das Angebot an Cloud-Anwendungen für Mitarbeiter wächst ständig, weshalb die notwendige Integration in AD nicht nur für das Identitätsteam eine Herausforderung ist. Auch die Erweiterung von Sicherheits- und Zugriffsrichtlinien vom lokalen AD in die Cloud birgt Sicherheitsrisiken. All den AD-Experten, die das Berechtigungsmodell ihrer lokalen Umgebung gewohnt sind, kann das Umdenken bei der Integration von lokalem AD und Azure Active Directory (AAD) schwerfallen. (Die Auswirkungen der parallelen Verwaltung von lokalem AD und AAD in einer Hybrid-Umgebung werden ausführlich behandelt im Artikel „Die größten Sicherheitsrisiken bei der Umstellung auf hybride Identitätsverwaltung“ von Doug Davis, Senior Product Manager bei Semperis.)

Allerdings gilt auch hier, dass diese Veränderung Chancen mit sich bringt. Im Bemühen um den digitalen Wandel ist es unverzichtbar, die neuen Risiken für Unternehmen zu verstehen und zu wissen, welche Rolle AD für die Sicherheit spielt. Identitätsexperten, die Sicherheitsteams oder C-Level-Führungskräfte fachkundig beraten können, tragen optimal zur Sicherheitsstrategie des Unternehmens bei und bauen dadurch die eigenen Karrierechancen aus.



Ausbau des Wissens zu Identitäten und Sicherheit

Für Experten im Bereich Active Directory und andere Identitätsdienste, die ihren Beitrag zur Sicherheitsstrategie des Unternehmens leisten möchten, kommt es vor allem darauf an, jederzeit auf dem neuesten Wissensstand zu sein – einer der anstrengendsten (und dankbarsten) Aspekte einer IT-Laufbahn. Man denke nur an all die Technologien, mit denen IT-Profis sich im Laufe ihrer Karriere vertraut machen mussten und die heute nicht mehr relevant sind. Wie viele Technologien wurden eingestellt und werden nicht mehr unterstützt? Nur wer sich regelmäßig fortbildet, kann mit den ständigen Neuerungen bei IT-Sicherheit und -Betriebsabläufen Schritt halten.

Die gute Nachricht: Im Internet finden Sie zahllose Ressourcen für IT-Profis. Channel 9 beispielsweise ist eine Fundgrube für Anleitungsvideos zu Microsoft Produkten. Auch Microsoft selbst stellt Material zur Vorbereitung auf Microsoft Zertifizierungsprüfungen bereit. Für Identitätsexperten bieten sich die Sicherheitszertifizierungen „Security, Compliance, and Identity Fundamentals“ sowie „Security Fundamentals“ an. Diese und andere Zertifizierungen werten nicht nur den eigenen Lebenslauf auf, sondern sie schaffen zudem ein stabiles Fundament in Bezug auf die Sicherheitskonzepte, mit denen Identitätsexperten im Gespräch mit IT-Führungskräften vertraut sein müssen.

Grundsätzlich aber geht nichts über Erfahrung. Nur durch praktische Erfahrung in einer Laborumgebung – nicht nur mit lokalem AD, sondern auch mit Hybrid-Umgebungen, in denen Azure, AWS und Google Cloud zum Einsatz kommen – erwirbt man umfangreiche Kompetenzen in der effektiven und sicheren Verwaltung solcher Systeme.

Man lernt nie aus in Bezug auf Identitäten und Sicherheit

Für alle Karrierepfade in der IT gilt: Veränderung ist die einzige Konstante. Wer einen Aspekt der Branche – von Sicherheit bis App-Entwicklung – umfassend beherrschen will, muss in Bezug auf unterschiedlichste Technologien und Trends jederzeit auf dem Laufenden sein. Da identitätsrelevante Sicherheitsrisiken und die Cloud-Akzeptanz ständig zunehmen, müssen AD-Experten verstehen, wie die Identitätsverwaltung in die Sicherheitsstrategie ihres Unternehmens passt und entsprechende Initiativen proaktiv anstoßen.

Drei Schritte zur Absicherung von Active Directory angesichts der jüngsten Angriffe

VON **BRIAN DESMOND,** *Principal bei Ravenswood Technology Group*

In einem Webinar, das ich kürzlich gemeinsam mit Semperis (dem Anbieter des Sicherheitstools Purple Knight) veranstaltete, ging es um einen der gemeinsamen Hauptfaktoren bei einer Reihe von sehr prominenten Angriffen: Active Directory. Unter dem Thema „So wird Active Directory ausgenutzt: Erfahrungen aus prominenten Angriffen" nahm ich mit Sean Deuby und Ran Harel von Semperis vier Vorfälle unter die Lupe, die kürzlich viel Aufmerksamkeit erhalten hatten: SolarWinds, der Zero-Day-Angriff auf Exchange durch Hafnium, der Angriff auf Colonial Pipeline und der Ransomware-Angriff auf das irische Gesundheitswesen. Zwar waren Taktik und Akteure bei jedem Vorfall völlig unterschiedlich, jedoch waren die Folgen durchweg verheerend. Im Rahmen des Seminars befassten wir uns mit drei der wichtigsten Präventivmaßnahmen, mit denen sich Unternehmen gegen Cyberangriffe zur Wehr setzen können.

1 Schutz vor hoch entwickelten E-Mail-Bedrohungen

Eines der häufigsten Einfallstore für Angreifer sind E-Mails. Ausgefeilte Phishing-Kampagnen wirken höchst überzeugend auf Endbenutzer, sodass Kriminelle auf diesem Weg Anmeldedaten abgreifen oder Schadsoftware auf Endpunkte einschleusen können. Um sich möglichst effektiv vor solchen Bedrohungen zu schützen, müssen Unternehmen auf eine mehrdimensionale Strategie setzen. Sicherheitsschulungen und Phishing-Simulationen sind ein wirksames Mittel, um das Sicherheitsbewusstsein zu fördern und Risiken besser einschätzen zu können. Allerdings wird es trotz der besten Schulungen immer wieder erfolgreiche Angriffe geben. Daher muss eine moderne und erfolgreiche Lösung zum Schutz vor E-Mail-Bedrohungen, die mehr leistet, als Spam und Viren zu verhindern, ein integraler Bestandteil der Verteidigungsstrategie sein. Angesichts der aktuellen Bedrohungslage ist ein Service unverzichtbar, der Algorithmen für maschinelles Lernen und andere fortschrittliche Methoden einsetzt, um Phishing-Nachrichten und verdächtige Anhänge zu erkennen und zu blockieren.

„Man muss schon das letzte Jahr hinter dem Mond gelebt haben, wenn man von den fast schon wöchentlichen Vorfällen im Bereich Cybersicherheit nichts mitbekommen hat. Wir reden viel über die neuen Angriffsmethoden, aber es geht den Kriminellen nicht darum, immer neue Methoden zu entwickeln. Sie wollen vor allem erfolgreich in Unternehmen eindringen – und da ist Active Directory quasi wie ein Scheunentor ."

– SEAN DEUBY, *Director of Services bei Semperis*

2 Verhindern von lateraler Bewegung

Ist ein Angreifer erst einmal in einen Client-Rechner oder einen Mitgliedsserver eingedrungen, wird er versuchen, weitere Endpunkte im Netzwerk zu erreichen, um seine Rechte zu erweitern. Durch die Unterbindung von lateraler Bewegung wird dies erheblich erschwert. Sie können technisch einfache Kontrollen implementieren, die allerdings bisweilen die Betriebsabläufe verkomplizieren. Erstens muss der lokale Administrator jedem Endpunkt ein eindeutiges Kennwort zuweisen. Microsoft bietet die kostenlose Lösung Local Administrator Password Solution (LAPS), mit der sich dies erreichen lässt. Zweitens darf die Gruppe der lokalen Administratoren keine verschachtelten Konten enthalten, um den Zugriff durch den IT-Support zu vereinfachen. IT-Mitarbeiter müssen zum Abrufen von Admnden.t be different.

3 Sicherer Zugriff auf privilegierte Anmeldedaten

Kriminelle daran zu hindern, sich privilegierten Zugriff – vor allem auf die Konten von Domänenadministratoren – zu verschaffen, ist ein wichtiger Aspekt einer Verteidigungsstrategie. Mit erweiterten Berechtigungen können Angreifer mehr Kontrolle erlangen oder sogar das gesamte Netzwerk übernehmen. Die Implementierung von effektiven Sicherheitskontrollen, mit denen sich privilegierte Anmeldedaten isolieren und schützen lassen, ist daher von größter Wichtigkeit. Zwei Maßnahmen, die wir bei Ravenswood Technology Group am häufigsten einsetzen, sind gestaffelte Sicherheitskontrollen sowie Privileged Access Workstations (PAWs). Gestaffelte Sicherheitskontrollen verhindern den Zugriff auf privilegierte Anmeldedaten durch risikobehaftete Assets, wie etwa Client-Computer, über die solche Anmeldedaten gestohlen werden könnten. PAWs sind höchst sichere Workstations, mit denen sich Admin-Aufgaben von der alltäglichen Arbeit eines Administrators auf herkömmlichen Rechnern isolieren lassen. Dadurch bleiben Anmeldedaten und Admin-Sitzungen vor Angriffen über E-Mail und Internet sowie vor bestimmter Schadsoftware geschützt

Ist Ihr AD gerüstet für die moderne Bedrohungslandschaft?

Die Angriffe, die in diesem Webinar behandelt wurden, sind nur vier von zahllosen Beispielen für Datenschutzverletzungen, die Tag für Tag in den Schlagzeilen zu finden sind. Die Absicherung der IT-Umgebung ist extrem wichtig und für nahezu jedes Unternehmen muss die Verteidigung von Active Directory in der Sicherheitsstrategie eine zentrale Rolle spielen. Wenn Sie Ihre Sicherheitskontrollen für Active Directory beurteilen lassen möchten, nutzen Sie die kostenlose Testversion von Purple Knight. Über Ravenswood und Semperis hinaus dürfte es keine anderen Organisationen geben (mit Ausnahme von Microsoft selbst), die gemeinsam über mehr AD-Sicherheitskompetenz verfügen. Dank unserer sehr engen Partnerschaft können wir Unternehmen weltweit helfen, neue Maßstäbe bei der Hybrid-Identitätssicherheit zu setzen.

Weitere Informationen dazu, wie Sie Ihre Organisation effektiv schützen können, erhalten Sie im erwähnten On-Demand-Webinar. Zudem können Sie Purple Knight kostenlos herunterladen, um AD-Sicherheitslücken zu identifizieren und zu beheben und für eine zuverlässige Absicherung ihrer AD-Umgebung zu sorgen – wie komplex, verschachtelt oder vernachlässigt sie auch sein mag.

RESSOURCEN

- Cyber-First Notfallwiederherstellung für Active Directory
- Wiederherstellung von Active Directory ohne Schadsoftware
- Wiederherstellung von Active Directory nach Cyberkatastrophen)

Der praktische Mehrwert einer schnellen Active Directory-Wiederherstellung

VON **SEAN DEUBY,** *Director of Services bei Semperis*

Jeder IT-Manager und Administrator weiß, wie wichtig ein robuster Active Directory-Wiederherstellungsplan für jede Business-Continuity-Strategie ist. Jedoch ist die realistische Berechnung des finanziellen Returns (ROI) eines optimierten AD-Wiederherstellungsplans bekanntermaßen äußerst schwierig. Zu viele Variablen stehen einer belastbaren, präzisen Berechnung im Weg. Um die Erwartungen von vornherein zurechtzurücken: Ich werde hier keinen interaktiven ROI-Rechner anbieten.

Stattdessen möchte ich auf einige praktische Möglichkeiten eingehen, durch eine sinnvolle AD-Wiederherstellung für eine optimale Amortisation zu sorgen – und zwar so, dass Sie Ihre eigenen Berechnungen anstellen und Ihre eigenen Schlüsse ziehen können. Der Verlust eines Domänencontrollers ist an sich schon ein Problem, aber sehen wir uns ein Szenario an, das immer häufiger auftritt und katastrophale Folgen hat: ein Ransomware-Angriff, durch den jeder einzelne Domänencontroller an allen Unternehmensstandorten ausgeschaltet wird. In einer solchen Situation ist die AD-Wiederherstellung eine extreme Herausforderung mit höchstem Zeitdruck.

Letztes Jahr haben wir uns mit zahlreichen Ransomware-Angriffen befasst, bei denen Cyberkriminelle AD auf die eine oder andere Weise modifiziert haben – weit über Änderungen von Benutzerkonten oder Kennwörtern hinaus –, um sich Zugang zu Informationssystemen zu verschaffen und Schadsoftware in parallelen Systemen zu verbreiten. Ransomware-Architekten beschäftigen jetzt Programmierer, die AD und seine Sicherheitsupdates sezieren, um Möglichkeiten zur Erweiterung von Berechtigungen sowie zur schnellen Verbreitung von Schadsoftware im gesamten Unternehmen zu finden. Forensische Ermittlungen nach früheren Ransomware-Angriffen, bei denen AD betroffen war, haben ergeben, dass böswillige Akteure es vor allem auf Gruppenkonten, Benutzerkonten, Gruppenrichtlinienobjekt, die SYSVOL-Freigabe und Domänencontroller abgesehen haben.

Angesichts dieser Taktiken von Cyberkriminellen sollten Sie bei der Berechnung Ihres eigenen ROI für die AD-Wiederherstellung folgende Faktoren berücksichtigen:

Kosten aufgrund von Betriebsausfällen

Mit großer Wahrscheinlichkeit ist ein Großteil Ihrer Betriebsabläufe auf ein funktionsfähiges AD angewiesen, da für den Zugriff auf Anwendungen, Systeme und Daten ständig Benutzer authentifiziert werden müssen. Wie viel Umsatz oder Produktivität würde Ihr Unternehmen pro Stunde verlieren, wenn AD ausfiele? Nach wie vielen Stunden, Tagen oder Wochen wäre der Punkt erreicht, an dem das Unternehmen finanziell nicht mehr zu retten wäre? Erinnern Sie sich an die Ransomware-Attacke auf die Stadtverwaltung von Baltimore? Die Wiederherstellung sämtlicher Betriebsabläufe dauerte Monate und kostete über 18 Millionen US-Dollar.

Kein Business-Continuity-Plan, der AD berücksichtigt

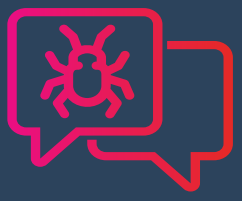
Unternehmen, die eine gewisse Reife erreicht haben, verfügen in der Regel über Pläne für Business Continuity/Notfallwiederherstellung, in denen das Vorgehen zur Wiederherstellung der Betriebsabläufe nach einem Ausfall detailliert beschrieben sind. In den meisten Fällen ist der Verlust der Infrastruktur oder eines ganzen Standorts nach einer Naturkatastrophe abgedeckt. Jedoch findet sich nur bei wenigen Unternehmen ein Plan, der sich mit der Wiederherstellung nach einem Cyberangriff befasst – vor allem nach solchen Angriffen, die so unabsehbare Folgen haben wie Ransomware-Attacken. Das Vorgehen zur Wiederherstellung von AD in einer solchen Situation ist davon abhängig, welche Modifikationen die Cyberkriminellen an AD vorgenommen haben. Vielleicht sieht Ihr Plan das Zurücksetzen auf eine frühere AD-Version vor, aber wie bestimmen Sie, welche Vorversion ausreichend sicher ist? Welche AD-abhängigen Systeme, Dienste und Anwendungen sind beeinträchtigt oder nicht mehr funktionsfähig, wenn die ganze Umgebung pauschal auf einen früheren AD-Zustand zurückgesetzt wird? Sind Sie zuversichtlich, dass Sie ein relativ aktuelles und nicht von Schadsoftware befallenes Backup überhaupt finden können? Ohne einen Plan oder die Möglichkeit, vor einer Wiederherstellung genau zu ermitteln, welche AD-Modifikationen es gegeben hat, wird Ihr Unternehmen wertvolle Zeit darauf verschwenden, die Probleme zu beheben, die durch die Wiederherstellung verursacht wurden.

Wiederherstellung ist möglicherweise nicht die Lösung

Wenn die Änderungen, die Angreifer vorgenommen haben, sich beispielsweise auf das Hinzufügen eines Kontos zur Gruppe der Domänenadministratoren beschränken, ist das Zurücksetzen von AD auf einen Stand von vor einigen Tagen oder vom letzten Monat wahrscheinlich nicht die beste Lösung. Stattdessen wäre es weniger aufwändig und kostspielig, die AD-Modifikationen zu überwachen und eine Möglichkeit zu schaffen, entweder Änderungen an „geschützten" Konten (wie etwa der Gruppe „Domänen-Admins") zu unterbinden oder Modifikationen automatisch auf eine genehmigte Konfiguration zurückzusetzen.

Die oben genannten Überlegungen decken drei Risiken ab: das Risiko einer langsamen Wiederherstellung, das Risiko einer Wiederherstellung, die zusätzliche Korrekturmaßnahmen nach sich zieht und das Risiko einer Wiederherstellung, die für die Art der AD-Modifikationen im Rahmen des Angriffs als überzogen verstanden werden kann.

BERICHTE AUS DER PRAXIS



Semperis stellt bestbewertete Lösungen zur Notfallwiederherstellung für Active Directory bereit. Hier sind einige der Erfolge, die unsere Kunden nach der Bereitstellung von Semperis Active Directory Forest Recovery zu vermelden hatten:

- Die israelische Fluglinie El Al konnte durch die Bereitstellung von Semperis ADFR die Wiederherstellung der vollst2ändigen AD-Gesamtstruktur von 24 auf 2 Stunden beschleunigen.
- Ein globaler Einzelhändler mit 2,2 Millionen Benutzern und 500 Domänencontrollern wechselte von seiner bisherigen Lösung zu Semperis ADFR und verkürzte die Dauer zur Bereitstellung einer AD-Gesamtstruktur von 6 Tagen auf 6 Stunden.
- Ein Gesundheitsunternehmen mit einem DIT von 65 GB beschleunigte die Wiederherstellung der AD-Gesamtstruktur von 1,5 Tagen mit der früher verwendeten Lösung auf weniger als 4 Stunden mit Semperis ADFR.

Ein alternativer Ansatz für die Berechnung des ROI der AD-Wiederherstellung

Statt sich bei der Berechnung der Amortisation der AD-Wiederherstellung auf irgendeinen Online-Rechner zu verlassen, empfiehlt es sich, verschiedene tatsächliche Szenarien auszuwerten und anhand der folgenden Fragen zu beurteilen, wie Ihre aktuellen Methoden zur AD-Wiederherstellung abschneiden würden:

→ Welche kritischen Betriebsabläufe sind auf ein funktionierendes AD angewiesen? Welche geschätzten Kosten verursacht ihr Ausfall?

→ Wie lange dauert es, AD unter Berücksichtigung der bei einem Angriff vorgenommenen Modifikationen wiederherzustellen?

→ Können Sie nachvollziehen, welche böswilligen Änderungen an AD vorgenommen wurden? Wenn nicht, wie weit zurück müssen Sie ermitteln und wie lange wird dies dauern?

→ Wird die Wiederherstellung andere Betriebsabläufe beeinträchtigen, die dann korrigiert werden müssen? Wenn ja, wie lange wird dies dauern? (Beachten Sie: Wenn Kennwörter für Konten nicht mehr stimmen, ist die Anmeldung bei der Domäne nicht möglich. Zudem fehlen bei früheren Versionen möglicherweise Konten, Gruppenmitgliedschaften, DNS-Einträge usw.)

→ Sind Sie zuversichtlich, dass sich durch eine Wiederherstellung ein sicherer Zustand erreichen lässt? Es besteht ein Unterschied zwischen der Wiederaufnahme und der Wiederherstellung des Geschäftsbetriebs: Wenn Sie nicht über ein Backup verfügen, das frei von Schadsoftware ist und das Sie zur Wiederherstellung nutzen können, schaffen Sie womöglich wieder die gleichen Schwachstellen, die den Angriff ermöglicht haben.

Kurz gesagt, hat die Anlagenrendite der AD-Wiederherstellung vor allem damit zu tun, wie Sie Ihre Systeme nach einem Angriff auf einen bekannten sicheren Produktivzustand zurücksetzen und weniger mit einem Online-ROI-Rechner, der die zahlreichen Variablen eines Ransomware-Angriffs nicht berücksichtigen kann. Indem Sie einige Szenarien durchspielen und sich ihre derzeitigen Wiederherstellungsoptionen konkret vor Augen führen, werden Sie Kosten aufdecken, die sich mithilfe einer professionellen AD-Wiederherstellungslösung vermeiden lassen, da eine solche Lösung dafür konzipiert ist, böswillige AD-Modifikationen zu verhindern und ggf. rückgängig zu machen.

Schutz vor unbemerkbaren Active Directory-Angriffen

VON **GUIDO GRILLENMEIER,** *Chief Technologist bei Semperis*

Cyberkriminelle setzen auf immer neue Strategien und Methoden, um sich Zugriff auf Active Directory zu verschaffen. Die dabei angerichteten Schäden werden ständig mehr, weshalb es so wichtig ist, die Angriffe rechtzeitig zu erkennen.

Einer der wichtigsten Bestandteile jeder Cybersicherheitsstrategie ist die Erkennung. Nur wer in der Lage ist, böswillige Akteure beim Eindringen, Durchsuchen oder sogar Manipulieren des Netzwerkes zu beobachten, kann auch schnell reagieren.Die durchschnittliche unerkannte Verweildauer eines Angreifers im Netzwerk von 146 Tagen, (laut Microsoft) macht deutlich, dass Kriminelle ihre Aktivitäten sehr gut verbergen können.

Wenn es darum geht, potenziell schädliche Aktivitäten in Active Directory (AD) aufzudecken, setzen die meisten Unternehmen auf die Konsolidierung von Domänencontroller-Ereignisprotokollen sowie auf SIEM-Lösungen, um ungewöhnliche Anmeldungen und Änderungen zu erkennen. All dies funktioniert durchaus – solange der Angriffsversuch in den Protokollen aufgezeichnet wird.

Es wurden jedoch bereits eine Reihe von Angriffen beobachtet, die keine erkennbaren Spuren oder zumindest keine Beweise für böswillige Aktivitäten hinterlassen. Einige Beispiele:

DCShadow-Angriff:

Unter Verwendung der DCShadow-Funktion des Hacker-Tools Mimikatz wird bei diesem Angriff zunächst die Konfigurationspartition von AD modifiziert, um einen unbefugten Domänencontroller (DC) zu registrieren. Anschließend nimmt der Angreifer böswillige fingierte Änderungen vor (z. B. an den Gruppenmitgliedschaften von Domänen-Admins oder auch weniger offensichtliche Änderungen, wie etwa das Hinzufügen der SID der Gruppe „Domänen-Admins“ zum Attribut „sidHistory“ eines gehackten normalen Benutzers). Bei diesem Vorgehen wird die herkömmliche SIEM-basierte Protokollierung umgangen, da der unbefugte DC die Änderungen nicht meldet. Stattdessen werden Änderungen direkt in den Replikationsdatenstrom der Produktions-Domänencontroller eingefügt.

Änderungen an einer Gruppenrichtlinie

Bei einem dokumentierten Angriff mit der Ransomware Ryuk wurden Änderungen an einem Gruppenrichtlinienobjekt vorgenommen, das die Installation von Ryuk auf Remote-Endpunkten im Zielunternehmen erzwang. Standardmäßig enthalten Ereignisprotokolle keine Details zu den Änderungen an einer Gruppenrichtlinie. Wenn also ein Angreifer eine böswillige Änderung vornimmt (wie im Fall von Ryuk), findet sich im Protokoll nur ein Hinweis, dass ein Konto mit Zugriff auf die Gruppenrichtlinie diese geändert hat, was durchaus normal ist.

Zerologon-Angriff

Nachdem Exploit-Code als Machbarkeitsstudie veröffentlicht worden war, konnte ein Angreifer mit Netzwerkzugriff auf einen Domänencontroller spezielle Netlogon-Befehle senden, deren Zeichenfolgen lediglich Nullen enthielten und so erzwingen, dass das Kennwort für den Domänencontroller in eine leere Zeichenfolge geändert wurde. Wenn eine Anmeldung nicht mehr erforderlich ist, hat ein Angreifer Vollzugriff auf den Domänencontroller, kann beliebige Änderungen an AD vornehmen und auf diesem Weg auch in andere Systeme Ihrer Infrastruktur eindringen. Es ist höchst unwahrscheinlich, dass Ihre Überwachungstools nach unangekündigten Kennwortänderungen auf Ihren Domänencontrollern Ausschau halten.

Dass solche Angriffe keine Spuren hinterlassen, ist kein Zufall, sondern durchaus gewollt. Kriminelle verbringen extrem viel Zeit damit, die Funktionen ihrer Zielumgebungen auszuspionieren und Möglichkeiten zu finden, Erkennungsmethoden – also auch Protokolle – zu umgehen und zu täuschen.

Da diese Art von Angriffen nun einmal Realität ist, stellt sich die Frage, was Sie dagegen unternehmen können – sowohl proaktiv als auch reaktiv.

Schutz vor böswilligen Active Directory-Änderungen

Es gibt drei Methoden zum Schutz Ihres Unternehmens vor böswilligen AD-Änderungen:

- **Überwachung von AD auf böswillige Änderungen:** Dies geht über SIEM hinaus und erfordert eine Lösung eines Drittanbieters, die jede einzelne Veränderung innerhalb von AD erkennt – unabhängig davon, wer sie auf welchem DC mit welcher Methode usw. vornimmt. Idealerweise ist diese Lösung in der Lage, den Replikationsdatenverkehr der Domänencontroller selbst mitzulesen und zu interpretieren. Dabei müssen auch Änderungen an den Gruppenrichtlinien berücksichtigt werden. In vielen AD-Überwachungslösungen können spezifische geschützte Objekte für die Überwachung auf Änderungen – beispielsweise an den Mitgliedern der Gruppe „Domänen-Admins" – festgelegt werden, sodass bei jeder Modifikation dieser Objekte ein Warnhinweis ausgegeben wird. Die Lösung sollte nicht nur Änderungen an Gruppenrichtlinien abdecken, sondern auch für Transparenz in Bezug auf die Replikation sorgen.

- **Ausschau halten nach DCShadow:** Mimikatz hinterlässt Spuren in Form von Artefakten und es gibt einige Anzeichen für den Einsatz von DCShadow im Netzwerk. Im Rahmen von regelmäßigen Überprüfungen der AD-Sicherheit müssen auch diese Anzeichen berücksichtigt werden. Sobald Sie Spuren von Mimikatz DCShadow in Ihrer Umgebung entdecken, müssen Sie schnell handeln, denn sicherlich sind Sie bereits einem Angriff zum Opfer gefallen. An diesem Punkt werden Sie sich wünschen, Sie hätten zusätzlich eine Lösung, die Ihnen alle Änderungen auf der Replikationsebene auflistet, damit Sie diese analysieren und idealerweise rückgängig machen könnten.

- **In der Lage sein, AD wiederherzustellen:** Ihr Unternehmen muss über die Fähigkeit verfügen, bei Verdacht auf einen erfolgreichen Angriff die komplette AD-Umgebung aktiv wiederherzustellen. In manchen Fällen eignen sich Datensicherungen und eine Notfallwiederherstellungsstrategie für die Wiederherstellung von AD nach einem Cyberangriff. Sollte es tatsächlich erforderlich sein, den gesamten AD-Forest wiederherzustellen, weil Sie möglicherweise einem Malware-Angriff zum Opfer gefallen sind, machen Sie sich bewusst, dass ein funktionierendes Domänencontroller-Backup nicht mit einer nahtlosen und schnellen AD-Wiederherstellung gleichzusetzen ist. Es empfiehlt sich, das gesamte Wiederherstellungsverfahren regelmäßig anhand des umfangreichen Leitfadens für die Wiederherstellung des Active Directory-Forests von Microsoft zu proben. Ebenso sinnvoll ist es aber auch, nach Lösungen zu suchen, die Änderungen bis auf die Attributebene rückgängig machen können oder sogar in der Lage sind, Änderungen an geschützten Objekten bei ihrer Erkennung automatisch rückgängig zu machen.

Gezielte Angriffe auf Active Directory und dessen Anpassung an die eigenen Zwecke sind heutzutage eine derart übliche Strategie von Cyberkriminellen, dass die bisherige Erkennungsmethode mittels Beobachtung von AD-Überwachungsereignissen immer mehr an Bedeutung verliert. Unternehmen, die auf die Sicherheit und Integrität ihrer AD-Umgebung Wert legen, müssen nach zusätzlichen Möglichkeiten suchen, sich Einblicke in jede einzelne AD-Änderung zu verschaffen und diese bei Bedarf rückgängig zu machen oder die Umgebung wiederherzustellen.

Kennen Sie die Sicherheitslücken ihres Active Directory?

VON **SEAN DEUBY,** *Director of Services bei Semperis*

Zur Absicherung von Microsoft Active Directory (AD) müssen unterschiedliche Risiken berücksichtigt werden, von Administrationsfehlern bis hin zu nicht gepatchten Schwachstellen. Wir schreiben immer wieder darüber, dass Cyberkriminelle AD ins Visier nehmen, um Berechtigungen zu erweitern und sich so im Unternehmensnetzwerk dauerhaft einzunisten. Wenn Sie typische Systemeinbrüche untersuchen, werden Sie feststellen, dass in der Regel gestohlene Anmeldedaten verwendet wurden, um ins Netzwerk einzudringen oder sich Zugang zu kritischen Systemen zu verschaffen und dadurch dem betroffenen Unternehmen zu schaden.

Die Absicherung von AD beginnt damit, die Schwachstellen und üblichen Konfigurations- und Administrationspannen in den Griff zu bekommen, die Angreifern den Weg ebnen. Administratoren, die AD verteidigen wollen, müssen wissen, wie Kriminelle zum Eindringen in ihre Umgebung vorgehen. Wie viele von ihnen könnten aber sämtliche Arten von Sicherheitslücken auflisten, die böswillige Akteure bei ihren Angriffen ausnutzen?

Authentifizierungsfehler

Es entbehrt nicht einer gewissen Ironie, dass die häufigsten und schädlichsten AD-Konfigurationsfehler mit der Authentifizierung zu tun haben. Angenommen, ein Unternehmen möchte einer Anwendung von Drittanbietern oder aus eigener Entwicklung Zugriff gewähren. Die Anwendung selbst bietet keine Integration mit AD, soll aber trotzdem aktive Benutzer von AD abrufen können. Dies lässt sich am einfachsten bewerkstelligen, indem der anonyme Zugriff auf Active Directory aktiviert wird. Aus Sicht der Produktivität ist dies für vielbeschäftigte Administratoren ein durchaus sinnvolles Vorgehen, allerdings sind dadurch auch nicht authentifizierten Benutzern AD-Abfragen möglich. Wird diese Funktion ohne einschränkende Sicherheitskontrollen aktiviert, ergibt sich ein deutlich höheres Risikoprofil für das ganze Unternehmen.

Die 2020 aufgedeckte Zerologon-Schwachstelle wurde innerhalb kürzester Zeit von Angreifern ausgenutzt, denn sie ermöglichte es, das Kennwort für einen Service-Account auf einem Domänencontroller zu ändern oder ganz zu entfernen. Ein erfolgreicher Exploit kann katastrophale Folgen haben. Schwache, zeitlich unbegrenzte oder fehlende Kennwörter sind Anzeichen für die mangelhafte Sicherheit der AD-Umgebung eines Unternehmens.

Richtlinien für sichere Kennwörter sind für die gesamte Active Directory-Infrastruktur unverzichtbar. Jedes Konto, bei dem das Attribut PASSWD_NOTREQD gesetzt ist, muss genauestens daraufhin untersucht werden, ob es einen triftigen Grund für diese Konfiguration gibt. Darüber hinaus müssen Kennwörter – vor allem solche von Dienstkonten – regelmäßig geändert werden. Kennwörter, die über längere Zeiträume hinweg nicht geändert werden, erhöhen die Wahrscheinlichkeit einer erfolgreichen Brute-Force-Attacke, da Angreifer mehr Zeit haben, Kombinationen durchzuprobieren.

- Computer und gruppenverwaltete Service-Accounts (gMSA), deren Kennwörter vor mehr als 90 Tagen festgelegt wurden
- Kennwörter mit umkehrbarer Verschlüsselung, die in Gruppenrichtlinienobjekten (GPOs) enthalten sind
- Anonymer Zugriff auf Active Directory aktiviert
- Ungepatchte Zerologon-Schwachstelle (CVE-2020-1472)

Folgende Authentifizierungsprobleme müssen im Blick behalten werden:

Übermäßige Berechtigungen zugelassen

Da die meisten AD-Umgebungen schon seit vielen Jahren in der Produktion eingesetzt werden, hat sich ihre Angriffsfläche vergrößert. Viele Schwachstellen, die sich mit der Zeit in einer Gesamtstruktur angesammelt haben, lassen sich auf ein bestimmtes Muster zurückverfolgen: Jemand muss schnell etwas erledigen und die sicherste Methode ist zu zeitaufwendig, zu kompliziert oder schlicht nicht bekannt. Der Benutzer oder die Gruppe werden daraufhin mit übermäßigen Berechtigungen versehen, um sicherzustellen, dass die Aktion gelingt und das Ticket geschlossen werden kann. Natürlich werden diese zusätzlichen Berechtigungen anschließend nicht mehr entfernt, sodass die Angriffsfläche immer weiterwächst.

In der Praxis ist es nicht unüblich, dass es in AD-Umgebungen unnötig viele Domänenadministratoren gibt – eine Tatsache, die problematisch werden kann, wenn diese Konten verwaist und für Angriffe verwundbar sind. Dienstkonten mit übermäßigen Berechtigungen stellen ebenfalls ein hohes Risiko dar, da ihre Kennwörter in der Regel zeitlich unbegrenzt und in vielen Fällen zu schwach sind (was sie für Kerberoasting-Angriffe interessant macht). Mit steigender Anzahl von Benutzern mit Admin-Berechtigungen wächst auch die Angriffsfläche, die geschützt werden muss. Die Mitgliedschaft in diesen Gruppen muss einer strikten Kontrolle unterliegen.

Natürlich lassen sich Fehler nie ganz vermeiden. Je größer und komplexer eine AD-Umgebung wird, desto schneller passiert es, dass jemand beispielsweise die geerbten Berechtigungen aus dem Blick verliert und einem Konto versehentlich überhöhte Rechte zuweist. Aber selbst eine korrekt verwaltete Zuweisung von Berechtigungen schützt nicht vor aggressiven Angriffen.

Ein Beispiel hierfür sind die Auswirkungen eines AdminSDHolder-Angriffs. Zur Erinnerung: Im AdminSDHolder-Objekt ist die Sicherheitsbeschreibung für privilegierte Gruppen gespeichert. In der Standardeinstellung vergleicht der SDPROP-Prozess (Security Description Propagation) alle 60 Minuten die Berechtigungen für geschützte Objekte und setzt sie bei Abweichungen auf die Definition gemäß dem AdminSDHolder-Objekt zurück.

Bei einem AdminSDHolder-Angriff nutzen Kriminelle SDPROP aus, um die Berechtigungen eines Objekts durch die unzulässigen Änderungen des Angreifers zu ersetzen und sich so im System permanent einzunisten. Wenn zwar die Berechtigungsänderungen erkannt und rückgängig gemacht werden, die Änderungen des AdminSDHolder-Objekts dagegen unerkannt bleiben, werden die Modifizierungen des Angreifers wiederhergestellt.

Die beste Verteidigung gegen den Missbrauch von Rechten ist die Prüfung von Berechtigungen und die Überwachung auf verdächtige Aktivitäten.
Folgende Berechtigungsprobleme müssen im Blick behalten werden:

- Privilegierte Objekte mit nicht privilegierten Besitzern
- Geänderte Berechtigungen im AdminSDHolder-Objekt
- Nicht privilegierte Benutzer mit Synchronisierungsrechten für Domänencontroller in der Domäne
- Änderungen des Default Security Descriptor Schemas innerhalb der letzten 90 Tage

*To defend AD, administrators **need to know** how attackers are targeting their environment.*

DIE GRÖSSTEN SICHERHEITSRISIKEN BEI DER UMSTELLUNG AUF HYBRIDES IDENTITÄTSMANAGEMENT

VON **DOUG DAVIS,** *Senior Product Manager bei Semperis*

Es ist durchaus nachvollziehbar, dass Unternehmen verstärkt auf eine hybride Identitätsverwaltung setzen, die eine optimale Kombination aus Cloud- und lokalen Systemen verspricht. In einer auf Active Directory ausgerichteten Umgebung setzt die Nutzung der Cloud die Integration mit Azure Active Directory voraus.

Schließlich wurde bei der Entwicklung von Azure Active Directory (AAD) auch an SaaS-Anwendungen gedacht, die Single Sign-On und Zugriffskontrolle ermöglichen. Mit zunehmender Akzeptanz der Cloud gewinnt die Fähigkeit, sowohl den lokalen als auch den Cloud-Zugriff verwalten zu können, immer mehr an Bedeutung. Durch die parallele Nutzung von AAD und Active Directory (AD) wird Hybrid-Identitätsverwaltung Wirklichkeit.

Wie in allen Bereichen der IT gilt allerdings auch hier der Grundsatz: Vorsicht ist besser als Nachsicht.

Monumentale Veränderungen durch die Verlagerung in die Cloud

Jede Verlagerung von IT-Betriebsabläufen in die Cloud erfordert Anpassungen. Das gilt auch für die Benutzerauthentifizierung. Bei der Ausarbeitung eines Konzepts müssen Unternehmen drei wichtige Aspekte berücksichtigen.

1. Ein neues Authentifizierungsmodell

Nachdem 20 Jahre lang eine bestimmte Methode zur Identitätsverwaltung etabliert war, bringt die Integration von AAD zahlreiche Umstellungen mit sich. Der Wechsel von einem rein lokalen AD zu einem System mit Cloud-Authentifizierung erfordert ein Umdenken und einen ganz neuen Ansatz. Bei AAD gibt es weder Organisationseinheiten oder Gesamtstrukturen noch Gruppenrichtlinienobjekte. Die bisweilen mühsam erarbeiteten Konzepte zur Absicherung von Identitäten in AD treffen auf AAD nicht mehr zu.

Viele Administratoren sind zunächst der Auffassung, die Absicherung von AAD sei der Absicherung von AD sehr ähnlich, was aber nicht der Fall ist. Hinzu kommt, dass Sie AAD vielleicht schon verwenden, ohne sich dessen bewusst zu sein. Wenn in Ihrem Unternehmen Microsoft Clouddienste eingesetzt werden, wie etwa Office 365, dann läuft AAD bereits im Hintergrund. AAD wird zudem intensiv zur Vernetzung mit SaaS-Anwendungen von Drittanbietern genutzt, beispielsweise Salesforce. All diese Faktoren bringen neue Überlegungen und Auswahlmöglichkeiten mit sich, wie etwa die Frage, ob AD und AAD getrennt bleiben oder mithilfe von Azure AD Connect zusammengeführt werden sollten. Viele neue Konzepte müssen verstanden werden, damit Sie diese Entscheidungen treffen können, ohne die Sicherheit der Informationssysteme zu gefährden.

2. Erweiterung des Perimeters

Mit dem Umstieg auf die Cloud fällt der herkömmliche Netzwerkperimeter weg. IT-Administratoren, die zwei Jahrzehnte lang mit einem lokalen AD gearbeitet haben, verlangt dies ein enormes Umdenken ab. In einer Umgebung mit Hybrid-Identitätsverwaltung müssen Unternehmen sich darauf einstellen, eine schier endlose Zahl von potenziellen Angriffspunkten abzusichern.

3. Radikale Änderungen beim Berechtigungsmodell

Der Umstieg auf AAD bringt auch drastische Veränderungen beim Berechtigungsmodell, das Unternehmen absichern müssen, mit sich. Auf lokaler Ebene lässt sich der physische Zugriff auf Domänencontroller relativ unkompliziert kontrollieren und insgesamt sind die Zugangspunkte für die Verwaltung präzise definiert und dokumentiert. In einer Hybrid-AD-Umgebung sind Identitäten zusätzlich in der Cloud gespeichert und damit anfällig für Angriffe aus dem Internet. Plötzlich müssen sich Administratoren mit einem von Natur aus offenen Zugriffsmodell befassen, durch das sich – in Kombination mit der größeren Anzahl von erforderlichen Diensten, Rollen und Berechtigungen – das Risiko deutlich erhöht.

Microsoft stellt aktiv Schulungsressourcen bereit, um Unternehmen zu helfen, sich auf die Veränderungen vorzubereiten, die eine Einführung von AAD mit sich bringt. Allerdings sind sich viele IT-Organisationen nach wie vor der umfangreichen Auswirkungen einer Hybrid-Identitätsverwaltung nicht bewusst. Da immer mehr Unternehmen auf ein Hybrid-Modell setzen, haben auch Angreifer ihre Methoden entsprechend ausgebaut.

Im September 2020 meldeten Forscher bei Mandiant (FireEye) eine Häufung von Vorfällen in Verbindung mit Microsoft 365 und Azure Active Directory, bei denen überwiegend über Phishing-E-Mails versucht wurde, die potenziellen Opfer zur Eingabe ihrer Anmeldedaten für Office 365 auf einer Phishing-Website zu bewegen. Die Forscher beobachteten darüber hinaus die Verwendung eines PowerShell-Moduls namens „AADInternals“, mit dem sich Angreifer von der lokalen Umgebung aus Zugang zu AAD verschaffen, Backdoors einrichten, Kennwörter abgreifen und andere schädliche Aktivitäten durchführen konnten. Mit dem exponentiellen Wachstum des Interesses an Azure und Office 365 werden auch solche Angriffe zunehmen.

Berechtigungen, Berechtigungen, Berechtigungen

Von den drei oben genannten Themen stellen die Änderungen am Berechtigungsmodell das mit Abstand größte Sicherheitsrisiko dar. Durch die Umstellung auf eine Umgebung mit Hybrid-Identitätsverwaltung sind in Unternehmen zahlreiche neue Dienste verfügbar. Anstelle von präzise definierten Administrationsgruppen in Active Directory gibt es in Azure AD Rollen und dieses Konzept mag zunächst wenig vertraut sein. Eine Liste dieser Rollen finden Sie hier. Für jede Rolle gibt es eine lange Liste von zugewiesenen Berechtigungen. Die Bedeutung der einzelnen Berechtigungen lässt sich allein anhand der Beschreibung nicht ohne Weiteres verstehen und der Zugriff ist in vielen Fällen sehr umfangreich, was nicht unbedingt offensichtlich ist.

Zudem werden durch die Verknüpfung von SaaS-Diensten mit AAD – was vermutlich das Hauptargument für die Einführung von AAD war – weitere Berechtigungsmodelle hinzugefügt, die ebenfalls verwaltet werden müssen. Microsoft Teams nutzt beispielsweise die SharePoint-Integration im Backend. Bei einer fehlerhaften Konfiguration ist ein Gast, der zu Teams hinzugefügt wird, möglicherweise in der Lage, auf Dateien zuzugreifen, die in SharePoint für Teams gespeichert sind. Die anderen Mitglieder sind sich nicht unbedingt darüber im Klaren, dass ein Gastbenutzer, der ihrem Kanal nur für ein kurzes Gespräch hinzugefügt wurde, über Zugriffsrechte für diese Dateien verfügt. Darüber hinaus weitet die Möglichkeit, Apps in Teams hinzuzufügen, im Wesentlichen das Berechtigungsmodell auf diese Apps von Drittanbietern aus. Dies ist nur ein Beispiel für die zahlreichen komplexen Probleme, die jeder einzelne über AAD verwaltete Dienst verursachen kann.

Die Berechtigungen der Apps von Drittanbietern im Griff zu behalten, ist extrem wichtig und bei den meisten AAD-Implementierungen hat dieser Bereich eine zu geringe Priorität. Eine solche Berechtigungsanforderung löst eine einmalige Popupmeldung aus, in der sämtliche von der App benötigten Berechtigungen aufgelistet sind. Auch wenn diese Listen sehr lang sein können, müssen sie vor der Bestätigung sorgfältig durchgesehen werden, was allerdings selten geschieht.

Unternehmen können in Verbindung mit Berechtigungen auch mit den folgenden beiden neuen Szenarien konfrontiert werden, die im Sicherheitskontext verstanden werden müssen:

- **Tools von Drittanbietern, die Daten von Azure AD abrufen und in einer eigenen Datenbank speichern.** Beispielsweise ist eine in Azure AD registrierte Anwendung, die einem CRM-System das Lesen von Benutzerprofilen oder anderen Informationen ermöglicht, grundsätzlich in der Lage, Daten abzurufen und selbst zu speichern. Diese Daten befinden sich dann zusätzlich in einer externen Datenbank und das Unternehmen muss sich auf das Sicherheitsframework des Tools von Drittanbietern verlassen.

- **Tools von Drittanbietern mit Schreibzugriff, die Änderungen am Mandanten vornehmen können.** In diesem Fall wird die erforderliche Authentifizierung für Änderungen am Mandanten von Azure AD auf die entsprechenden Funktionen des externen Tools übertragen. Möglicherweise kann sich ein Benutzer ohne Multi-Faktor-Authentifizierung beim Tool anmelden, da dieses keine Unterstützung für Single Sign-On (SSO) bietet. Stattdessen agiert die Anwendung als Berechtigungs-Proxy und führt die Aktion ohne die sonst erforderlichen Prüfungen durch.

IT-Organisationen sollten unbedingt beschränken, welche Benutzer Anmeldungen zulassen dürfen oder zumindest eindeutige Richtlinien dazu herausgeben, welche Berechtigungen angemessen sind und welche nicht. Bei einem Hybrid-Ansatz in Bezug auf Identitäten muss ein deutlich umfangreicheres Berechtigungsmodell verwaltet werden. Dies ist nur dann effektiv möglich, wenn Unternehmen klare Richtlinien aufstellen und durchsetzen, welche Apps aktiviert werden dürfen und welche Zugriffsrechte sie erhalten.

Das Risiko einer Hybrid-Identitätsverwaltung verstehen

Unabhängig davon, ob Authentifizierung lokal, in der Cloud oder in beiden erfolgt, muss die Sicherheit immer an erster Stelle stehen. Die Verwaltung einer Identität mag so trivial erscheinen wie das Einbinden eines Windows-Geräts in AAD. Wer aber die sich ständig ändernden Risiken außer Acht lässt, öffnet Problemen Tür und Tor, die auch langfristig schwerwiegende Folgen haben können. Wissen ist immer die beste Verteidigung, allerdings wirkt die riesige Menge an Dokumentation zur AAD-Sicherheit abschreckend. Tools aus eigener Entwicklung oder von Drittanbietern, mit denen die komplexen Zusammenhänge besser verstanden und Abläufe automatisiert werden können, tragen dazu bei, das Sicherheitsrisiko während und nach der Einführung der Hybrid-Umgebung zu mindern.

NEUE PERSPEKTIVEN ZUM SCHUTZ VON HYBRIDEN IDENTITÄTEN

Von Experten für Identitätssicherheit auf der #HIPEurope2021

„Wenn ein Angreifer sich Zugriff auf AD verschafft hat, zählt jede Sekunde. Wir müssen dafür sorgen, dass der Angriff nicht auf alle Active Directory-Forests ausgeweitet werden kann. Wir müssen den Angriffsvektor analysieren, die potenziellen Folgen überschlagen und ein Sicherheitsnetz etablieren. Außerdem müssen wir AD innerhalb von Stunden statt Tagen wiederherstellen.“

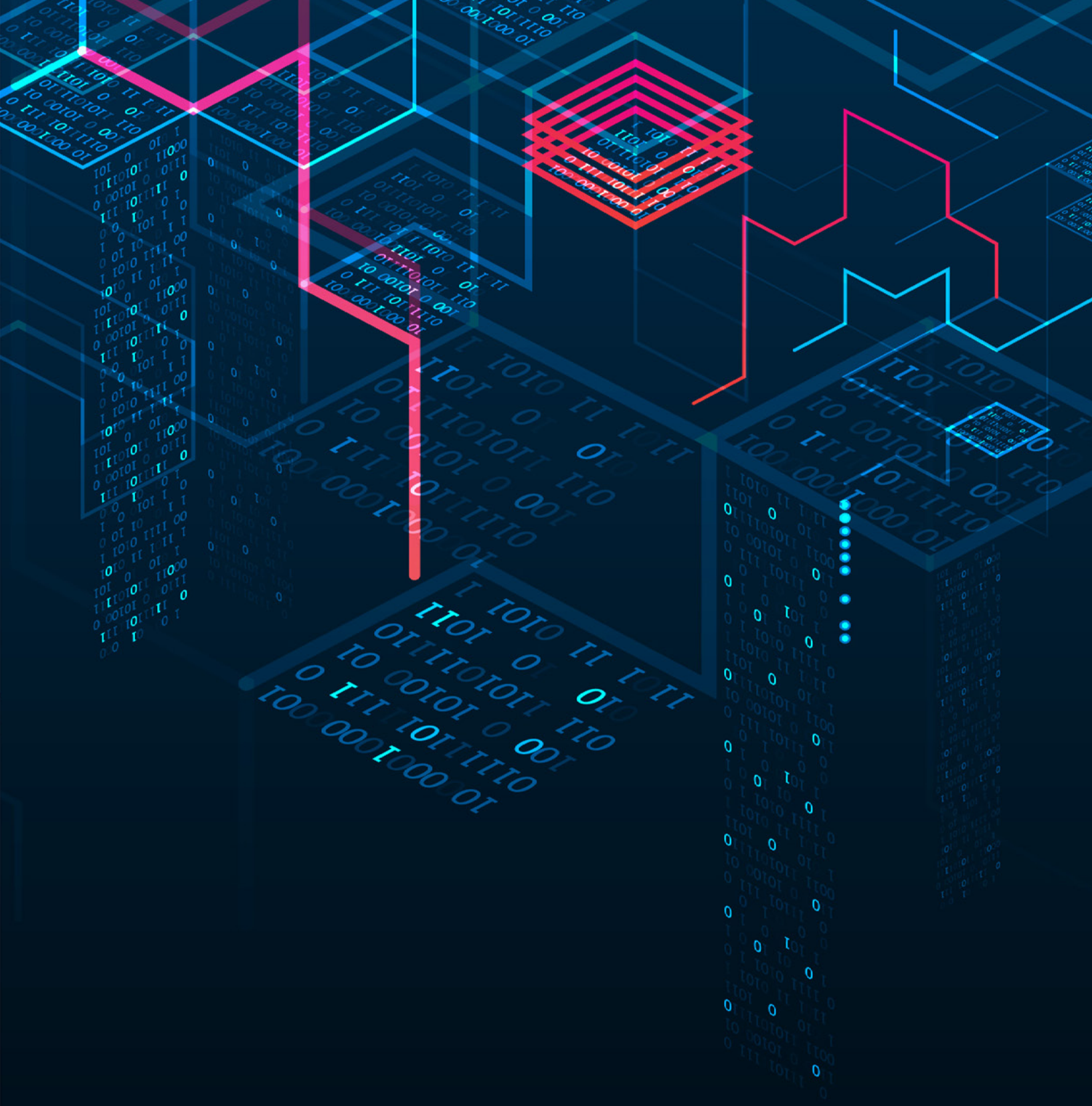
Ben Cauwel
Security Delivery Manager bei Accenture

„Heutzutage ist eines der größten Probleme mit der Cloud-Sicherheit, dass nicht überall das gemeinsame Verantwortlichkeitsmodell verstanden wird.“

Jan de Clercq
Senior Security Architect bei HPE

Pamela Dingle
Director of Identity
Standards bei Microsoft

„An alle da draußen, die noch keine MFA implementiert haben: Sie müssen ihre Prioritäten neu definieren!
Angreifer finden Wege, um in Ihre Unternehmensinfrastruktur einzudringen und nutzen dann die Tatsache aus, dass einige von Ihnen die wahnwitzige Vorstellung haben, dass nur weil die Benutzer vor Ort sind, sie auch vertrauenswürdig wären. Kompromittierungen sind kompliziert, teuer und folgenschwer. Ich will damit nicht sagen, dass die Implementierung von MFA einfach ist, aber die Alternative ist außerordentlich schwerwiegend.“



semperis

semperis.com