Gefühlt sicher: Sicherheitsmythen und -irrtümer

Viele Halbwahrheiten, Glaubensfragen und veraltete Weisheiten bestimmen die IT-Sicherheit. Den Verantwortlichen ist nicht bewusst, wie sehr das die Unternehmens-IT gefährden kann.

Von Frank Ully

Admins oder Sicherheitsverantwortliche fühlen sich oft sicher, obwohl sie es gar nicht sind. Die Daten und damit vermeintlich die Verantwortung sind in die Cloud abgewandert, eine Richtlinie erfordert komplexe Passwörter und ein zweiter Faktor schützt mit Push-Nachrichten gegen illegitime Anmeldeversuche.

In der Praxis sind das Irrtümer, die Angreifer sich zunutze machen. Sie missbrauchen Fehlkonfigurationen. Sie finden komplexe, aber unsichere Passwörter und melden sich damit aus dem Internet an Diensten der Organisation an. Und sie können oft die Abfrage eines zweiten Faktors umgehen.

Dieser erste von zwei Artikeln beschreibt verbreitete Sicherheitsmythen und was wirklich stimmt und hilft. Verteidiger sollten wissen, wie Angreifer denken, und deren Sichtweise verstehen. Schließlich schützen sie sich nicht im luftleeren Raum vor einer virtuellen Bedrohung, sondern vor echten menschlichen Gegnern und ihrem kreativen Vorgehen.

Der Microsoft-Mitarbeiter John Lambert schrieb den lesenswerten Blogbeitrag „Defender's Mindset", der Verteidigern Erkenntnisse aus seiner Berufspraxis mitgibt (dieser und die weiteren hier zitierten Artikel und Angriffe sind über ix.de/z9xw zu finden). Lambert ist der Leiter des Threat Intelligence Centers von Microsoft. Sein Bonmot „Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win" fasst das Vorgehen von Angreifern zusammen, die Abhängigkeiten ausnutzen, während Verteidiger daran denken, wie sie die einzelnen Systeme absichern. Es beschreibt gut die Funktionsweise des Active-Directory-Angriffswerkzeugs BloodHound, das Angriffspfade grafisch darstellt und das in der Artikelreihe zu Microsofts On-Premises-Verzeichnisdienst genauer vorgestellt wurde [1].

In seinem Blogartikel teilt Lambert weitere Erkenntnisse über das Verteidigen. Wie dessen Titel nahelegt, geht es nicht um bestimmte Angriffstechniken, sondern die zugrunde liegende Denkweise: die Denkweise von Angreifern und was das für die Denkweise von Verteidigern bedeutet.

iX-TRACT

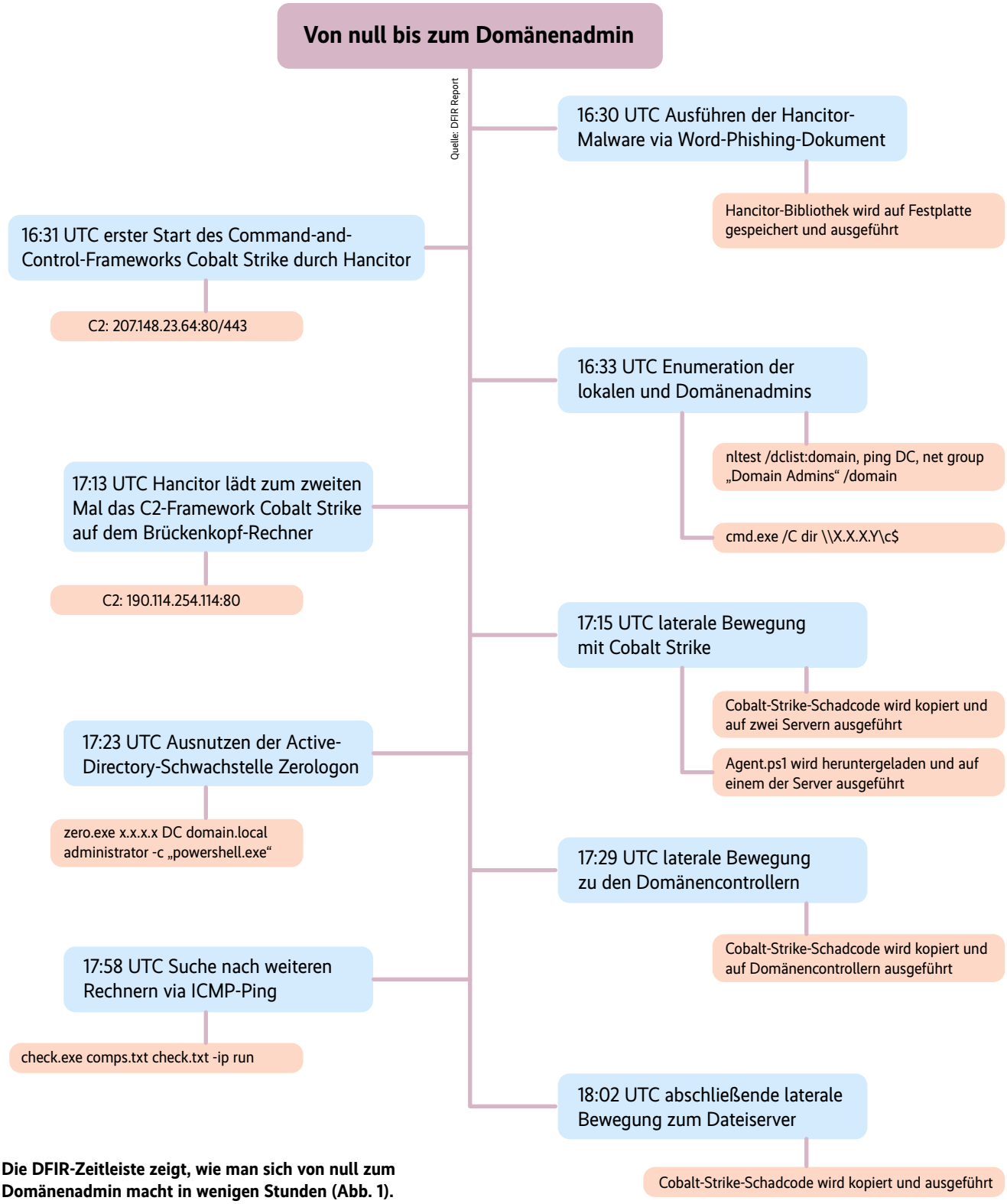
- Oft fühlen sich Admins oder Sicherheitsverantwortliche fälschlicherweise sicher: Policies einzuführen und Sicherheitssoftware einzusetzen schützt nicht vor schlechten Implementierungen oder Fehlkonfigurationen, die Angreifern Tür und Tor öffnen.
- Mangelnde IT-Sicherheitsbestrebungen hängen auch mit dem Verdrängungstalent der Menschen zusammen: Die Gefahr kann noch so präsent sein, man glaubt nicht, dass es einen selbst treffen wird.
- Um sich gut zu verteidigen, muss man wissen, wie die Angreifer ticken. Das betrifft weniger die technische Seite als die grundsätzliche Denkweise von Angreifern.

„Uns trifft es eh nicht"

Der Mensch neigt dazu, in seinem Alltag lauernde Gefahren nicht wahrzunehmen. Wer beim Autofahren Textnachrichten verschickt, würde dies nicht tun, wenn er wirklich glaubte, er könnte derjenige sein, dessen Körper von der Feuerwehr aus dem Autowrack herausgeschnitten wird. Der in der Informationstechnik beschäftigte Mensch glaubt, seinen Systemen werde nichts Schlimmes passieren. Erpressergangs würden sie nicht in Geiselhaft nehmen – während er auf heise Security von den jüngst lahmgelegten Industrieunternehmen, Stadtverwaltungen oder Hochschulen liest.

Dabei kann es jeden treffen, ob über eine Website, eine Kundendatenbank oder einfach ein paar Rechner in einem Active Directory, an denen Mitarbeiter E-Mails lesen und im Web surfen – sie alle sind anfällig für Cyberangriffe.

Viele Angriffe beginnen mit Scans, die im gesamten Internet nach verwundba-



Die DFIR-Zeitleiste zeigt, wie man sich von null zum Domänenadmin macht in wenigen Stunden (Abb. 1).

ren Systemen suchen. Automatisiert spüren Angreifer beispielsweise ungepatchte Exchange-Mailserver auf oder Remote-Desktop-Zugänge, an denen sie massenweise Passwörter ausprobieren. Als Einfallstor können ebenso Phishingmails dienen oder in Google-Suchergebnisse eingeschleuste Schadsoftware-Downloadseiten. Wer glaubt, die eigene IT gesichert zu haben, kann in einen Angriff auf die Lieferkette verwickelt werden, wie bei SolarWinds oder Kaseya. Die europäische Cybersicherheitsagentur ENISA hat umfangreiche Berichte zu Ransomware, Supply-Chain-Angriffen und zur allgemeinen Bedrohungslage veröffentlicht (siehe ix.de/z9xw).

Unterschätzte Folgen

Eine Variante des Irrtums „Mich trifft es ohnehin nicht“ ist „Mich hat es bislang noch nie erwischt“. Nur weil Verantwortliche selbst noch nicht von einem Sicherheitsvorfall betroffen waren, unterschätzen sie, welche Verwüstung er anrichten kann. Verwüstung im Unternehmen, das nach einem Betriebsstillstand in die Insolvenz rutschen kann wie der Fahrradhersteller Prophete. Verwüstung bei Mitarbeitern, die durch den stressigen Vorfall und die folgenden wochen-, oft monatelangen Aufräumarbeiten an Burn-out erkranken. Laut Statistiken der ENISA kostet ein Sicherheitsvorfall im Durchschnitt 200 000 Euro.

Überdies kann das Unternehmen schon kompromittiert sein – und hat es nur noch nicht entdeckt. Das ist besonders dann wahrscheinlich, wenn Verantwortliche nichts tun, um verdächtige Aktivitäten zu erkennen. Die wenigsten Un-

iX-Workshops zum Absichern Ihrer IT-Infrastruktur

Das iX-Magazin veranstaltet unter dem Dach der Lernplattform heise Academy Workshops zu verschiedenen Sicherheitsthemen. Im Workshop **Digital Forensics & Incident Response** lernen Teilnehmer, wie sie im Falle eines Cybervorfalls wie eines Ransomware-Angriffs oder Business Email Compromise richtig und angemessen reagieren sowie forensische Artefakte sammeln und interpretieren können.

Wie man seine Active-Directory-Umgebung vor Eindringlingen und Missbrauch schützt, kann man vom Autor dieses Artikels im Workshop **Angriffsziel lokales Active Directory: effiziente Absicherung** erfahren. Denn nach wie vor ist diese Schaltzentrale vieler Unternehmensnetze ein beliebtes Ziel von Ransomware und anderen Angriffen. Das gilt auch für das Azure Active Directory. Im Workshop **Angriffe auf und Absicherung von Azure Active Directory** zeigt Frank Ully, wie Angreifer Fehlkonfigurationen der Microsoft-Cloud und fehlende Härtungsmaßnahmen ausnutzen und mit welchen Maßnahmen man das verhindern kann.

Alle drei Workshops finden online statt, die Termine für das laufende Jahr sind über ix.de/z9xw zu finden.

ternehmen merken selbst, dass sie gehackt wurden. Laut Verizon Data Breach Investigations Report 2022 (DBIR; siehe ix.de/z9xw) informieren meist Externe wie Sicherheitsforscher oder Behörden über einen Vorfall. In den vergangenen Jahren machten oft die Angreifer auf einen Vorfall aufmerksam, indem sie Lösegeld forderten oder die Unternehmensdaten in einem Untergrundforum zum Verkauf anboten.

„Wir sind nicht wichtig und interessant genug und haben nichts zu verbergen“

Einige Organisationen glauben, wegen ihrer unspektakulären Branche oder ihres gewöhnlichen Geschäftsmodells hätten es Hacker nicht auf sie abgesehen. Nach manchen Berichten über Cyberangriffe könnte man annehmen, dass es in erster Linie Große erwischt. Das Gegenteil ist der Fall: Laut DBIR sind kleinere und mittlere Unternehmen mit weniger als tausend Mitarbeitern doppelt so häufig von Angriffen betroffen wie größere Organisationen, zumindest in den Fällen, die sich der Unternehmensgröße zuordnen lassen. Das überrascht nicht, denn der Großteil der Unternehmen hierzulande zählt zu den KMU.

Kleinere und mittlere Organisationen werden häufig Zufallsopfer von massenhaft ausgeführten Eindringversuchen über Phishing oder ungesicherte aus dem Internet erreichbare Systeme. Sie fallen solchen Angriffen wahrscheinlicher zum Opfer, denn es fehlt an Personal und Budget für kostspielige Securitylösungen. Viele Cyberkriminelle nehmen sie eher ins Visier als größere Unternehmen.

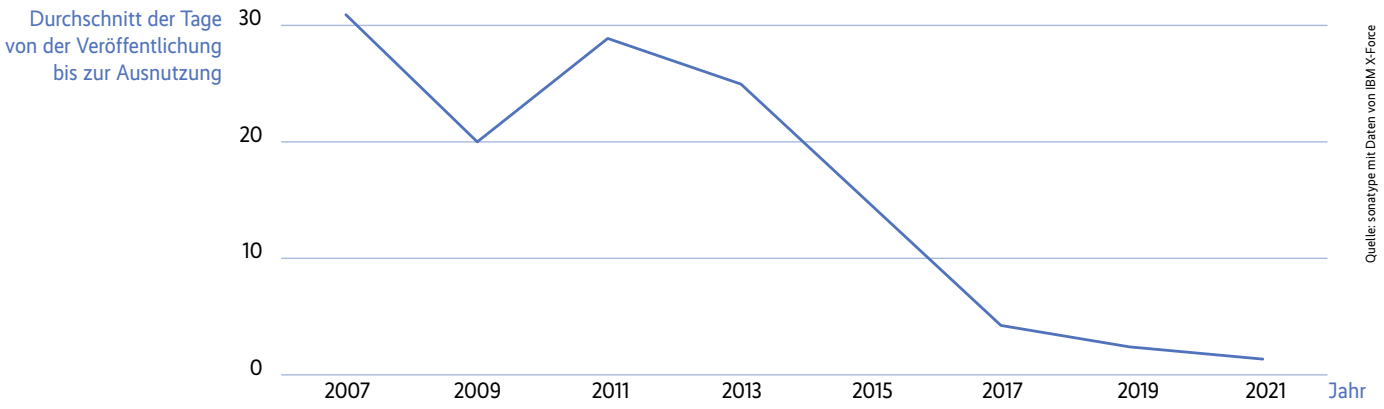
Der Tätergruppe der Initial Access Broker (IAB) beispielsweise geht es nicht um ein spezielles Opfer. Sie verkaufen den initialen Zugang in ein Unternehmensnetzwerk meistbietend auf dem Schwarzmarkt (siehe ix.de/z9xw).

Die meisten Angriffsversuche stammen von Opportunisten auf der Suche nach leichter Beute. Es spielt keine Rolle, ob man eine weltweit bekannte Marke ist oder ein Tante-Emma-Laden. Verfügt eine Organisation über irgendeine Art von Daten, die es wert sind, gestohlen zu werden, muss sie sich als potenzielles und wahrscheinliches Ziel für einen Zufallsangriff betrachten. Der Eindringling, der es gezielt auf eine Firma absieht, ist eher selten. Geschäftsführung und Admins sollte daran gelegen sein, kein Routineopfer einer ohne großen Aufwand durchgeführten Massenattacke zu werden.

Gefahr des Bankrotts

Ransomware ist ein Großschadensfall, über den immer prominenter berichtet wird und den Verantwortliche zu Recht fürchten [2]. Wie erwähnt gibt es Fälle, in denen Unternehmen aufgrund eines Angriffs ihre Geschäftstätigkeit einstellen müssen, weil sie bankrottgehen, und nicht, weil ihr Ruf ruiniert ist, wie man es vielleicht eher erwarten würde. Im Allgemeinen sind Kriminelle nicht darauf aus, eine Firma in den Konkurs zu treiben. Vielmehr wollen sie unmittelbar Geld erpressen, eine Hintertür hinterlassen, damit sie oder Dritte wiederkommen können, und Daten kopieren.

Auf dem Schwarzmarkt floriert der Handel mit dem initialen Zugang. Daneben blüht ein schwunghafter Austausch von verwendeten Passwörtern und hinterlegten Zahlungsdaten. Personalakten oder Geschäftskontakte kaufen andere Kriminelle illegal für Spear-Phishing oder gezielte Passwortangriffe. Kompro-



Daten belegen: Das Fenster zum Schließen von Beinahe-Zero-Days wurde in den letzten Jahren immer kleiner (Abb. 2).

Quelle: Mark Simos auf Twitter

„Wir patchen nicht“ ist ein weitverbreitetes Verhaltensmuster verursacht durch:

„Wenn es nicht kaputt ist, fass es nicht an“
aus der Angst heraus, dass Systeme zerbrechlich sind und leicht kaputtgehen können.

Bewährte Praktik – Einführung eines **„Patch by Default“-Modells,** das davon ausgeht, dass die Hersteller aus gutem Grund in Patches investieren, und selbst Patches automatisch anwenden (es sei denn, es treten Probleme durch eine schrittweise Einführung auf).

„Ich akzeptierte das Risiko“,
weil Anreize Verfügbarkeit begünstigen, aber das organisatorische Risiko nicht berücksichtigen.

„Wir wollen keine Ausfallzeiten“,
weil die Prozess- und Systemeigentümer keine Verantwortung für Ausfallzeiten durch Sicherheitsrisiken tragen.

Sie haben die Wahl zwischen Ausfallzeiten, um Patches nach Ihrem Zeitplan anzuwenden oder um Systeme wiederherzustellen nach dem Zeitplan des Angreifers.

Bewährte Praktiken

- **Verantwortlichkeit und Anreize** – Sicherstellen, dass die Business Owner der Systeme verantwortlich sind für Sicherheitswartung und das Risiko der Vernachlässigung.
- **Teamansatz** – Bilden Sie ein Team mit den Verantwortlichen für Anwendungen und Infrastruktur, die dafür zuständig sind, Patches anzuwenden, den Compliance-Verantwortlichen, die unabhängige Audits durchführen, und dem Posture Management, das technische Hilfe bietet.

„Ich warte auf perfekte Patches“
aufgrund der falschen Vorstellung, dass Hersteller perfekte Patches für alle Szenarien anbieten können.

Bewährte Praktik – Integrieren Sie Ausfallsicherheit und Patching in die normalen IT-Betriebsprozesse (Wartungsfenster, Image-Bereitstellung usw.), um die Zuverlässigkeit und Agilität der digitalen Transformation zu erhöhen.

„Uns greift niemand an“,
weil es noch nie passiert ist oder nicht entdeckt wurde.

Bewährte Praktik – Erkennen Sie die aktive Nutzung durch Angreifer und nutzen Sie Branchenrichtlinien, um ein Bewusstsein bei und Unterstützung durch Führungskräfte zu gewinnen, um der Systemwartung Priorität einzuräumen.

Die Hitliste der Ausreden, warum man nicht patcht, und wie man gegensteuern und die Argumente entkräften kann (Abb. 3).

mittierte Server und Clients dienen als Teil eines Botnets für DDoS-Attacken oder sie errechnen Einnahmen durch Cryptomining.

Bei staatlich geförderten Angreifern steht das Abziehen von Daten im Fokus, meist für Industriespionage. Das kann kleine Unternehmen treffen, die sich ihrer Rolle in der Lieferkette [3] nicht bewusst sind — etwa wenn sie ein wichtiges Werkstück für eine Schlüsselindustrie herstellen, auf die Nationalstaaten wie China setzen. Partnerbeziehungen sind für Eindringlinge interessant, wenn sie vom schlechter gesicherten Netzwerk eines angebundenen Zulieferers oder IT-Dienstleisters zum eigentlichen Ziel vordringen, das mehr in Sicherheit investiert.

„Es waren staatlich geförderte Hacker. Da kann man leider nichts machen“

Das Klischee vom Hoodie tragenden hackenden Computergenie ist out, in Wirklichkeit ist Cyberkriminalität arbeitsteilig und erfordert erschreckend wenig technisches Verständnis. Auch der Kriminelle hat geregelte Arbeitszeiten, ein (Heim-) Büro und sitzt zum Abendessen am Familientisch. Einige Mitglieder der gefürchteten Lapsus$-Gang, die Microsoft und T-Mobile kompromittierten, waren Teenager im Keller ihrer Elternhäuser.

Häufig missbraucht: die Werkzeuge der Guten

Die „GitHubifizierung“ der Informationssicherheit (John Lambert in einem anderen Blogartikel; siehe ix.de/z9xw) bewirkt, dass dank der Codeaustauschplattform Sicherheitstester im Auftrag ihrer Kunden deren Systeme mit komplexen und neuen Attacken angreifen. Weniger fähige und böswillige Hacker nutzen die von Experten geschriebenen Tools von GitHub ebenso. Mit einfachen Google-Suchen und zahlreichen YouTube-Tutorials finden Skript-Kiddies ungepatchte Server und richten dort eine Webshell ein. Lambert schlägt in seinem Artikel vor, auch Verteidiger sollten mehr Daten und Werkzeuge kostenfrei teilen.

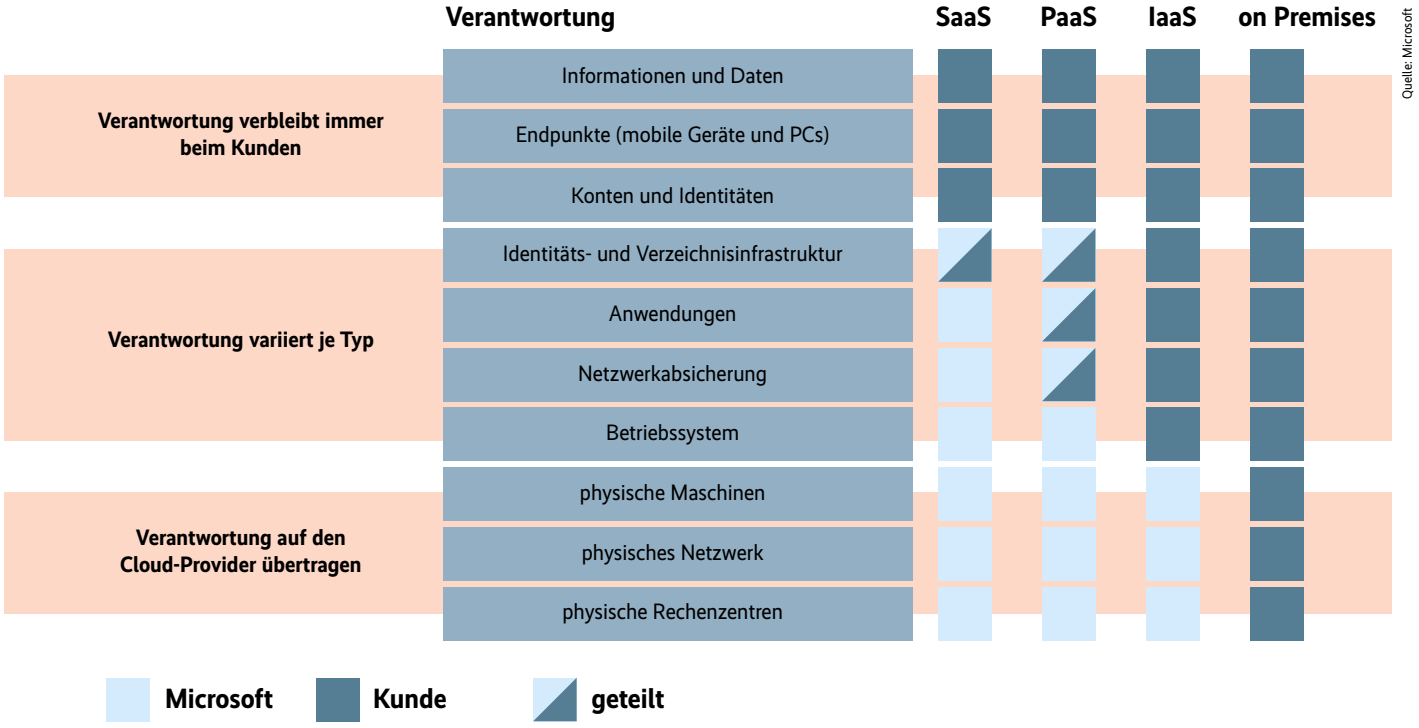
Ransomware as a Service (RaaS) senkt die Schwelle für Angreifer noch weiter [2]. Entwickler von Erpressungssoftware vermieten ihre leicht bedienbaren Werkzeugsammlungen auf einem Schwarzmarkt und bieten Produktsupport an.

Allerdings braucht es häufig noch nicht einmal komplexe oder raffinierte Methoden, um eine Organisation zu kompromittieren und in kurzer Zeit an die Kronjuwelen zu gelangen. Wie Kriminelle vorgehen, zeigt der „DFIR Report“ (DFIR steht für Digital Forensics and Incident Response): Wie sie beispielsweise nach einer Phishingmail in kurzer Zeit eine schlecht gesicherte Active-Directory-Umgebung übernehmen, manchmal in weniger als 24 Stunden, zeigt die DFIR-Zeitleiste in Abbildung 1.

Keine PR-Abteilung will, dass die Berichte über die Datenpanne ihres Unternehmens davon handeln, wie leicht es für die Einbrecher war. Weniger peinlich ist es, wurde man von hochkomplexen und noch nie dagewesenen Hacking-Methoden kompromittiert, die man unmöglich vorhersehen oder abwehren konnte.

„Gegen Zero-Day-Schwachstellen kann man sich sowieso nicht wehren“

Besonders bei Zero-Day-Schwachstellen befürchten Admins und Sicherheitsverantwortliche, dass sie wenig dagegen ausrichten können: Softwarelücken, mit hohem Aufwand von womöglich staatlichen Angreifergruppen gefunden, von denen der Hersteller und seine Kunden nichts wissen.



Das Modell der gemeinsamen Verantwortung nach Microsoft funktioniert nicht immer wie gewünscht. Nicht alle Unternehmen kümmern sich um ihren Teil der Pflichten (Abb. 4).

Gegen Beinahe-Zero-Days (siehe ix.de/z9xw), die Angreifer viel häufiger ausnutzen und die nicht weniger gefährlich sind, können Verteidiger sich aber schützen. Dabei handelt es sich um Sicherheitslücken, für die der Hersteller schon einen Patch bereitstellt, der in der eigenen Umgebung aber noch nicht oder zumindest nicht flächendeckend ausgerollt ist. Wenn der Hersteller einmal nachbessern musste, steht zu befürchten, dass in der betroffenen Komponente weitere Lücken klaffen. Das hat sich beispielsweise im Exchange-Mailserver von Microsoft gezeigt, dessen Webschnittstellen von ProxyLogon, ProxyShell und ProxyNotShell betroffen waren.

Informieren und zügig patchen

Regelmäßiges Einspielen von Softwareflicken kann und sollte gelebte Praxis sein; bei außerplanmäßigem Erscheinen auch kurzfristig. Angreifer scannen, schon einen Tag nachdem ein Patch erschienen ist, nach Schwachstellen in VPN-, Web- oder Mailservern und anderen Systemen, die aus dem Internet erreichbar sind (Abbildung 2).

Besonders brenzlig wird es, sobald Skripte zum Scannen und Ausnutzen auf GitHub veröffentlicht sind, die Skript-Kiddies und Gelegenheitsangreifer verwenden können. Eine Liste von Patch-Antimustern mit schlechten Ausreden fürs Nicht-Updaten hat ein Microsoft-Mitarbeiter zusammengestellt (Abbildung 3).

Sicherheitsrelevante Bugs, die mit einer neuen Version der Anwendung ausgebügelt werden, gibt es unzählige. Im Jahr 2022 wurden knapp 26 000 Schwachstellen mit einer CVE-Nummer registriert und öffentlich gemacht. Besonders brenzlige Lücken, die Kriminelle zum Eindringen in eine Organisation oder zum Ausbreiten in deren Netzwerk aktiv ausnutzen, verzeichnet der „Known Exploited Vulnerabilities Catalog“ (siehe ix.de/z9xw) der amerikanischen Cybersecurity-Behörde CISA. Schwachstellen, die darin aufgeführt sind, sollten Admins unverzüglich durch ein Update beheben. Vor allem, weil viele der dort gelisteten knapp 900 Bugs schon seit Jahren bekannt sind.

„Die Cloud gewährleistet unsere Datensicherheit“

Der Vorteil einer öffentlichen Datenwolke ist die geballte Expertise des Anbieters. Falls eine patchbare Softwarelücke bei einem Cloud-Service-Provider auftritt, stopft der Anbieter das Loch für alle Kunden, ohne dass sie aktiv werden müssten. Die „Open Cloud Vulnerability & Security Issue Database“ (siehe ix.de/z9xw) verzeichnet solche Schwachstellen. In der Praxis führten sie bislang zu wenigen Einbrüchen durch Kriminelle.

Ein Großteil der Zuständigkeit für die Sicherheit lastet im Modell der gemeinsamen Verantwortung (Abbildung 4) jedoch auf den Schultern des Cloud-Nutzers. Problematisch wird es, wenn eine Organisation sich auf die unzureichenden Standardeinstellungen etwa von Azure Active Directory (Azure AD) verlässt oder ihre eigenen Pflichten vernachlässigt und nicht die (manchmal kostenpflichtigen) eingebauten Sicherheitsmechanismen oder (häufig kostenfreien) Dritt-Auditwerkzeuge nutzt [4].

Das führt zu kompromittierten Cloud-Umgebungen aufgrund unzureichender Konfiguration. Nur weil man die Daten in der Cloud eines Anbieters speichert, hat man sich nicht der Verantwortung entledigt. Für Sicherheit und Sicherung der Daten ist weiterhin das Unternehmen zuständig.

„Alle Sicherheitsupdates sind installiert, uns kann nichts passieren“

Auch wer ein überdurchschnittliches Patch-Management fährt, sollte sich nicht in falscher Sicherheit wiegen. Patches halten Hacker nicht auf, wenn die Systeme unsicher konfiguriert sind. Für Angreifer ist es manchmal einfacher, sich über unzureichende Konfiguration Zugang oder erweiterte Rechte zu verschaf-

fen, als zu lernen, eine bestimmte bekannte Schwachstelle auszunutzen.

In Fällen, die der DBIR untersucht, war 2020 ein Einbruch aufgrund fehlkonfigurierter Cloud-Dienste wie Azure AD [5] wahrscheinlicher als wegen Anwendungsschwachstellen.

On Premises sind viele Active-Directory-Umgebungen nur lückenhaft gegen schwerwiegende Man-in-the-Middle-Angriffe wie Net-NTLM-Relaying [6] gesichert. Dabei genügt für einen Angreifer zum Beispiel ein Blick eines Domänenadministrators in eine präparierte Netzwerkfreigabe, um dessen Zugangsdaten auf einen Server weiterzuleiten, im schlimmsten Fall einen Domänencontroller. Als Abhilfe hierfür müssten Systemverwalter SMB-Signierung und LDAP-Kanalbindung in der gesamten Domäne testen und konfigurieren und die Nebenwirkungen umschiffen.

Angreifer werden jede effiziente Methode nutzen, um in eine Umgebung einzudringen oder ihre vorgefundenen Berechtigungen zu erweitern: das Kompromittieren eines Cloud-Dienstes oder eines vernetzten Druckers mit Adminzugangsdaten zur Domäne, beides Folge von unsicheren Standardeinstellungen oder Konfigurationsfehlern. Aufgabe der Verteidiger ist es, die für Angreifer einfachsten, billigsten und nützlichsten Lücken zu verstehen und zu beseitigen.

„Das System ist nur intern oder über VPN erreichbar, Zugriffe sind somit vertrauenswürdig“

Oft versuchen Admins nur, Systeme zu sichern, die direkt mit dem Internet verbunden sind – und belassen es dabei. Eine Fehleinschätzung ist es, interne Systeme und Anwendungen zu vernachlässigen, weil man von externen Widersachern ausgeht.

Das interne Netz ist nicht so vertrauenswürdig wie gedacht. Ein Insider ist schon drin. Angreifer kompromittieren den Rechner eines Mitarbeiters im Homeoffice oder im Büro besonders leicht, wenn sie wegen fehlender Awareness-Schulungen unachtsame Opfer finden. Oder sie steigen übers virtuelle Netzwerk ein, falls der VPN-Server nicht aktualisiert ist.

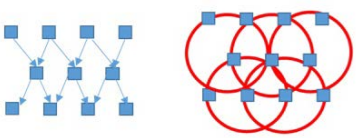
Bei fehlender Netzsegmentierung gelangt jeder Besucher einer Einzelhandelsfiliale aus dem offenen Gäste-WLAN direkt zu den Servern in der Zentrale. Sind diese ungepatcht und für eine bekannte Windows- oder Active-Directory-Schwachstelle anfällig, ist der Schaden groß. Interne Dienste müssen Verteidiger ebenso sichern und aktualisieren wie

Sünden bei der Verwaltung von Windows-Zugangsdaten

Quelle: John Lambert

Sünden des Mirror-Imaging

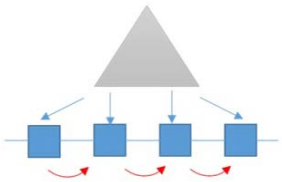
Das Netzwerk so sehen, wie man es verwaltet, und nicht, wie Angreifer es sehen.



Administratoren arbeiten im Bereich des Verwaltbaren und Angreifer im Bereich des Möglichen.

Sünden des Verzichts

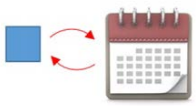
Versäumen, lokale Konten zu verwalten.



Lokale Anmeldungen sind für einen Domänencontroller nicht sichtbar und Zugangsdaten laufen selten ab.

Sünden der Kompromisse

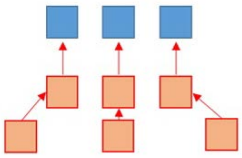
Zugangsdaten übermäßig lange gültig lassen, um Dienstunterbrechungen zu vermeiden.



Angreifer schätzen langlebige Anmeldeinformationen noch mehr als Endbenutzer.

Sünden der Unvollständigkeit

Server absichern, aber nicht die Arbeitsplätze der Administratoren oder andere sicherheitsrelevante Abhängigkeiten.



Das Netzwerk ist keine Liste von Assets, sondern ein gerichteter Graph von Anmeldedaten und Anmelderechten.

Sünden des Wunschdenkens

In 2FA verliebt sein, aber vergessen:

$$\lim_{OS<Win10} mimikatz(2FA) = 1FA$$

Single Sign-on wandelt Zwei-Faktor-Authentifizierung in einen einzigen Faktor, der ausgelesen und wiederverwendet werden kann.

Sünden der Hygiene

Versäumen, Zugangsdaten sicher zu speichern.

Bei der Zugangsdatenverwaltung unter Windows kann man vieles falsch machen, hier die schlimmsten Sünden (Abb. 5).

externe; der Hersteller sollte sie noch unterstützen. Im Oktober 2023 stellt Microsoft den Support für Windows Server 2012 (R2) ein, bis dahin sollte man sich nach Server 2008 und Windows 7 auch von diesen Systemen trennen – oder sie abschotten.

Zero Trust: gesundes Misstrauen

Moderne, gehypte Ansätze wie Zero Trust schärfen den Blick, dass nicht allem, was intern ist, vorbehaltlos zu vertrauen ist. „Wir leben Zero Trust und sind deswegen sicher“ gilt trotzdem nicht. Die Realität zeigt, dass Unternehmen selten alle auf dem Papier sinnvollen Maßnahmen einhundertprozentig umsetzen, wenn sich eine alte Branchensoftware sträubt. Lücken entstehen mit den notwendigen Ausnahmen. Wichtige Bestandteile von Zero Trust wie Echtzeit-Zugriffsentscheidungen – beispielsweise nach dem Whitepaper von Microsoft (siehe ix.de/z9xw) – sind kaum nachträglich in den On-Premises-Bestand anzuflanschen, sondern erfordern meist Cloud-Umgebungen.

Es lohnt sich, sich an grundlegende Sicherheitseigenschaften von Firewalls zu erinnern und wie Admins sie überwiegend einsetzen. Sie filtern meist nur eingehenden Datenverkehr. Schadsoftware kann unbehelligt ausgehende Verbindungen zu den Kontrollservern der Angreifer herstellen.

„Wir haben eine starke Richtlinie für Passwörter und wechseln diese jeden Monat“

Microsoft veröffentlichte schon 2000 die „zehn unumstößlichen Gesetze“ der sicheren Administration (siehe ix.de/z9xw). Eines von ihnen: „Da draußen sitzt wirklich jemand und versucht, Ihre Passwörter zu erraten.“ Denn ohne weitere Sicherheitsmaßnahmen verschafft sich ein Angreifer Zugang zum Firmennetzwerk oder der Cloud, wenn er hinter das Passwort eines einzigen Benutzers kommt, der sich von außerhalb anmelden darf.

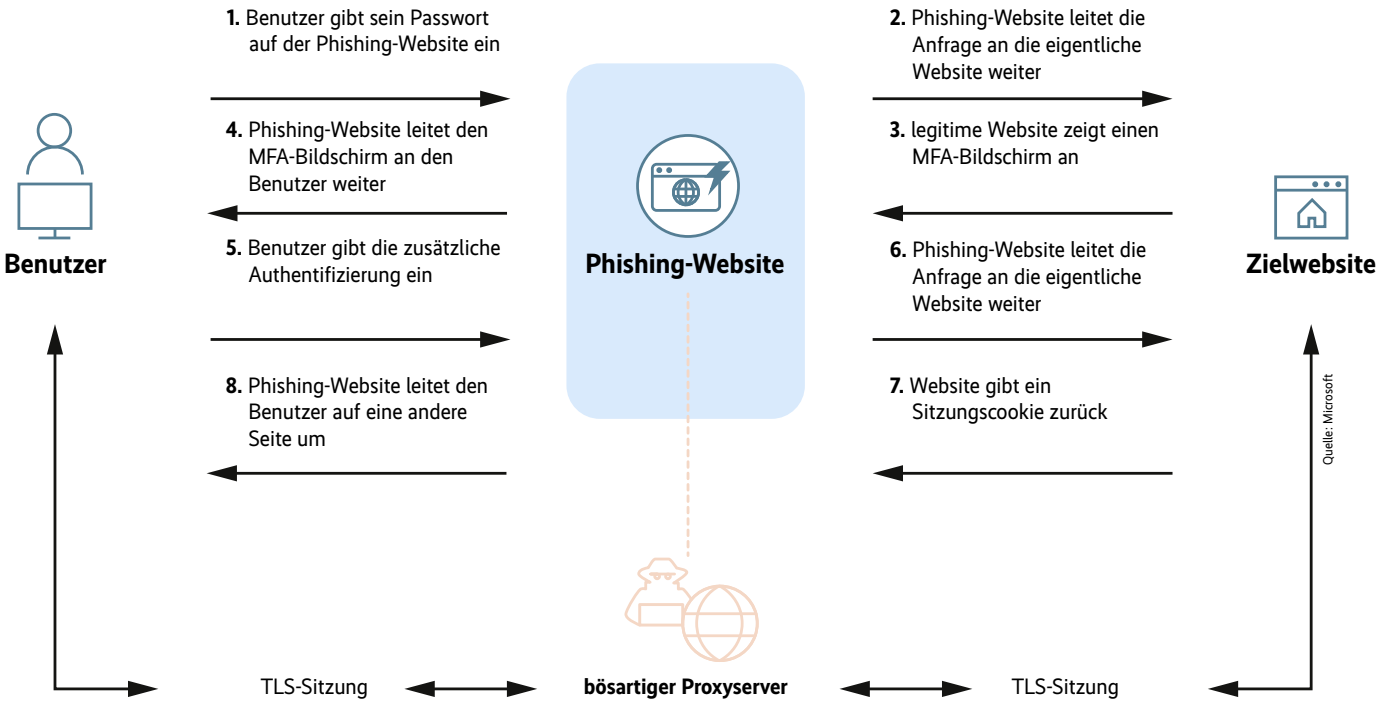
Als Abhilfe haben sich Komplexitätsrichtlinien für Passwörter etabliert. Sie zwingen zu einer Mindestlänge und zum Verwenden von Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen – und sperren nach einer festgelegten Anzahl an Fehleingaben das Konto. Eine starke Kennwortrichtlinie allein führt leider nicht automatisch zu starken Passwörtern, auch schlechte Passwörter erfüllen solche Richtlinien.

Eine gängige und erfolgreiche Methode von Angreifern ist das Password Spraying, etwa gegen Outlook-Web-Access, VPN-Endpunkte oder Cloud-Anmeldeseiten. Sie probieren ein wahrscheinlich verwendetes Passwort wie „Winter2022!“ oder „Unternehmensname2023!“, das Komplexitätsrichtlinien genügt, an allen bekannten Benutzerkonten durch. Eine Liste der Benutzer zu erstellen ist nicht schwierig [4]. Da sich Anmeldeversuche mit einem Passwort auf alle Benutzer verteilen, wird kein Konto gesperrt, im Gegensatz zu Dutzenden oder Hunderten fehlerhaften Versuchen bei einem einzelnen Benutzer. Ähnlich zielgerichtet funktioniert Credential Stuffing, bei dem Angreifer Kombinationen aus Benutzernamen und Kennwort ausprobieren, die in Datenlecks abflossen. Das wird gefährlich, wenn Benutzer vermeintlich komplexe Passwörter wiederverwenden.

Passwort-Audits als Mittel der Wahl

Lange Zeit galt es als sicher, Kennwörter regelmäßig zwangsweise zu wechseln. In der Praxis führte das zu erratbaren Mustern wie Hochzählen einer Ziffer, dem Verwenden der Jahreszeit oder dem Anhängen des Jahres. In Audits knacken Experten einen Großteil der Passwörter. Modernes Passwortraten nutzt nicht nur unveränderte Listen mit geleakten Passwörtern, sondern wendet Regeln an, die Varianten erzeugen wie „p@sswort“, „Passwort02“ oder „Passwort2023!“ [7].

Wirken können einfache Maßnahmen. Mit übersichtlicher Benutzeroberfläche



Beim Adversary-in-the-Middle-Phishing versucht ein Angreifer, das Sitzungscookie eines Benutzers zu erlangen. So kann er den Authentifizierungsprozess übergehen und im Namen des Benutzers handeln (Abb. 6).

hilft die kostenfreie Closed-Source-Software SpecOps Password Auditor: Sie prüft im AD verwendete Passwörter (genauer: ihre Hashes) gegen eine große Liste gestohlener Zugangsdaten vom bekannten Dienst Have I Been Pwned. Taucht ein Passwort darauf auf, ist es häufig vom Kaliber „Sommer2021“ und sonst per Definition schlecht, da geleakt. Wer lieber quelloffene Software einsetzt, verwendet das PowerShell-Modul DSInternals (alle genannten Tools siehe ix.de/z9xw), weniger komfortabel auf der Kommandozeile.

Zugangsdaten öffnen Türen

Gerade Administratoren sollten sich vor manchen Irrtümern in Bezug auf Zugangsdaten hüten (Abbildung 5). Von John Lambert stammt die Aussage, Angreifer benötigen Zugangsdaten dringender als Malware. Schadsoftware ist ein Mittel zum Zweck, den ersten Fuß in die Tür zu bekommen. Wollen Eindringlinge Daten abziehen oder verschlüsseln, brauchen sie ein Konto mit weitreichenden Rechten.

Selbst ein an sich sicheres Passwort für das lokale Standardadministratorkonto von Windows kann dazu führen, dass eine Organisation komplett kompromittiert wird, wenn auf jedem System dasselbe Passwort für den lokalen Admin gesetzt ist [8]. Auch andere Anmeldeinformationen im Arbeitsspeicher, in Dateien, in Browser-Cookies, Konfigurationsdateien oder der PowerShell-Historie sind für Angreifer interessant.

Ein starkes Passwort kann verloren gehen, ausgespäht werden oder hilft nichts, wenn es im Klartext auf einer öffentlichen Netzwerkfreigabe liegt. Passwortmanager unterstützen Administratoren genauso wie normale Mitarbeiter, für jeden Zugang ein eigenes, zufällig ausgewürfeltes Passwort zu verwenden.

„Wir verwenden Mehr-Faktor-Authentifizierung“

Zwei- oder Mehr-Faktor-Authentifizierung (2FA, MFA) macht Anmeldungen sicherer und kann helfen, Passwortangriffe einzudämmen. Anwender müssen neben dem Passwort noch einen kurzzeitig gültigen Code eingeben oder eine Nachfrage auf dem Smartphone bestätigen.

Sie muss durchgängig implementiert sein – vor allem bei Anmeldeendpunkten, die aus dem Internet erreichbar sind. Sichert kein zweiter Faktor einen VPN-Zugang, einen Terminalserver oder gerade das Mailpostfach, nützt der erweiterte Schutz an anderen Stellen nichts.

Cyberkriminelle haben sich darauf eingerichtet, dass Organisationen zunehmend mehrere Authentifizierungsfaktoren nutzen. Bei Adversary-in-the-Middle-Phishing-Angriffen (AiTM) leiten sie den Verkehr vom Benutzer zur legitimen Website über einen bösartigen Proxyserver. Abfragen nach einem zweiten Faktor werden unbemerkt durchgeschleift [9]. Anschließend sind sie auf dem Zieldienst mit denselben Rechten wie das Opfer angemeldet und können das Sitzungscookie stehlen (Abbildung 6).

Ein zum Anmelden erforderlicher zweiter Faktor täuscht darüber hinweg: Eindringlinge, die per klassischer Malware beliebige Befehle auf dem Rechner eines Systemverwalters ausführen, sehen beispielsweise dessen zuletzt besuchte Webseiten samt Sitzungscookies – im Zusammenhang mit Web-APIs auch Zugriffstoken [10]. Solange die Sitzung gültig ist, authentifizieren sie sich damit gegenüber der verwendeten Anwendung, ohne dass nach einem zweiten Faktor gefragt würde.

Sitzungscookie klauen, zweiten Faktor umgehen

Im Windows-Umfeld schützt MFA oft nur vor interaktiven Passwortangriffen. Liest der Angreifer den Arbeitsspeicher eines kompromittierten Rechners aus, kann er von Windows und Active Directory intern verwendete Zugangsdaten wie NTLM-Passworthashes, Kerberos-Tickets oder Zertifikate stehlen. Damit meldet er sich ohne Abfrage eines weiteren Faktors an anderen Systemen an [11], selbst bei passwortlosen Verfahren wie Smartcards (siehe ix.de/z9xw).

Kriminelle haben gelernt, einfache Push-Nachfragen zu umgehen, die der Anwender auf seinem Smartphone entweder bestätigt oder ablehnt. Wiederholt und automatisiert fordern sie die Authentifizierung an, besonders in den Abend- und Nachstunden, bis das von den wiederholten Verifizierungsanfragen bombardierte Opfer ermüdet ist und eine bestätigt. Mit sogenannten MFA-Fatigue-Attacken gelang Angreifern der Zugriff auf das Firmen-VPN selbst bei einem Schwergewicht wie Cisco, das den MFA-Anbieter Duo Security gekauft hatte, wie im Vorfallbericht nachzulesen (siehe ix.de/z9xw).

Microsofts Dokumentation zu Authentifizierungsmethoden ist ein guter Einstieg, um Phishing-sichere Anmeldung einzuführen, wobei etwa FIDO2-Sicherheitsschlüssel helfen (siehe ix.de/z9xw).

Teil 2 des Titels klärt über weitere Irrtümer auf: Warum Compliance nicht sicher macht, Sicherheitsanwendungen wie Malware-Scanner oder EDR (Endpoint Detection and Response) keine Allheilmittel sind und Organisationen das Erkennen von Angriffen vergessen, weil sie sich auf das Verhindern konzentrieren. (ur@ix.de)

Quellen

[1] Frank Ully; Himmelsgeschenk; Active Directory: Komfortable IT-Schaltzentrale mit Schwachpunkten; iX 10/2020, S. 40

[2] Manuel Atug, Lisa Lobmeyer; Erpresst und ausgecybert; Wie Ransomware-Angriffe heute ablaufen; iX 3/2022, S. 46

[3] Henrik Plate, Wolfram Fischer; Angriffe auf die Softwarelieferkette; iX 10/2022, S. 44

[4] Frank Ully; Das Netz verstärkt; Azure Active Directory und Azure-Dienste absichern; iX 4/2022, S. 44

[5] Frank Ully; Ins Netz gegangen; Angriffe auf das Azure Active Directory und auf Azure-Dienste; iX 4/2022, S. 50

[6] Hans-Martin Münch; Mein Name ist Hase; Kompromittierung von Windows durch LLMNR Spoofing und NTLM Relaying; iX 10/2016, S. 106

[7] Sandro Affentranger; Schwierige Wahl; Passwortsicherheit (nicht nur) im Active Directory; iX 1/2022, S. 116

[8] Marco Wohler; Mit aller Härte; Wie Administratoren ihr Active Directory absichern; iX 5/2021, S. 106

[9] David Kelm; Angriffswelle auf Log-in-Daten; iX 10/2022, S. 100

[10] Frank Ully; APIs sicher entwickeln; iX 7/2022, S. 52

[11] Frank Ully; Fette Beute; Passwörter und Hashes – wie Angreifer die Domäne kompromittieren; iX 11/2020, S. 94

[12] Die im Text angesprochenen Artikel, Angriffe und Werkzeuge sind über ix.de/z9xw zu finden.

FRANK ULLY

ist Head of Research der Oneconsult Deutschland AG in München. Er beschäftigt sich mit aktuellen Themen der offensiven IT-Sicherheit.