Rubrik Zero Labs

DIE IDENTITÄTS-KRISE

WAS SIE ÜBER IDENTITÄTSBEZOGENE BEDROHUNGEN WISSEN MÜSSEN UND WIE SIE SICH DAVOR SCHÜTZEN

INHALT

03

Kurzfassung

05

Identitätsdiebstahl: Das Einfallstor für „Living-off-the-Land“-Angriffe

09

Die Folgen identitätsbasierter Vorfälle

10 Wie reagieren Unternehmen?

15

Warum dauert die Wiederherstellung so lange?

15 MTTR als datengestützte Antwort

16 Ein neues Framework zur Aufschlüsselung der MTTR

17 Warum die MTTR wichtig ist

18

Aufbau von Identitätsresilienz: Empfehlungen und Abwehrfunktionen

20 Der Lebenszyklus der Cyber-Resilienz

21

Daten und Methodologie

KURZFASSUNG

Rubrik Zero Labs und Wakefield Research haben kürzlich eine Umfrage unter 1.625 IT- und Sicherheitsmanagern aus Unternehmen auf der ganzen Welt durchgeführt, um zu ermitteln, wie gut sie darauf vorbereitet sind, identitätsbasierte Angriffe abzuwehren und sich davon zu erholen. Die dabei erfassten Angaben sollen zusammen mit den Erkenntnissen aus den mehr als 2,2 Millionen Snapshots, die Rubrik täglich auf der Suche nach Bedrohungen in Backup-Daten scannt, Aufschluss über die Lage geben.

Die Umstellung auf die Cloud, Remote-Arbeit und nun auch agentische KI lassen die herkömmlichen Netzwerkgrenzen zunehmend verschwimmen. Daher sind Identitäten nicht länger nur eine reine Kontrollebene, sondern eine wichtige Angriffsfläche, über die sich Kriminelle Zugang zu IT-Umgebungen verschaffen, um im Rahmen von LotL-Angriffen (Living of the Land) unternehmenseigene Tools und Systeme für ihre Zwecke auszunutzen. Heutzutage lassen sich die meisten Datensicherheitsverletzungen auf die Ausnutzung von Vertrauen und gültigen Anmeldedaten zurückführen und nicht auf die Umgehung von Schutzmaßnahmen für das Netzwerk.

Da nahezu alle Angriffe menschliche oder nicht-menschliche Identitäten umfassen – sei es für den Erstzugriff, die Ausweitung von Berechtigungen oder die Ausbreitung in der Umgebung –, überrascht es nicht, dass die meisten Umfrageteilnehmer (90 %) identitätsbasierte Angriffe als größte Bedrohung für ihr Unternehmen einschätzen.

In diesem Bericht ermitteln wir anhand von Zahlen und Fakten, Schwerpunktbereichen und Details zu Wiederherstellungszeiten, wie gut Unternehmen in der Lage sind, sich vor Identitätsangriffen zu schützen.

Darüber hinaus untersuchen wir die grundlegenden Elemente der Identitätsresilienz, darunter:

- Integration von Transparenz-, Abwehr- und Wiederherstellungsfunktionen in Echtzeit für alle lokalen und Cloud-basierten Identitätsanbieter (sowohl für menschliche als auch für nicht-menschliche Identitäten)
- Aufbau eines hohen Vertrauensniveaus in die Fähigkeit des Unternehmens, die zentrale Identitätsinfrastruktur schnell und zuverlässig wiederherzustellen und in einen Zustand vor einem Angriff zurückzuversetzen
- Identitätshärtung und Aufbau von Resilienz mit Zero-Trust-Prinzipien zur Minimierung der Angriffsfläche sowie des Schadensausmaßes nach einem erfolgreichen Identitätsangriff
- Integration von Identitätsresilienz in den übergreifenden Cyber-Resilienzplan eines Unternehmens

Nur mit einem ganzheitlichen Ansatz können Unternehmen ihre Identitätsinfrastruktur absichern und potenzielle Ausfallzeiten, Umsatzverluste und Reputationsschäden vermeiden.

Sehen wir uns zunächst Vergleichszahlen zum Vorjahr aus unseren Umfragen an.

2024 VS. 2025
TRENDS AUS DER UMFRAGE
(Wakefield)

90 %
waren im vergangenen Jahr von einem Cyber-Angriff betroffen.

Das ist derselbe Prozentsatz wie im Jahr 2024.

89 %
der von einem Ransomware-Angriff betroffenen Unternehmen zahlten Lösegeld, um ihre Daten zu retten oder die Attacke zu stoppen.

20 %
verzeichneten mehr als 25 Angriffe (im Vergleich zu 18 % im Jahr 2024).

11 % erlitten mindestens 100 Angriffe; ein leichter Anstieg gegenüber 2024 (8 %).

DAS VERTRAUEN IN EINE SCHNELLE WIEDERHERSTELLUNG NIMMT AB.

Im Jahr 2025 glaubten nur 28 %, dass sich ihr Unternehmen innerhalb von maximal 12 Stunden vollständig von einem Cyber-Vorfall erholen könnte, verglichen mit 43 % im Jahr 2024.

77 %
müssen größere Cloud-Umgebungen verwalten als im Vorjahr.

58 %
gehen davon aus, dass agentische KI mindestens für die Hälfte aller Cyber-Angriffe im kommenden Jahr verantwortlich sein wird.

58 %
vermuten, dass ihr Unternehmen mindestens zwei Tage benötigt, um nach einem Vorfall wieder zum Normalbetrieb überzugehen.

IDENTITÄTS-DIEBSTAHL:

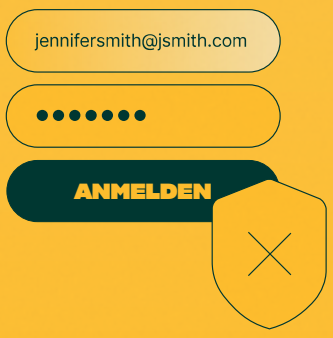
DAS EINFALLSTOR FÜR „LIVING-OFF-THE-LAND“-ANGRIFFE

Bei den meisten modernen Cyber-Vorfällen spielt die eine oder andere Art von Identitätsdiebstahl eine Rolle. Dabei sind die Identitäten jedoch eher Mittel zum Zweck und nicht die eigentlichen Angriffsziele. Angreifer betrachten sie in der Regel als ein Tool, mit dem sie ihr Endziel erreichen – sei es Ausspähung, Datendiebstahl oder Erpressung.

86 %

der einfachen Angriffe auf Webanwendungen werden heute mit gestohlenen Anmeldedaten durchgeführt.

(Verizon)[1]



79 %

der mit CrowdStrike gescannten Instanzen waren „frei von Malware“, d. h. die Angreifer loggten sich ein und nutzten keine herkömmliche Malware.

(Crowdstrike 2025)[2]

4,67

MILLIONEN USD

kostet ein einziger Sicherheitsvorfall im Schnitt,

wenn Angreifer kompromittierte Anmeldedaten nutzen.

(IBM)[3]

Identitätsdiebstahl ist ein Bedrohungsvektor, mit dem Angreifer:

„Living-off-the-Land“-Kampagnen initiieren können und sich der Aufdeckung entziehen, indem sie legitime Prozesse wie Admin-Tools, SaaS-Services oder auch die Identitätsworkflows selbst missbrauchen.

Folgeangriffe mithilfe kompromittierter Anmeldedaten starten können.

sich in der Zielumgebung frei bewegen können, mitunter durch das Anlegen von „Schatten“-Identitätsplattformen, also nicht legitimen Mandanten oder Identitätsinfrastrukturen außerhalb des Governance- und Sichtbarkeits-Frameworks eines Unternehmens.

[1] https://www.verizon.com/business/de-de/resources/reports/dbir/
[2] https://www.crowdstrike.com/de-de/resources/reports/global-threat-report-executive-summary-2025/
[3] https://www.ibm.com/de-de/reports/data-breach

Menschliche Identitäten sind nicht das einzige Ziel von Angreifern, auch nicht-menschliche Identitäten (Non-Human Identities; NHIs) sind beliebt. Dabei handelt es sich oftmals um API-Tokens, die zur Authentifizierung von automatisierten IT-Prozessen, Zertifikaten, Containern, Automatisierungstools, Service-Accounts und KI-Agenten genutzt werden.

Heute beträgt das Verhältnis von NHIs zu menschlichen Benutzern 82 zu 1.[4] Dadurch steht Bedrohungsakteuren eine wesentlich größere Angriffsfläche zur Verfügung, die sich durch die zunehmende Nutzung agentischer KI noch ausdehnen wird.

Ob menschliche Identitäten oder NHIs angegriffen werden, hängt vom Ziel der Hacker ab. Um sich wirksam schützen zu können, müssen Sie daher wissen, welche Identitäten zu welchem Zweck ins Visier genommen werden:

	Menschliche Identitäten (Mitarbeiter-Accounts, Admin-Logins usw.)	**Nicht-menschliche Identitäten** (Service-Accounts, API-Schlüssel, Tokens usw.)
Wichtigstes Ziel	Erstzugang, Ausspähung und Ausnutzung vorhandener Benutzerberechtigungen	Unerkanntes Eindringen in die Umgebung, Persistenz und Systemzugriff mit umfangreichen Privilegien
Größtes Risiko	Social Engineering	Fehlkonfigurationen, Tendenz der uneingeschränkten Verbreitung
Umgehung von Schutzmechanismen	Langfristig schwierig: Accounts menschlicher Benutzer sind meistens durch MFA, Zugriffsrichtlinien und Verhaltensanalysen (wie unwahrscheinliche Standorte) geschützt.	Langfristig relativ einfach: NHIs nutzen oft keine MFA, werden nicht so strikt überwacht und nutzen automatisierte Abläufe, die leicht im legitimen Alltagsbetrieb untergehen.
Berechtigungen	Berechtigungen sind in der Regel an eine bestimmte Rolle gebunden, z. B. Engineering oder Vertrieb.	Berechtigungen sind oft systemorientiert und zu weit gefasst, z. B. ein Service-Account, der Lesezugriff auf jede Datenbank im System hat.
Dauer	Leicht zu widerrufen: Ein menschlicher Account kann gesperrt werden, Passwörter können rotiert werden und eine Sitzung kann innerhalb weniger Minuten nach der Aufdeckung eines Sicherheitsvorfalls abgebrochen werden.	Schwer zu widerrufen: NHIs sind oft langlebig, werden vergessen oder unterstützen geschäftskritische Vorgänge, weshalb das Rotieren schwierig und betriebsstörend sein kann.

[4] https://www.cyberark.com/de/resources/white-papers/identity-security-landscape-2025-executive-summary

ANGREIFER UND IHRE VORLIEBE FÜR IDENTITÄTEN

Identitäten – sowohl menschliche als auch nicht-menschliche – standen in jüngster Zeit im Mittelpunkt einiger aufsehenerregender Cyber-Sicherheitsvorfälle.

Laterale Ausbreitung mit Entra ID und n0Auth

Im Juni 2025 wurde festgestellt, dass Entra ID, der Cloud-basierte Microsoft-Dienst für die Identitäts- und Zugriffsverwaltung (IAM), immer noch eine Schwachstelle enthielt, die es Bedrohungsakteuren ermöglicht, von bestimmten kompromittierten SaaS-Anwendungen auf die zentralen Microsoft 365-Ressourcen eines Unternehmens zuzugreifen und darüber Zugang zu sensiblen Geschäftsdaten zu erhalten.[5]

Indem ein einziges E-Mail-Attribut manipuliert wird, sodass es mit der Adresse des anvisierten Opfers übereinstimmt, kann sich ein Benutzer über die Funktion „Mit Microsoft anmelden" einer anfälligen SaaS-Anwendung Zugang verschaffen. Diese Ausnutzung der Durchsetzungslogik für Identitäten ermöglicht Angreifern, sich schnell in der Umgebung auszubreiten und auf wichtige Produktivitätstools wie SharePoint und Teams zuzugreifen.

Obwohl diese Sicherheitslücke bereits 2023 entdeckt wurde, ist davon auszugehen, dass sie immer noch Zehntausende von SaaS-Apps betrifft. Da n0Auth Abhilfemaßnahmen nur auf Mandantenseite zulässt, ist es unmöglich, diese Schwachstelle mit einem globalen Patch zu beheben, und die Beliebtheit von Microsoft-Produkten vergrößert die potenzielle Angriffsfläche enorm. Angreifer haben Entra ID daher auch 2025 noch ausgenutzt – oft, um Berechtigungen auszuweiten.

ToolShell-Angriffe auf lokale SharePoint-Server

Die ToolShell-Angriffe im Juli 2025 zeigen, wie identitätsbezogene Aspekte – wie die Authentifizierung von Schlüsseln – aufgrund von Sicherheitslücken ausgenutzt werden können. In diesem Fall stahlen die (vermutlich staatlich gesponserten) Angreifer Geräteschlüssel, um sich auf lokalen SharePoint-Servern zu authentifizieren, auf denen sich für sie lohnende Daten befanden. Vermutlich bestand das Ziel darin, langfristige Ausspähkampagnen innerhalb der Unternehmensumgebungen durchzuführen.[6]

Hier zeigt sich der Wert von NHIs für Bedrohungsakteure, die anhaltende Angriffsaktivitäten – unter anderem zu Spionagezwecken – planen. Da Schlüssel langlebiger sind als Tokens, müssen Sicherheitsteams dafür sorgen, dass Schlüssel nach einem Cyber-Vorfall oder bei Bekanntwerden einer CVE (Common Vulnerability or Exposure) zeitnah rotiert werden. Das sollten wir aus den ToolShell-Angriffen gelernt haben.

Scattered Spider: Der Faktor Mensch als Einfallstor

Die Hackergruppe Scattered Spider ist bekannt dafür, sich als IT- oder Helpdesk-Mitarbeiter auszugeben, um Personen dazu zu verleiten, ihre Anmeldedaten preiszugeben oder die Multi-Faktor-Authentifizierung zu umgehen. Ihr Erfolg beruht im Wesentlichen auf der Ausnutzung der menschlichen Gutgläubigkeit. Insbesondere haben sie es auf die schnelle Reaktionsfähigkeit und das Mitgefühl von Supportteams abgesehen, die oft unter Druck stehen, Probleme zeitnah zu lösen. Im August 2023 sollen die Hacker dem Hersteller von Reinigungsmitteln Clorox Schaden in Höhe von 380 Millionen USD zugefügt haben, indem sie beim externen Helpdesk des Unternehmens anriefen und das Zurücksetzen eines Passworts beantragten.[7]

Der Erfolg von Scattered Spider hängt nicht davon ab, dass die Gruppe Zero-Day-Schwachstellen in Software findet. Vielmehr nutzt sie Social Engineering für den anfänglichen Zugriff und missbraucht anschließend native Tools wie PowerShell und SaaS-Dienste. Daraus lässt sich ableiten, dass rein technische Lösungen keinen ausreichenden Schutz bieten. Stattdessen müssen Unternehmen in menschenorientierte Sicherheit investieren, zum Beispiel in kontinuierliche, flexible Schulungen für die Sicherheitssensibilisierung und zum Aufbau einer resilienten Identitätsinfrastruktur.

[5] https://www.infosecurity-magazine.com/news/microsoft-noauth-flaw-2025/
[6] https://www.recordedfuture.com/blog/toolshell-exploit-chain-thousands-sharepoint-servers-risk
[7] https://www.cybersecuritydive.com/news/clorox-380-million-suit-cognizant-cyberattack/753837/

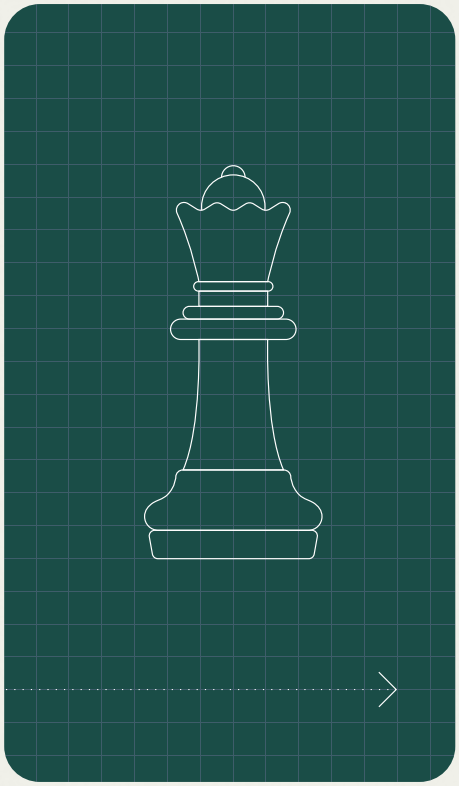
DIE FOLGEN IDENTITÄTSBASIERTER VORFÄLLE

Identitäten sind der Schlüssel zu Ihrem digitalen Reich. Wenn Angreifer sie stehlen, können sie im Rahmen von LotL-Kampagnen legitime Tools für Ausspähung und Datenausschleusung missbrauchen.

Wenn man bedenkt, welchen Schaden eine einzige erfolgreiche Kompromittierung anrichten kann, wird klar, warum Identitäten zu einen zunehmend beliebten Angriffsziel geworden sind:

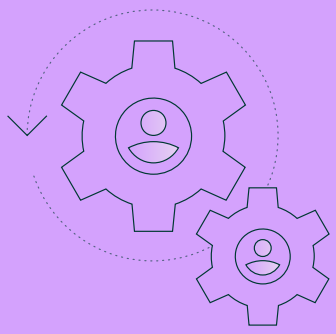
Art der Störung	Folgen	Betroffene geschäftliche Assets
Datenschutzverletzung	Exfiltration von personenbezogenen Daten, geistigem Eigentum, Finanzdaten oder anderen wertvollen Informationen	Kunden- und Mitarbeiterdaten, Geschäftsgeheimnisse, Wettbewerbsvorteile, Finanzunterlagen
Finanzielle Verluste	Betrug, Incident-Response-Kosten, Rechtskosten, Bußgelder	Budget, Umsatz, Rechtsabteilung
Rufschädigung	Verlust des Kundenvertrauens, Schädigung des Markennamens, negative Schlagzeilen	Markenwert, Beziehungen zu Kunden und Partnern, Marktwert
Betriebsunterbrechungen	Systemausfall, Service-Unterbrechung, gesperrte Accounts	Umsatz, IT-Infrastruktur, Sicherheitskontrollen
Persistenz und Ausweitung von Berechtigungen	Installation von Backdoors (Dienstprinzipale, Änderungen an föderierten Identitäten), Anlegen von Schatten-Identitätsplattformen	IT-Infrastruktur, Identitäts- und Zugriffsmanagement, Sicherheitskontrollen
Compliance und rechtliche Risiken	Verstöße gegen Datenschutzbestimmungen (DSGVO, CCPA), gerichtliche Klagen	Rechts- und Compliance-Ressourcen
Lieferkettenangriffe	Angriffe auf Geschäftspartner und Drittanbieter (Kettenreaktion)	Ökoysteme von Partnern, Lieferkettenintegrität, Ruf

WIE REAGIEREN UNTERNEHMEN?



90 %

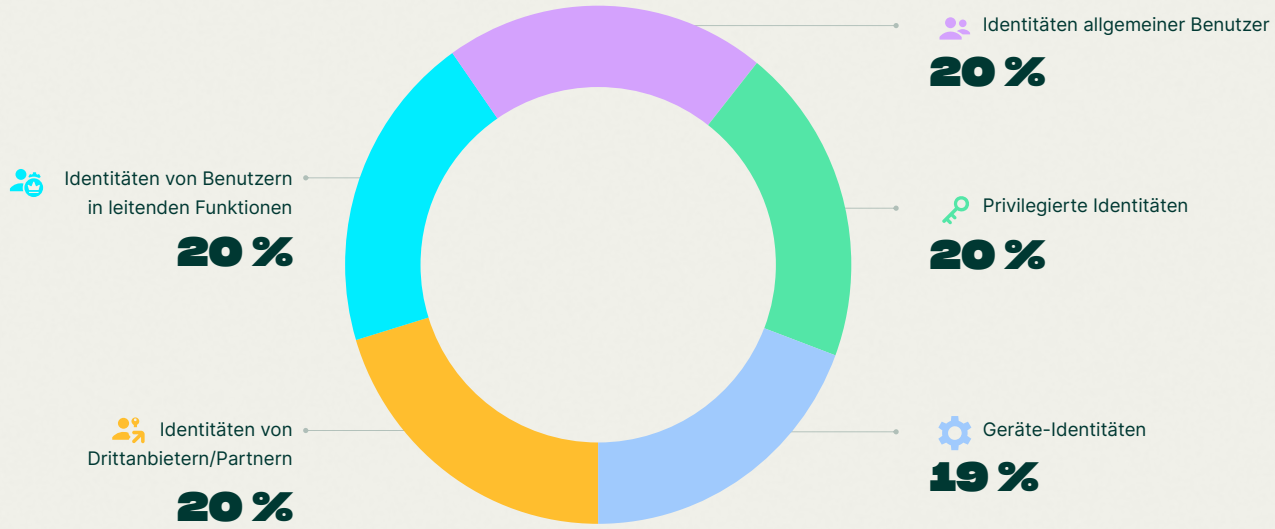
der befragten IT- und Sicherheitsmanager nennen identitätsbezogene Cyber-Angriffe als größte Bedrohung für ihr Unternehmen.



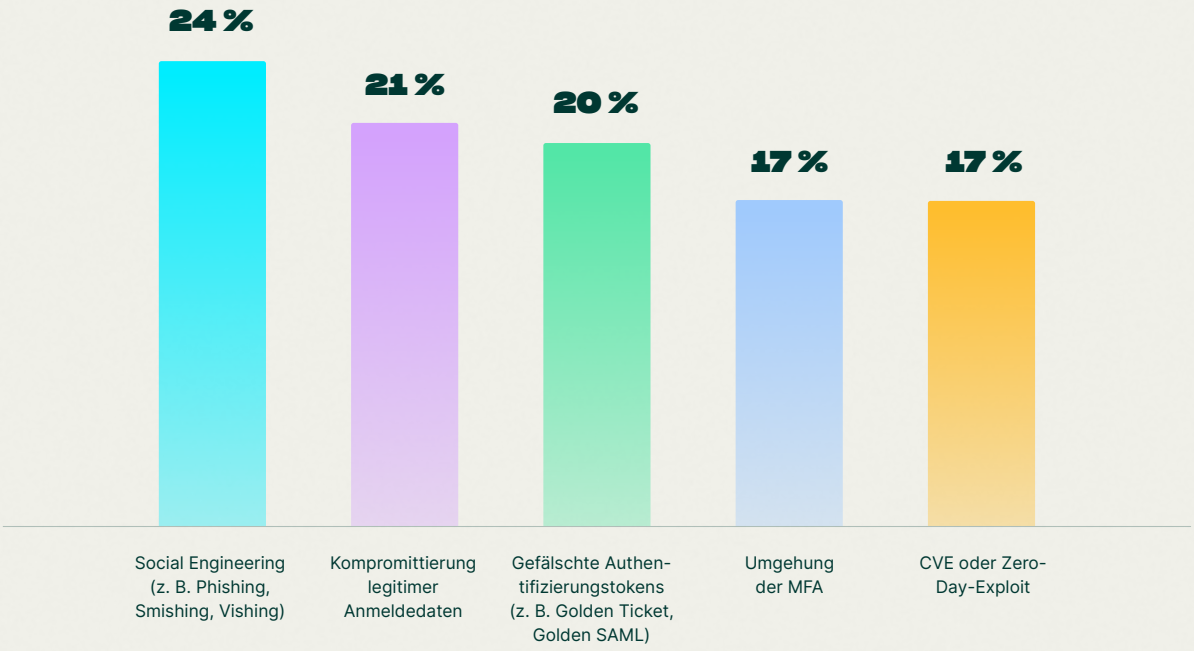
89 %

planen, in den nächsten zwölf Monaten Fachpersonal für die Verwaltung bzw. Optimierung digitaler Identitäten, der Identitätsinfrastruktur und/ oder der Identitätssicherheit einzustellen.

Welche Arten von Identitäten sind Ihrer Meinung nach am meisten gefährdet?



Früher haben IT- und Sicherheitsmanager sich vornehmlich auf Accounts mit privilegierten Rechten konzentriert, aber heute ist man sich einig, dass alle Identitäten von kritischer Bedeutung sind. Es wird also eingeräumt, dass jeder kompromittierte Account unabhängig von den zugewiesenen Berechtigungen ein gefährliches Einfallstor ist, das Angreifer für die Ausbreitung in der Umgebung und für die Ausweitung von Rechten missbrauchen können.



Darüber hinaus deuten die Daten auf eine Verlagerung bei den Sicherheitsprioritäten hin. Zwar steht Social Engineering mit 24 % an der Spitze, aber die Umgehung der MFA (17 %) und gefälschte Authentifizierungstokens (20 %) werden inzwischen als ebenso gefährlich angesehen wie Zero-Day-Exploits (17 %).

Dies ist eine tiefgreifende Veränderung, die zeigt, dass IT- und Sicherheitsmanager ein neues Realitätsbewusstsein entwickelt haben: Angreifer, die sich mit missbräuchlich erworbenen Identitäten anmelden, stellen eine größere Gefahr dar als herkömmliche Brute-Force-Exploits.

Mandiant beobachtete 2024 nach eigenen Angaben mehr Cloud-basierte Sicherheitsverletzungen als je zuvor[8] und nannte Identitätslösungen ohne ausreichende Sicherheitskontrollen als Hauptgrund. Identitäten kristallisieren sich zunehmend als Angriffsvektor heraus und Lösungen für das Identitäts- und Zugriffsmanagement (IAM) können mit den neuen Angriffstechniken oft nicht mithalten.

Das ist vermutlich auf verschiedene Faktoren zurückzuführen:

Identitäten sind vielschichtig

Die Verwaltung des privilegierten Zugriffs (PAM), rollenbasierte Zugriffskontrollen (RBAC) und API-Sicherheit sind jeweils Teilbereiche von IAM, wobei jede Komponente unter Umständen von einem anderen Anbieter abgedeckt wird. Dadurch vergrößert sich die Angriffsfläche.

Es kommen kontinuierlich neue Identitätstypen auf

KI-Bots und KI-Agenten sind Arten von NHIs, die es vor fünf Jahren noch nicht gab, und APIs werden mehr denn je eingesetzt. Die Nutzung von Agenten wird zu einem explosionsartigen Anstieg der Anzahl von Maschine-zu-Maschine-Identitäten führen, deren Lebenszyklusmanagement (d. h. Bereitstellen, Rotieren und Entfernen) oft nicht so ausgereift ist wie bei Accounts für menschliche Benutzer.

Angreifer nutzen Identitäten auf neue Art und Weise

Da die Sicherheitsmaßnahmen für Endpunkte und Perimeter immer effektiver werden, setzen Bedrohungsakteure zunehmend auf den Diebstahl von Zugangsdaten, um sich anzumelden (statt einzubrechen).

Die Cloud bringt neue Risiken mit sich

Die Komplexität und Granularität Cloud-nativer IAM-Systeme machen sie sehr anfällig für Bedienfehler und Fehlkonfigurationen. Angreifer suchen aktiv nach solchen Fehlkonfigurationen wie Rollen mit zu weit gefassten Rechten oder versehentlich erteilten öffentlichen Berechtigungen.

[8] https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

Folgende Zahlen sollten daher niemanden überraschen:

87 %

der IT- und Sicherheitsmanager planen derzeit einen Wechsel des IAM-Anbieters oder haben diesen Prozess bereits eingeleitet.

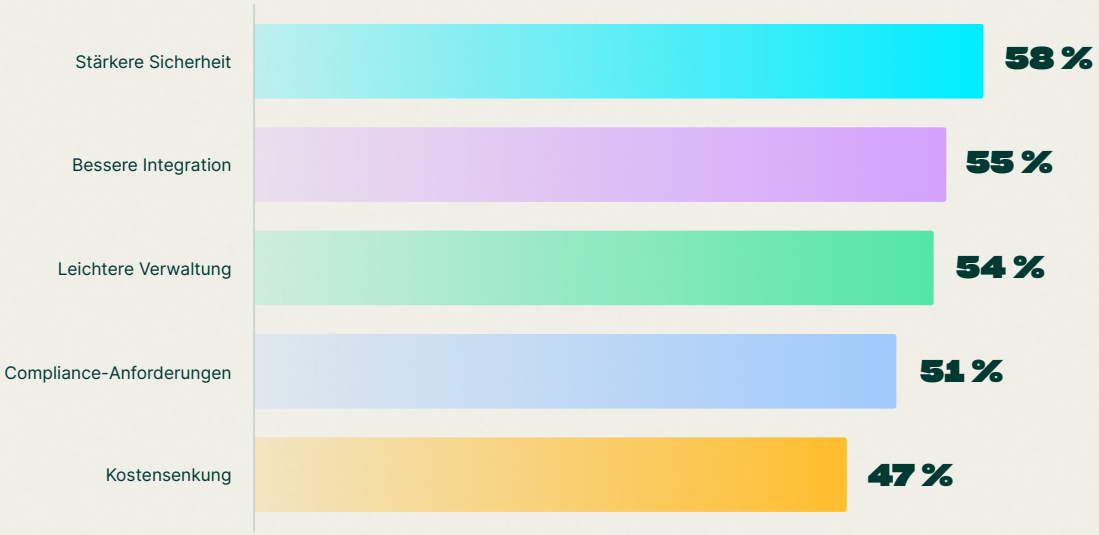
58 %

gehen diesen Schritt aus Sicherheitsgründen, was darauf hindeutet, dass es vielen Einzellösungen an Funktionen zur Bekämpfung identitätsbasierter Bedrohungen fehlt.

60 %

der Befragten haben in den letzten drei Jahren bereits ihren IAM-Anbieter gewechselt und planen dennoch einen erneuten Anbieterwechsel.

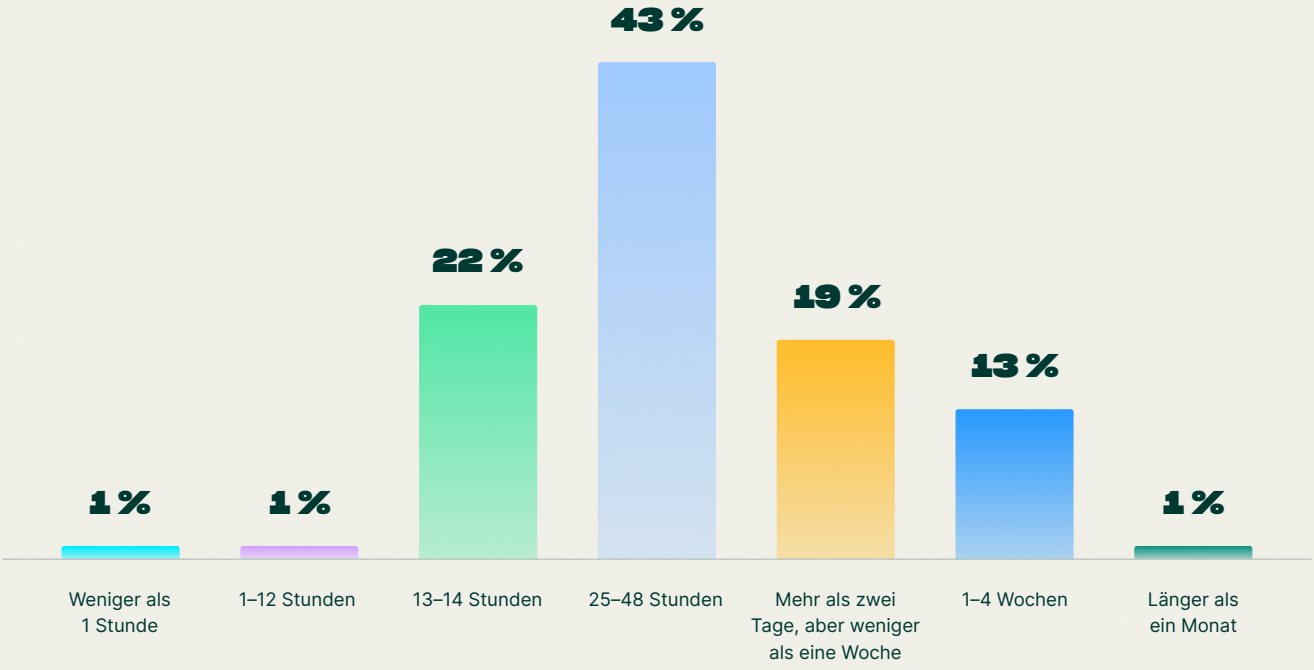
Die meistgenannten Gründe für einen Wechsel des Identitätsanbieters:



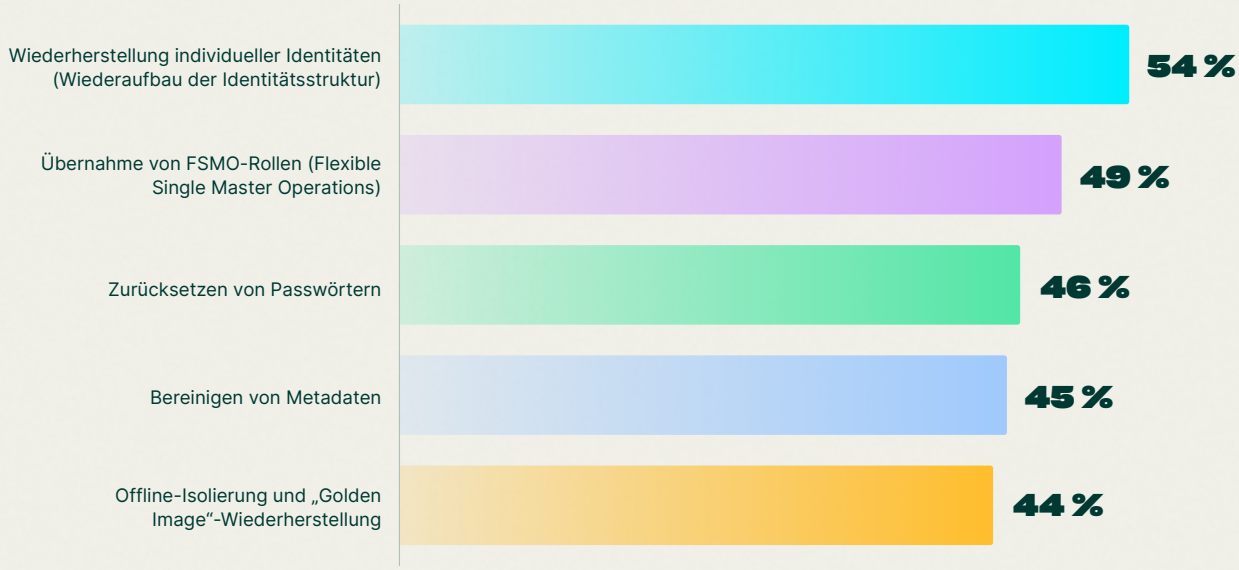
Viel besorgniserregender ist, wie lange die meisten Unternehmen brauchen würden, um ihre Identitätsinfrastruktur nach einem Sicherheitsvorfall wieder auf Kurs zu bringen. Geht man davon aus, dass Ausfallzeiten ein Unternehmen bis zu 6.000 USD pro Minute kosten können,[9] dann sehen sich die Unternehmen, die sich auf manuelle Wiederherstellungsprozesse verlassen (54 %) schnell sehr hohen Kosten gegenüber.

[9] https://www.isaca.org/resources/news-and-trends/industry-news/2024/centralized-services-and-their-impact-on-business-continuity

So lange benötigen Unternehmen nach eigenen Angaben, um die Identitätsinfrastruktur nach einem Angriff wiederherzustellen:



Prozesse, die manuelle Wiederherstellungsschritte erfordern:



Interessanterweise haben 89 % der Befragten KI-Agenten bereits komplett oder teilweise in ihre Identitätsinfrastruktur integriert. Diese neuen Arten von NHIs müssen ebenfalls umfassend während ihres gesamten Lebenszyklus geschützt werden, um einen Missbrauch durch Angreifer zu verhindern. Schon heute schätzt mehr als die Hälfte der Umfrageteilnehmer (58 %), dass im nächsten Jahr mindestens 50 % aller Cyber-Attacken auf agentische KI zurückzuführen sein werden.

Wenn Unternehmen nicht wissen, welche Bedrohungsakteure es aus welchen Gründen auf welche Identitäten abgesehen haben, sind sie nicht in der Lage, Incident-Response- und Wiederherstellungszeiten effektiv zu messen und zu verbessern.

WARUM DAUERT DIE WIEDERHERSTELLUNG SO LANGE?

MTTR ALS DATENGESTÜTZTE ANTWORT

Viele Unternehmen streben Cyber-Resilienz an, können sie aber nicht quantifizieren. Wie also lässt sich die Fähigkeit eines Unternehmens, Cyber-Bedrohungen zu antizipieren, abzuwehren, sich von ihnen zu erholen und aus den Erfahrungen zu lernen, wirksam messen?

Oft werden die Recovery Time Objective (RTO) und die Recovery Time Objective (RPO) als Messwerte herangezogen, aber sie sind nicht immer aussagekräftig. So mag ein Unternehmen eine RTO von vier Stunden haben, aber in Realität hat es 32 Tage gedauert, bis der Normalbetrieb wieder hergestellt war. Mitunter wird die RPO in Minuten angegeben, doch im Bankwesen und anderen Branchen kann die Durchsetzung dieses Zielwerts dazu führen, dass Hunderttausende von Transaktionsdaten verloren gehen. Wir sehen hier, dass die verantwortlichen Teams die Zielvorgaben nicht erreicht haben, doch die Gründe sind unklar.

Zudem nutzen Unternehmen oft unterschiedliche Messwerte, was es unmöglich macht, Wiederherstellungszeiten branchenübergreifend objektiv nachzuvollziehen. Manche messen die Zeit bis zur Aufdeckung einer Bedrohung, andere bis zur vollständigen Beseitigung. Das macht es schwierig, die Cyber-Resilienz einer Organisation effektiv zu ermitteln.

Um die Fähigkeit zu messen, sich von einem Cyber-Vorfall zu erholen, empfiehlt Rubrik Zero Labs daher die mittlere Wiederherstellungszeit (Mean Time to Recover; MTTR) als eine datengestützte Branchenmetrik, die die verschiedenen Phasen berücksichtigt.

EIN NEUES FRAMEWORK ZUR AUFSCHLÜSSELUNG DER MTTR

Die MTTR lässt sich nicht über eine einzelne Messung ermitteln. Sie umfasst einen Prozess mit mehreren Phasen, die jeweils aussagekräftige Einblicke und Bereiche mit Verbesserungspotenzial vermitteln:

Erkennen	Dies ist der Ausgangspunkt für jeden Vorfall – sei es ein Cyber-Angriff oder ein versehentlicher Löschvorgang.
Ermitteln des Ausmaßes	In dieser Phase wird identifiziert, welche Systeme und Assets betroffen sind und welche Abhängigkeiten bestehen. Ein Überblick darüber, welche Anwendungen und Datenbanken jeweils voneinander abhängig sind, ist unerlässlich.
Identifizieren eines sauberen Wiederherstellungspunkts	Dies ist oft die langwierigste und kritischste Phase, in der ein vertrauenswürdiges Backup ohne Malware identifiziert wird, das für die Wiederherstellung genutzt werden kann. Früher musste dafür in wochen- oder monatelanger Arbeit ein Clean Room eingerichtet werden. Heute beschleunigen Cloud-basierte Infrastrukturen und moderne Automatisierungstools diesen Prozess.
Wiederherstellen	In dieser Phase werden die Daten wiederhergestellt. Falls dieser Vorgang mehrere Wochen in Anspruch nimmt, könnte ein Durchsatzproblem vorliegen – ein datengestütztes Argument für Investitionen in die Infrastruktur, um risikobehaftete Wiederherstellungszeiten zu verkürzen. Angesichts der enormen Datenmengen in modernen Unternehmensumgebungen dauert diese Phase möglicherweise noch länger als die Identifizierung eines sauberen Wiederherstellungspunkts.
Validieren	Wie lange dauert es, bis Anwendungen wieder in einem einwandfreien Zustand sind und auf die Daten zugegriffen werden kann? Wie lange, bis die erforderlichen menschlichen und nicht-menschlichen Identitäten wieder korrekt funktionieren und kommunizieren?

Indem Unternehmen jede Phase einzeln messen, ersetzen sie eine einzige, kontextlose Zahlenangabe durch die notwendigen detaillierten Erkenntnisse, um Engpässe zu identifizieren und datengestützte Entscheidungen zu treffen.

Gemessene Phase	Beginn der Phase	Ende der Phase	Beschreibung
Mean-Time-to-Detect (MTTD)	Zeitstempel der Angriffsauswirkungen oder Zeitpunkt des Alarms	Bestätigung des bekannten Wiederherstellungsumfangs	Diese Phase umfasst Bedrohungserkennung, Anomalie-Analysen und SIEM-Korrelation.
Mean-Time-to-Scope (MTTS)	Validierte Erkennung der Bedrohung	Liste mit Wiederherstellungsobjekten wurde erstellt	Diese Phase basiert auf globalen Suchen, Datenklassifizierung und SLA-Metadaten.
Mean-Time-to-Clean-Snapshot (MTTCS)	Bestätigung des Umfangs	Identifizierung eines sauberen, nicht kompromittierten Snapshots	Unveränderlichkeit, Bedrohungsscans und eine Bewertung des Snapshot-Zustands können diese Phase verkürzen.
Mean-Time-to-Restore (MTTR)	Wiederherstellung wird initiiert	Daten werden den Workloads zur Verfügung gestellt	Diese Phase umfasst Instant Recovery, Live Mount und Funktionen für eine koordinierte Disaster Recovery in der Cloud.
Mean-Time-to-Validate (MTTV)	Datenzugriff ist wiederhergestellt	Bestätigung des einwandfreien Zustands von Anwendungen	Diese Phase wird durch App-Konsistenz, Automatisierungs-Playbooks und Malware-Scans nach der Wiederherstellung unterstützt.

MTTR insgesamt (Betrieb) = MTTD + MTTS + MTTCS + MTTR + MTTV

WARUM DIE MTTR WICHTIG IST

Viele moderne Unternehmen ignorieren die Erkenntnisse, die sie aus ihren Backup-Daten gewinnen könnten. Diese Daten ermöglichen nicht nur eine erfolgreiche Wiederherstellung, sondern können dank MTTR-Kennzahlen auch zur Messung der Resilienz genutzt werden.

Letztendlich ist die MTTR nur eine Phase in einem kontinuierlichen Zyklus der Reifegradbewertung mit folgenden Elementen:

1

Bestimmen der Resilienz

Mit einem effektiven Bewertungssystem (ähnlich einer Risikobewertung) können Unternehmen ihre derzeitigen Funktionen für die Angriffsabwehr einschätzen – basierend auf den wichtigsten Anwendungen und wahrscheinlichen Angriffsszenarien.

2

Definieren des MVB (Minimum Viable Business)

Unternehmen müssen verstehen, welche geschäftskritischen Anwendungen und Datenbanken erforderlich sind, um den Betrieb aufrechtzuerhalten, welche Abhängigkeiten bestehen und was priorisiert werden muss. Umfrageergebnisse und Anwendungslisten reichen nicht aus.

3

Validieren der Wiederherstellbarkeit

Echte Krisensimulationen – softwaregestützte Szenarien mit realistischen, interaktiven Übungen – produzieren messbare Kennzahlen in Bezug auf die Wiederherstellungszeit, die dann als Grundlage für Optimierungsinitiativen dienen.

4

Analysieren und Optimieren

In jeder Phase der Wiederherstellungsbemühungen muss ermittelt werden, wo Engpässe auftreten und wie sie behoben werden können. Wenn beispielsweise der Umfang der geschäftskritischen Daten von 20 TB auf 2 TB reduziert werden kann, verringert sich der Durchsatz bei der Wiederherstellung erheblich.

Durch die Anonymisierung und Zusammenführung von MTTR-Daten können Unternehmen aussagekräftige Benchmarks für den Branchen- und regionalen Vergleich erstellen. Wenn den Sicherheits-, IT- und für die Wiederherstellung verantwortlichen Teams dieselben Leistungskennzahlen (wie Wiederherstellungsgeschwindigkeit und -zuverlässigkeit) zur Verfügung stehen, können Führungskräfte leichter Finanzmittel für die Cyber-Resilienz beschaffen und Silos beseitigen.

AUFBAU VON IDENTITÄTS-RESILIENZ:

EMPFEHLUNGEN UND ABWEHRFUNKTIONEN

Identitäten sollten nicht nur als Assets betrachtet werden, die geschützt werden müssen. Vielmehr stellen sie eine wichtige Kontrollebene dar, die moderne Unternehmen bei allen Sicherheitsentscheidungen berücksichtigen müssen.

Es muss in umfassendes Identitätsmanagement, die Verwaltung des privilegierten Zugriffs und zeitgemäße Authentifizierungslösungen investiert werden, nicht nur in Schutzmaßnahmen für Endpunkte und Netzwerke. Eine kompromittierte Identität ist heute ein direkter und oft unentdeckter Weg zu den wichtigsten Assets eines Unternehmens. Daher ist jede Identität ein geschäftskritischer Kontrollpunkt.

Angesichts der zahlreichen Angriffe auf Identitäten sollten Unternehmen folgende Bereiche priorisieren:

Überblick über und Wiederherstellung von Identitäten

Welche Systeme müssen von der Umgebung abgetrennt werden, wenn ein Cloud-API-Schlüssel kompromittiert wurde? Angenommen, Hacker übernehmen die Kontrolle über einen Administrator-Account für Okta oder Active Directory. Können Sie das Problem schnellstens isolieren und erzwingen, dass sich die betroffenen Benutzer erneut authentifizieren? Die Beantwortung dieser Fragen erfordert Echtzeittransparenz und Wiederherstellungsfunktionen für hybride Identitätsumgebungen.

Aufbau von Identitätsresilienz

Resilienz ist die Fähigkeit, schnell und souverän wieder auf Kurs zu kommen. Unternehmen benötigen sichere Offline-Backups von Active Directory-Daten bzw. von Daten aus Cloud-Verzeichnissen, um Identitätsservices schnell wiederherstellen zu können, falls diese Daten verschlüsselt oder gelöscht werden. Unternehmen, die die Wiederherstellungsschritte synchron mit Sicherheitsmaßnahmen planen, reduzieren die mit einem Identitätsdiebstahl einhergehenden Ausfallzeiten und finanziellen Folgen.

Minimierung der Angriffsfläche und des Schadensausmaßes mit einem Zero-Trust-Ansatz

Identitäten sollten als Perimeter betrachtet werden. Jede Zugriffsanfrage – unabhängig davon, ob sie von einer Entität innerhalb oder außerhalb des Netzwerks gestellt wird – muss authentifiziert, autorisiert und verschlüsselt werden. In der Praxis bedeutet dies, starke MFA-Authentifizierung, bedingte Zugriffsrichtlinien und Zugriff nach dem Least-Privilege-Prinzip durchzusetzen.

ZERO-TRUST BEI DER IDENTITÄTSSICHERHEIT

Least-Privilege-Prinzip und rollenbasierte Zugriffskontrollen (RBAC)

Alle Benutzer und Geräte erhalten unabhängig von ihrem Standort nur die Mindestzugriffsrechte, die für die Erfüllung ihrer spezifischen Aufgaben erforderlich sind.

Just-in-Time-Zugriff (JIT)

Erweiterte Berechtigungen und erweiterter Zugriff werden nur für den spezifischen, begrenzten Zeitraum gewährt, den ein Benutzer benötigt, um eine sensible Aufgabe zu erledigen. Anschließend werden die Berechtigungen automatisch wieder entzogen.

Kontinuierliche Verifizierung

Zusätzlich zu starker MFA müssen während einer Sitzung die Benutzeridentität, der Gerätestatus und der Kontext (wie Standort und Uhrzeit) kontinuierlich überwacht und neu bewertet werden, um die Zugriffsrechte entweder aufrechtzuerhalten oder zu entziehen.

Mikrosegmentierung

Unternehmen sollten Netzwerke in isolierte Segmente unterteilen, um potenzielle Sicherheitsrisiken einzudämmen und zu verhindern, dass unbefugte Benutzer von einem Segment zum anderen wechseln und sich auf der Suche nach Angriffszielen ausbreiten können.

DER LEBENSZYKLUS DER CYBER-RESILIENZ

Echte Cyber-Resilienz geht über Cyber-Sicherheit hinaus und kombiniert zusätzlich Risikomanagement, Geschäftskontinuität sowie Incident Response zu einer einheitlichen Strategie. Das Ziel besteht nicht nur darin, Angriffe zu verhindern, sondern es geht auch darum, während eines Angriffs möglichst betriebsfähig zu bleiben und schnell und mit minimalem Schaden wieder auf Kurs zu kommen.

Der Lebenszyklus der Cyber-Resilienz

Das Framework von Rubrik Zero Labs zielt in Übereinstimmung mit den NIST-Richtlinien[10] darauf ab, Cyber-Angriffe zu antizipieren, abzuwehren, sich von ihnen zu erholen und aus den Erfahrungen zu lernen. Es soll den Expertenteams in der Praxis helfen, resiliente Prozesse einzuführen, und der Unternehmensleitung Benchmarks und Leistungskennzahlen für Optimierungsinitiativen an die Hand geben.

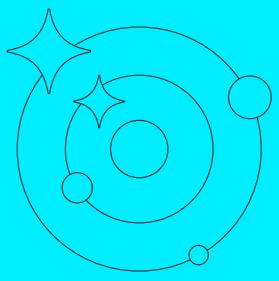
Wenn Unternehmen die Identitätsresilienz in weiter gefasste Programme zur Stärkung der Cyber-Resilienz integrieren, sind sie auf dem besten Weg, Störungen zu minimieren, geschäftskritische Assets zu schützen und das Vertrauen wichtiger Stakeholder zu gewinnen.

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

DATEN UND METHODOLOGIE

Rubrik Zero Labs hat sich das Ziel gesetzt, praxistaugliche, objektive Informationen bereitzustellen, die zur Minderung von Datensicherheitsrisiken genutzt werden können.

Zu diesem Zweck haben wir hauptsächlich Informationen aus drei verschiedenen Quellen in unseren Bericht aufgenommen:

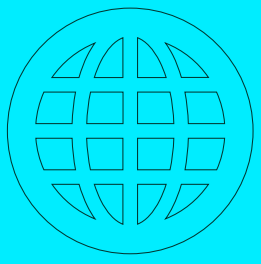


TELEMETRIEDATEN VON RUBRIK

Anhand der Telemetriedaten von Rubrik haben wir uns ein Bild vom Datenbestand eines typischen Unternehmens und den damit einhergehenden Risiken gemacht.

UNABHÄNGIGE FORSCHUNG

Ansichten von über 1.600 IT- und Sicherheitsmanagern (ermittelt von Wakefield Research)



BEITRAGENDE UNTERNEHMEN

Forschungsergebnisse renommierter Cyber-Sicherheitsunternehmen und institutionen