

COHESITY

# DIE IDENTITÄTSSCHICHT

IST DER AUSGANGSPUNKT FÜR CYBERANGRIFFE



*Warum Führungskräfte aus den Bereichen IT und Sicherheit nachweisen müssen, dass sie die Identitätsinfrastruktur wiederherstellen können*

# EINLEITUNG

Die Unternehmensidentität sollte Ihnen das Leben eigentlich erleichtern. Organisationen zentralisierten den digitalen Zugriff erstmals in den späten 1960er- und frühen 1970er-Jahren, wodurch sie an einer zentralen Stelle entscheiden konnten, wer Zugang erhielt und auf welche Ressourcen zugegriffen werden durfte. LDAP und Plattformen wie Active Directory machten diese Idee später zu einer einzigen Quelle der Wahrheit für das gesamte Netzwerk. Das funktionierte hervorragend.

Genau darin liegt das Problem.

Diese zentrale Quelle der Wahrheit ist nun der einfachste Weg, um einzudringen. Angreifer brechen nicht mehr ein. Sie melden sich mit gestohlenen Anmeldedaten und legitimen Zugriffsrechten an und gelangen so direkt zu Ihren kritischsten Systemen. Nichts passiert. Kein Alarm ertönt. Sie nutzen dieselbe Tür, die Ihre Mitarbeiter jeden Morgen benutzen – was dieses Problem grundlegend von dem unterscheidet, für dessen Lösung die meisten Sicherheitsprogramme entwickelt wurden.

Jahrelang haben Sie Ihre Abwehrmaßnahmen um einen Perimeter herum aufgebaut: eine Mauer, die Eindringlinge fernhalten sollte. Die Mauer steht noch immer, aber Angreifer klettern nicht mehr darüber. **Die Kompromittierung Ihrer Identitätsinfrastruktur ist einfacher, unauffälliger und zuverlässiger, weshalb die Identität den Netzwerkperimeter als primäres Schlachtfeld ersetzt hat.** Die meisten Sicherheits-Stacks wurden nie dafür konzipiert, auf diesem Terrain zu kämpfen.

Die Zahlen sind eindeutig. Im Jahr 2024 waren 79 % der Angriffe malwarefrei: kein Virus, der einen befallen könnte, sondern lediglich Social Engineering, gestohlene Anmeldedaten und vertrauenswürdige Fernzugriffstools, die sich der Erkennung entzogen. Im Jahr 2025 stieg dieser Anteil auf 82 %, da Angreifer noch stärker auf gültige Anmeldedaten, vertrauenswürdige Identitätsabläufe und genehmigte SaaS-Integrationen setzten, um unentdeckt zwischen Domänen zu wechseln (CrowdStrike Global Threat Report). Die Trendlinie zeigt eindeutig in eine Richtung.

Dies ist die unangenehme Ausgangslage, von der jedes ernstzunehmende Sicherheitsprogramm heute ausgehen muss. Das System, das Sie aufgebaut haben, um den Zugriff auf alles zu kontrollieren, hat sich still und leise zum einfachen Zugang zu allem entwickelt. Das ist kein Grund zur Panik. Es ist ein Grund, Identitäten an erster Stelle zu schützen und vor allem nachweisen zu können, dass Sie diese wiederherstellen können.

## Warum Unternehmensidentität angegriffen wird

Für einen Angreifer ist die Identität das wertvollste und am einfachsten zu erreichende Ziel in Ihrem Unternehmen, denn bereits ein einziger kompromittierter Satz Anmeldedaten kann den Zugang zu allem dahinter ermöglichen. Identität ist nicht nur ein weiterer Angriffsvektor. Sie ist der einzige Vektor, nach dem ein moderner Angreifer aktiv sucht.

Doch hier liegt der Haken: Fast nichts in Ihrer Infrastruktur wurde dafür entwickelt, dies zu verhindern. EDR, Firewalls und Netzwerksegmentierung sind alle darauf ausgelegt, Eindringlinge abzufangen – nicht aber, jemanden zu hinterfragen, der sich mit gültigen Anmeldedaten angemeldet hat. Für Ihre Abwehrsysteme sieht der Angreifer genau wie einer Ihrer Mitarbeiter aus.

Und dieser blinde Fleck wird immer größer. Die meisten Active-Directory-Umgebungen sind Jahrzehnte alt. Jahrelange Notlösungen, vergessene Konten und unbemerkte Fehlkonfigurationen haben sich im Hintergrund angehäuft, wo niemand hinschaut. Dieser Berg besteht nicht nur aus technischen Schulden. Es ist ein unverschlossenes Fenster, und genau danach suchen Angreifer als Erstes.

Hybride Identitäten machen die Situation noch schlimmer. Die meisten Organisationen nutzen mittlerweile eine Mischung aus lokalem Active Directory und Cloud-Identitätsanbietern wie Entra ID und Okta, und jede Verbindung zwischen ihnen vergrößert die Angriffsfläche. Noch schlimmer ist, dass sich eine Schwachstelle in Entra ID oder Okta oft direkt auf Active Directory zurückführen lässt, da Active Directory in der Regel die zentrale Quelle der Wahrheit ist, auf die sich alles andere verlässt. Knackt man das Fundament, wackelt die gesamte Struktur.

### ACTIVE DIRECTORY STEHT IM ZENTRUM DER UNTERNEHMENSIDENTITÄT

Active Directory verwaltet seit über 25 Jahren die Identitätsverwaltung in Unternehmen und ist nach wie vor in 90 % der Organisationen weltweit im Einsatz. Die meisten Cloud-Identitätsanbieter sind mit ihm vernetzt oder synchronisiert, was bedeutet, dass Active Directory auch bei der Einführung neuerer Plattformen weiterhin das Fundament bildet, auf dem alle anderen aufbauen.

#### Tatsächlich:

- Bei mehr als 78 % der von Menschen durchgeführten Angriffe kommt es zu einer Kompromittierung des Domänencontrollers.
- In 35 % dieser Fälle wird der Domänencontroller zum Ausgangspunkt, von dem aus sich Ransomware in der gesamten Umgebung ausbreitet.

Wenn ein Angriff erfolgt, ist Active Directory oft das Einzige, was zwischen Ihnen und der Wiederherstellung steht. Überlegen Sie, was das bedeutet: Wenn Sie sich nicht bei Ihrer eigenen Backup-Lösung anmelden können, können Sie mit der Wiederherstellung gar nicht erst beginnen. Angreifer wissen das nur zu gut, weshalb sie zunehmend gleichzeitig Ihre Backup-Systeme und Ihr Active Directory angreifen. Wenn beide außer Gefecht gesetzt sind, haben Sie nicht mehr nur einen schlechten Tag. Sie befinden sich in einer Geiselsituation.

Und die Zeit läuft gnadenlos ab. Eine vollständige Wiederherstellung der Active-Directory-Gesamtstruktur kann Tage oder sogar Wochen dauern, und jede Stunde Ausfallzeit kann Organisationen bis zu 730.000 USD pro Stunde kosten ([\*Forrester, The Total Economic Impact™ of Quest Recovery Manager for Active Directory Disaster Recovery Edition\*](#)).

Herkömmliche Backup-Tools helfen Ihnen hier nicht weiter. Sie können zwar einzelne Domänencontroller und Dateien kopieren, sind jedoch nicht in der Lage, die präzisen, aufeinander abgestimmten Schritte zu koordinieren, die für den Wiederaufbau einer gesamten Active Directory-Gesamtstruktur erforderlich sind. Die einzelnen Teile zu sichern ist nicht dasselbe wie sie wieder zusammenzusetzen.

## UNTERSTÜTZENDE DATEN

32%

**Anstieg identitätsbasierter Angriffe um 32 % im ersten Halbjahr 2025. 97 % davon waren Passwort-Spray- oder Brute-Force-Angriffe**

*(Microsoft Digital Defense Report 2025)*

22%

**aller Sicherheitsverletzungen betrafen gestohlene Anmeldedaten; 88 % der Angriffe auf einfache Webanwendungen erfolgten speziell unter Verwendung gestohlener Anmeldedaten**

*(Verizon 2025 Data Breach Investigations Report)*

35%

**der Cloud-Vorfälle wurden durch den Missbrauch gültiger Konten verursacht**

*(CrowdStrike 2025 Global Threat Report)*

# Identität ist die Grundlage von MVC und Vertrauen – heute und in Zukunft

Ein Minimum Viable Company (MVC) ist die kleinste und schlankste Version einer Organisation, die erforderlich ist, um zu überleben und wesentliche Abläufe aufrechtzuerhalten. Wenn Organisationen von einem Cybervorfall betroffen sind, scheitern sie bei der Wiederherstellung nicht daran, dass ihre Backups versagen. Oft scheitern sie daran, dass sie versuchen, alles auf einmal oder in der falschen Reihenfolge wiederherzustellen.

Die Ebene, die die meisten Organisationen übersehen, dreht sich um Vertrauen und Kontrolle, und die Identität steht genau an der Schnittstelle zwischen diesen beiden. Sie ist der Hauptschlüssel zum Unternehmen. Wenn Sie keine vertrauenswürdige Identität etablieren können, können Sie nichts anderes sicher wiederherstellen.

**Das Identitäts- und Zugriffsmanagement (Identity and access management – IAM) ist für drei Core-Funktionen zuständig:**

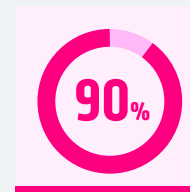
- **Identitätslebenszyklusmanagement:** Automatisiert die Einbindung neuer Mitarbeiter, Rollenaktualisierungen und die Aufhebung von Zugriffsrechten, sodass die Zugriffsrechte stets korrekt bleiben, wenn Mitarbeiter eintreten, ihre Rolle wechseln oder ausscheiden.
- **Authentifizierung:** Überprüft, ob eine Person tatsächlich die ist, für die sie sich ausgibt, in der Regel durch Multi-Faktor-Authentifizierung (MFA) und Single Sign-On (SSO).
- **Autorisierung:** Gewährt jedem authentifizierten Benutzer den spezifischen Zugriff, den er zur Erfüllung seiner Aufgaben benötigt, und schränkt alles andere ein.

Führt man diese drei Funktionen zusammen, sind Active Directory, Entra ID und Okta nicht mehr nur „Grundausstattung“, sondern werden zum betrieblichen Rückgrat Ihres Unternehmens. Sie authentifizieren jeden Mitarbeiter, jede Anwendung und jede Transaktion. Dies führt zu einer einfachen, unbequemen Wahrheit: Wenn die Identitätsinfrastruktur ausfällt, bricht das gesamte Geschäft mit ihr zusammen.

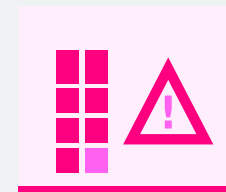
Und dieses betriebliche Rückgrat wird bald deutlich stärker exponiert sein. Während Organisationen sich beeilen, KI und agentenbasierte Arbeitsabläufe einzuführen, sind diese Agenten auf die Identitätsinfrastruktur angewiesen, um sicher zu funktionieren – und dieser Wandel ist bereits in den Daten erkennbar: 93 % der Organisationen nutzen bereits KI-Agenten oder planen deren Einsatz für sensible Sicherheitsaufgaben wie Passwort-Zurücksetzungen und VPN-Zugriff (Semperis, Mai 2026).

Hier ist der Punkt, der Ihre Aufmerksamkeit erfordert: Diese Agenten übernehmen häufig die Identitäten der Mitarbeiter, die sie anweisen, Aufgaben auszuführen und auf sensible Daten zuzugreifen. Jeder einzelne von ihnen stellt einen neuen Schlüsselsatz dar. Die Herausforderungen bei der Sicherheit, dem Schutz und der Wiederherstellung von Identitäten waren noch nie so groß wie heute.

## UNTERSTÜTZENDE DATEN



Active Directory und Entra ID werden von über 90 % der Unternehmen weltweit genutzt (Semperis).



Active Directory ist an 9 out of 10 Cyberangriffen, beteiligt – nicht, weil es schlecht konzipiert ist, sondern weil es überall im Einsatz ist (Cohesity CERT).

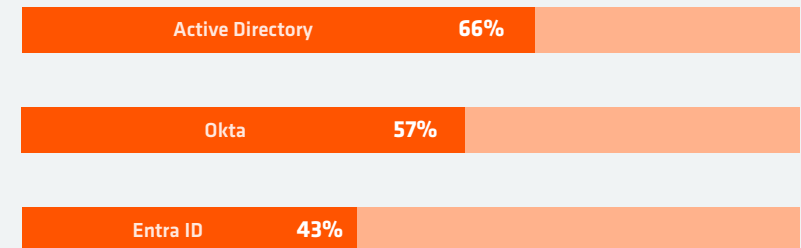
# Die Schnittstelle zwischen Identität, Geschäftskontinuität und Cyber-Resilienz

Bei der traditionellen Planung der Geschäftskontinuität wird Identität wie Strom behandelt: als Infrastruktur, von der man annimmt, dass sie verfügbar ist, sobald man den Schalter umlegt. Genau diese Annahme ist der Grund, warum Organisationen zugrunde gehen. Identität darf nicht länger eine Selbstverständlichkeit sein. Sie benötigt ihren eigenen Wiederherstellungsplan.

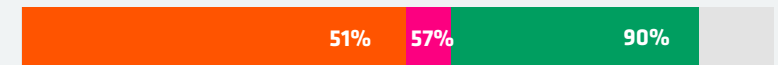
Cyber-Resilienz stellt diese Annahme auf den Kopf. Sie behandelt Identität als das Erste, was angegriffen wird, und als das Erste, was Sie wiederherstellen können müssen (unabhängig, getestet, isoliert und vertrauenswürdig) – selbst wenn alles um sie herum kompromittiert ist. Die Kluft zwischen „Wir gehen davon aus, dass es funktioniert“ und „Wir haben bewiesen, dass es funktioniert“ ist genau der Punkt, an dem Organisationen nach einem Angriff Tage oder Wochen verlieren. Sie können ihre Dateien zwar problemlos wiederherstellen. Sie können jedoch keine einzige Person anmelden, damit diese die Dateien nutzen kann.

**Für Führungskräfte aus den Bereichen Sicherheit, IT und Geschäftsleitung ist die Schlussfolgerung eindeutig: Geschäftskontinuität und Cyber-Resilienz sind nur dann erfolgreich, wenn proaktive Identitätssicherheit und Identitätswiederherstellung als eigenständige Disziplinen geplant, getestet und mit Ressourcen ausgestattet werden. Gehen Sie niemals davon aus, dass dies automatisch geschieht, während Sie alles andere wiederherstellen. Hoffnung ist kein Wiederherstellungsplan.**

## UNTERSTÜTZENDE DATEN



**Nur bei 66 % der Organisationen umfasst der Notfallwiederherstellungsplan Active Directory, bei 43 % Entra ID und bei 57 % Okta, sodass ein großer Teil der Kontinuitätspläne eine Lücke auf der Identitätsebene selbst aufweist** (*Semperis, Nov 2025*).



**90 % der Organisationen prüfen auf Identitätsschwachstellen, doch nur 51 % verfügen über Behebungsmaßnahmen, und lediglich 57 % automatisieren die Identitätswiederherstellung** (*Semperis, Nov 2025*).

## Die Kosten der **Untätigkeit**

Sprechen wir über den Preis des Abwartens, denn auch das Abwarten ist eine Entscheidung – und zwar die teuerste, die zur Auswahl steht. Nicht nur in finanzieller Hinsicht, sondern auch in Bezug auf den Betrieb und den Ruf.

**Diese Kosten bestehen nicht aus einer einzigen Rechnung. Es sind drei, und sie summieren sich:**

- **Die Kosten für die Sicherheitsverletzung:** Vorfallsreaktion, gesetzliche Bußgelder und rechtliche Risiken
- **Die Kosten für Ausfallzeiten:** Produktivitätsverluste, entgangene Einnahmen und wiederholte Angriffe, solange die Identitätsebene ungeschützt bleibt
- **Die Kosten des Vertrauensverlusts:** steigende Prämien für Cyberversicherungen, Haftungsrisiken für Führungskräfte und Geschäftsrisiken

Und durch das Abwarten bleibt der Zähler nicht stehen. Die Angriffsfläche im Bereich der Identitätsverwaltung gehört zu den am häufigsten ins Visier genommenen im Unternehmen – und zu denen, mit denen herkömmliche Abwehrmaßnahmen nicht Schritt halten können, sodass die Kosten der Untätigkeit nicht statisch bleiben. Sie steigen mit jedem Quartal, in dem Sie das Problem ungelöst lassen. Verzögerung ist keine Vorsicht. Vielmehr handelt es sich um Zinseszinsen auf eine Schuld, die Sie nie freiwillig auf sich genommen haben.

## UNTERSTÜTZENDE DATEN



Über einen Zeitraum von drei Jahren können Organisationen mit den Kosten eines erfolgreichen Identitätsangriffs in Höhe von **1,2 Millionen USD**, den Kosten für die manuelle Überwachung hybrider Identitäten in Höhe von **109.000 USD** sowie Produktivitätsverlusten und Ausfallzeiten aufgrund der manuellen Wiederherstellung von Active Directory in Höhe von **3,9 Millionen USD** konfrontiert sein. (Forrester Total Economic Impact study).



Die weltweiten Durchschnittskosten einer Datenschutzverletzung betragen **4,44 Millionen USD**, doch Angriffe auf Anmeldedaten verursachen Kosten von rund **4,67 Millionen USD** und benötigen etwa **292 Tage**, um identifiziert und eingedämmt zu werden – damit sind sie der langsamste aller Angriffsvektoren (IBM Cost of a Data Breach 2025).



Die wirtschaftlichen Rahmenbedingungen bei Ransomware verschieben sich, jedoch nicht ohne Schwierigkeiten: Der Medianwert der gezahlten Lösegeldsummen ist auf **115.000 USD** gesunken, und **64 %** der Opfer weigerten sich zu zahlen, was bedeutet, dass immer mehr Organisationen die betrieblichen Kosten für die Wiederherstellung selbst tragen, anstatt das Lösegeld zu zahlen, was den Druck auf die Geschwindigkeit der Identitätswiederherstellung weiter erhöht (Verizon DBIR 2025).



**8 von 8** großen Cyberversicherern verlangen und überprüfen mittlerweile identitätsspezifische Maßnahmen zur Sicherheit und Resilienz bei der Zeichnung von Cyberpolicen, und der Nachweis einer starken Identitätsabsicherung steht in direktem Zusammenhang mit niedrigeren Prämien und höherem Versicherungsschutz (Cohesity, "[Identity resilience is critical for cyber insurance](#)").

Dies sind keine voneinander unabhängigen Datenpunkte. Es handelt sich um die detaillierte Abrechnung der Kosten für Datenschutzverletzungen und Ausfallzeiten, dicht gefolgt von den Kosten für den Vertrauensverlust, da Versicherer die Prämien direkt mit Ihrer Identitätssicherheit verknüpfen. Alle diese Kosten steigen, je länger die Identitätssicherheit unberücksichtigt bleibt. Diese Rechnung müssen Sie ohnehin bezahlen. Die einzige Frage ist, ob Sie jetzt einen kleinen Betrag zu Ihren Bedingungen oder später den gesamten Betrag zu den Bedingungen des Angreifers zahlen.

# FAZIT

Identitätsbasierte Kompromittierungen treten mittlerweile bei fast jeder größeren Datenschutzverletzung auf, und das Muster ändert sich nie. Angreifer brechen nicht ein. Sie melden sich mit gültigen Anmeldedaten und vertrauenswürdigen Identitätsabläufen an und bewegen sich unentdeckt durch Umgebungen, die nie dafür ausgelegt waren, sie zu erwischen. Dann stehlen sie Ihre Daten, übernehmen Ihre Systeme und setzen ihre Ransomware ein.

## Nichts davon ist unvermeidlich.

Was die Organisationen, die sich innerhalb von Stunden wiederherstellen, von denen unterscheidet, die Wochen damit verbringen, das Vertrauen in ihre Identitätsdienste wiederherzustellen, hat nichts mit Glück zu tun und nichts damit, wie viel sie ausgegeben haben. Es läuft auf eine einzige Entscheidung hinaus: ob sie Identitätsresilienz als eigenständigen Bereich über den gesamten Angriffslebenszyklus hinweg aufgebaut haben, noch bevor sie sie überhaupt benötigten.

Behandeln Sie Identitätsresilienz daher als das, was sie geworden ist: nicht als Option, sondern als zentrale Anforderung an die Sicherheit des Unternehmens. Identität ist gleichzeitig Ihre Eingangstür, Ihr Fundament und Ihr Engpass bei der Wiederherstellung. Ein Flickenteppich aus Einzellösungen wird immer zu kurz greifen. Ebenso wie jeder Kontinuitätsplan, der einfach davon ausgeht, dass die Identität im entscheidenden Moment vorhanden sein wird. Die einzige Strategie, die den Kontakt mit einem echten Angriff übersteht, ist die, die Sie getestet haben und die sich bewährt hat, noch bevor Sie sie benötigten.

Die gute Nachricht ist, dass Sie dem zuvorkommen können. Sie können die Cyber-Resilienz Ihrer kritischsten Identitätssysteme beschleunigen.

Und wir können Ihnen dabei helfen.

**Mehr dazu** wie Cohesity beim Aufbau und der Stärkung der Identitätsresilienz helfen kann

**Erhalten Sie eine kostenlose Bewertung Ihrer Identitätssicherheit** um Schwachstellen und Lücken in Active Directory, Entra ID und Okta zu identifizieren





© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

6100036-001-DE 8-2026