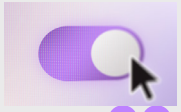
Commvault

eBOOK

DIE  WAHRHEIT ÜBER IDENTITÄTSRESILIENZ: DAS  NEUE IMPERATIV FÜR UNTERNEHMEN CYBERABWEHR 

Da die meisten Sicherheitslücken auf kompromittierte Zugangsdaten zurückzuführen sind, müssen Unternehmen über die Prävention hinausgehen und echte Identitätsresilienz aufbauen.

Identitätssysteme wie Microsoft Active Directory (AD), Entra ID und Okta sind die Kronjuwelen der Unternehmens-IT. Sie authentifizieren Benutzer und kontrollieren den Zugriff auf kritische Geschäftssysteme. Von der Anmeldung an Arbeitsstationen bis zum physischen Gebäudezugang ermöglichen Identitätssysteme den reibungslosen Betrieb von Organisationen und sind daher ein begehrtes Ziel für Cyberkriminelle.

Doch Folgendes ist den meisten Organisationen nicht bewusst: Herkömmliche Schutz- und Wiederherstellungsansätze für Identitätssysteme sind angesichts der heutigen Bedrohungslandschaft grundlegend unzureichend. Die Wahrheit über die Resilienz von Identitätssystemen geht weit über einfachen Datenschutz hinaus: Sie erfordert eine umfassende Strategie, die ausgeklügelte Angriffe antizipiert und eine schnelle Wiederherstellung in einen vertrauenswürdigen Zustand ermöglicht – mit der Geschwindigkeit moderner Geschäftsprozesse.resilience goes far beyond simple data protection: It requires a comprehensive strategy that anticipates sophisticated attacks and enables rapid recovery to a trusted state – at the speed of business.

Wenn Identitätssysteme nicht verfügbar oder kompromittiert sind, kann dies Geschäftsanwendungen und -prozesse massiv beeinträchtigen und den Zugriff der Benutzer auf wichtige Systeme und Ressourcen blockieren.

Hier wird Identitätsresilienz entscheidend. Resilienz bedeutet nicht nur die Sicherung Ihres Verzeichnisdienstes, sondern den Aufbau einer Identitätsinfrastruktur, die komplexen Angriffen standhält, sich an sie anpasst und sich schnell davon erholt, während gleichzeitig die Geschäftskontinuität gewährleistet wird.

IDENTITÄT: DIE PRIMÄRE ANGRIFFSFLÄCHE

Die Realität der modernen Cyberkriegsführung ist, dass die Identitätsinfrastruktur zum primären Schlachtfeld geworden ist. Angreifer erzwingen keinen gewaltsamen Zugriff mehr – sie loggen sich ein und nutzen kompromittierte Zugangsdaten, um sich legitimen Zugriff zu verschaffen. Einmal im System, können sie sich unbemerkt lateral bewegen.

die Umgebung, Berechtigungen ausweiten und die Wiederherstellungsmechanismen untergraben, bevor

Bevor überhaupt jemand bemerkt, was geschehen ist.

Die Statistiken zeichnen ein düsteres Bild der aktuellen Bedrohungslage.

88%

Bei Angriffen auf Webanwendungen wurden gestohlene Zugangsdaten verwendet.[1]

82%

Organisationen, die in den letzten [12] Monaten mindestens einen identitätsbasierten Angriff erlebt haben.[2]

57%

Die meisten Cyberangriffe begannen mit kompromittierten Identitäten.[3]

1 Bericht über die Untersuchung von Datenschutzverletzungen 2025Verizon
2 Bericht zur Zukunft der Identitätssicherheit 2025ConductorOne
3 Identity Crisis Report Varonis

IDENTITÄTSANGRIFFE SIND HEIMLICH, SKALIERBAR, UND SCHWER ZU ERKENNEN

Identitätsbasierte Angriffe sind aufgrund ihrer Subtilität besonders gefährlich. Indem sie sich als legitime Nutzer ausgeben, können Angreifer sich unauffällig in normale Aktivitäten einfügen.

Trotz der Vielfalt der angewandten Taktiken verfolgen diese Angriffe ein gemeinsames Ziel: die Ausnutzung von Identitäten, um autorisierten Zugriff zu erlangen und unentdeckt zu bleiben.

Diebstahl von Zugangsdaten
(Phishing, Token-Diebstahl, Malware)

Rechteausweitung durch Fehlkonfigurationen

Missbrauch übermäßiger Berechtigungen

Persistenz durch Verzeichnismanipulation oder Hintertürkonten

Heutzutage hat die KI-gestützte Automatisierung diese Angriffe beschleunigt, um Berechtigungen schneller auszuweiten und sich lateral auszubreiten. Unternehmen haben weniger Zeit denn je, um Kompromittierungen zu erkennen, Auswirkungen einzudämmen und sich zu erholen.

DIE KOMPLEXITÄT DES IDENTITÄTSSCHUTZES

Die unkontrollierte Ausbreitung von Identitäten beeinträchtigt Sichtbarkeit und Kontrolle.

Identitätsinformationen sind allgegenwärtig – in lokalen Systemen, Cloud-Plattformen und SaaS-Anwendungen. Diese Datenflut führt zu mehr Transparenzlücken und potenziellen Einfallstoren für Angreifer.

Komplexität vergrößert die Angriffsfläche.

Moderne Unternehmen arbeiten mit komplexen, miteinander verbundenen und voneinander abhängigen Identitätssystemen, die sich über lokale und Cloud-Umgebungen erstrecken. Dies vergrößert die Angriffsfläche und erschwert die Wiederherstellung.

Isolierte Werkzeugsysteme schaffen blinde Flecken.

Das Identitätsrisikomanagement erfolgt über voneinander getrennte Tools und Teams hinweg, was die Priorisierung erschwert, das frühzeitige Erkennen von Problemen beeinträchtigt und die Reaktion bei Vorfällen verlangsamt.

Mangelnde resiliente Wiederherstellung.

Viele Wiederherstellungsansätze sind langsam und komplex, was oft dazu führt, dass man auf kompromittierte Backups oder manuelle Neuaufbauten zurückgreifen muss, was die Ausfallzeit verlängert und das Risiko erhöht.

Diese Trends laufen zusammen und schaffen eine neue operative Realität:

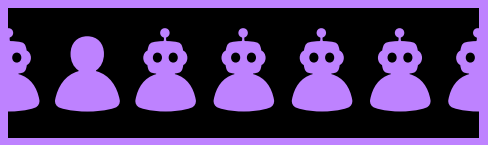
Identität ist die am stärksten angegriffene Ebene des Unternehmens.

Umgebungen für Identitäts- und Zugriffsmanagement (IAM) sind komplexer und stärker vernetzt als je zuvor.

Die Angriffe erfolgen schneller, leiser und sind schwieriger zu erkennen.

Eine schnelle und saubere Wiederherstellung ist wichtiger und gleichzeitig schwieriger als zuvor.

144:1



Verhältnis nicht-menschlicher Identitäten zu menschlichen Identitäten.[4]

75%

Organisationen nutzen mehrere Identitätsanbieter zur Verwaltung der Unternehmensidentität.[5]

4 Der NHI & Secrets Risikobericht H1 2025,Entro
5 Die Statusstudie zur Multi-Cloud-Identität,Strata

DIE AUSWIRKUNGEN IDENTITÄTSBASIERTER ANGRIFFE AUF ORGANISATIONEN

Die Bedeutung der Priorisierung von Identitätssicherheit wird deutlich, wenn man ihre Auswirkungen auf andere Workloads betrachtet. Anwendungen, Dateisysteme, E-Mail-Dienste und Datenbanken sind alle auf Identitätssicherheit für die korrekte Authentifizierung und den Benutzerzugriff angewiesen.

Wenn Identitätssysteme nicht verfügbar oder nicht vertrauenswürdig sind:

Mitarbeiter und Kunden können sich nicht authentifizieren.

Anwendungen und Dienste sind nicht mehr verfügbar.

Wiederherstellungszeiträume können sich auf Wochen oder Monate ausdehnen.

Identitätsresilienz erkennt diese grundlegende Abhängigkeit an. Da in modernen Unternehmen nahezu alles auf Identität beruht, wird der Aufbau einer resilienten Identitätsinfrastruktur zum Eckpfeiler organisatorischer Resilienz. Dies geht weit über die bloße Wiederherstellung von Identitätssystemen nach einem Angriff hinaus.

Durch die Etablierung von Maßnahmen zur Stärkung der Identitätsresilienz können Organisationen die Kontrolle über ihre Netzwerke und Systeme auch während aktiver Angriffe besser aufrechterhalten, Datensicherheits- und Zugriffsrichtlinien durchsetzen und eine stabile Grundlage schaffen, die eine schnelle Wiederherstellung anderer Systeme und Dienste ermöglicht.

DIE KOSTEN VON IDENTITÄTSKOMPROMITTIERUNG

Finanzielle Verluste

Identitätsbasierte Angriffe haben oft finanzielle Folgen, die weit über die anfängliche Schadensbegrenzung hinausgehen. Unternehmen sehen sich mit unmittelbaren Kosten konfrontiert, wie zum Beispiel Incident Response, Wiederherstellung und Ausfallzeiten, neben längerfristige Verluste wie Umsatzeinbußen und sinkendes Kundenvertrauen.

Betriebsstörungen

Da die Identität die Grundlage für den Zugriff auf kritische Systeme bildet, können Angriffe den Geschäftsbetrieb massiv lahmlegen. Mitarbeiter, Partner und Kunden verlieren den Zugriff auf Anwendungen und Dienste, die Produktivität sinkt, und die Wiederherstellungsmaßnahmen werden unter Umständen behindert.

Reputationsschaden

Identitätsbezogene Datenschutzverletzungen können das Kundenvertrauen und das Markenvertrauen unmittelbar beeinträchtigen. Negative Publicity und wahrgenommene Sicherheitslücken können zu Kundenabwanderung, geringerer Loyalität und langfristigen Schäden führen, die nur schwer vollständig behoben werden können.

Regulatorische Risiken

Wenn Identitätssysteme kompromittiert werden, kann der unbefugte Zugriff auf sensible Daten schwerwiegende regulatorische und Compliance-Folgen nach sich ziehen. Unternehmen können mit Bußgeldern, rechtlichen Schritten und verstärkter Überwachung rechnen, insbesondere in stark regulierten Branchen wie dem Finanz- und Gesundheitswesen.

50%

Organisationen meldeten im vergangenen Jahr Sicherheitsverletzungen im Zusammenhang mit kompromittierten Maschinenidentitäten.[6]

51%

Es kam zu Verzögerungen bei der Einführung von Anwendungen.[6]

44%

erlebten einen Ausfall oder eine Störung, die die Kundenerfahrung negativ beeinflusste.[6]

43%

Angreifer konnten sich unbefugten Zugriff auf Daten, Netzwerke und Systeme verschaffen.[6]

6 2025 State of Machine Identity Security Report, CyberArk

REALWELT-IDENTITÄTSBASIERTE STÖRUNG: WIE SOCIAL ENGINEERING DEN EINZELHANDEL MASSIV BEEINTRÄCHTIGTE

Im Jahr 2025 nutzte eine finanziell motivierte Bedrohungsgruppe koordinierte Social-Engineering-Taktiken, um Identitätssysteme in mehreren Einzelhandelsunternehmen im Vereinigten Königreich zu kompromittieren, darunter auch in der großen globalen Kette Marks & Spencer.[7]

Anstatt Software-Schwachstellen auszunutzen, zielten die Angreifer auf IT-Helpdesks und Supportprozesse ab. Sie gaben sich als Mitarbeiter aus, um Zugangsdaten zurückzusetzen, die Multi-Faktor-Authentifizierung zu umgehen und privilegierte Zugriffsrechte zu erlangen. Einmal im System, erweiterten sie rasch ihre Berechtigungen, griffen auf interne Systeme zu und störten den Betrieb.

In einigen Fällen nutzten Angreifer diesen Zugriff aus. um Ransomware einzusetzen, Daten zu exfiltrieren und geschäftskritische Dienste zu beeinträchtigen, die zeigen, wie schnell Identitätskompromittierung sich zu einer umfassenden operative Störung entwickeln kann.

Die Verstöße belaufen sich voraussichtlich auf einen finanziellen Gesamtschaden von

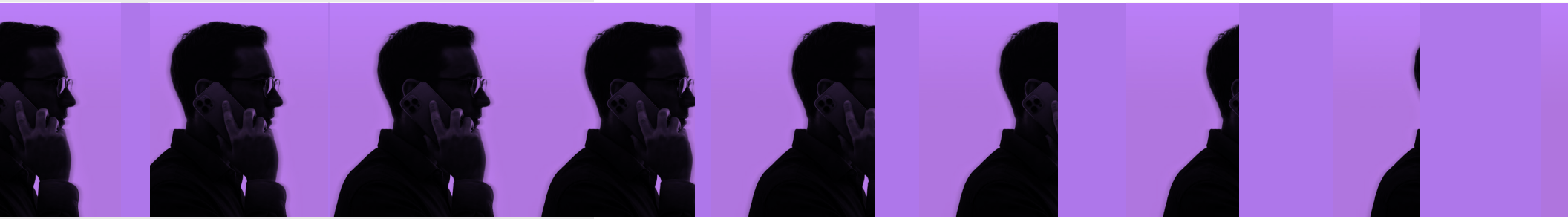
$592M[7]

Der Einzelhandel, die Lieferketten und die kundenorientierten Systeme waren von erheblichen Ausfällen und Beeinträchtigungen betroffen.[7]

46 TAGE:

Nach dem Angriff setzte M&S den Online-Verkauf vorübergehend aus.[8]

7 Die Hacker-Nachrichten
8 Reuters



WIE EIN ANRUF BEIM HELPDESK MILLIONENSCHÄDEN VERURSACHTE

In einem viel beachteten Vorfall aus dem Jahr 2023 wurde MGM, ein bedeutender Hotel- und Unterhaltungskonzern, durch Social Engineering zum Stillstand gebracht.

Die Angreifer gaben sich als interner Benutzer aus und kontaktierten den IT-Helpdesk. Sie konnten die Supportmitarbeiter erfolgreich davon überzeugen, Zugangsdaten zurückzusetzen und Zugriff auf privilegierte Konten zu gewähren. Von dort aus weiteten sie ihre Zugriffsrechte aus, bewegten sich lateral durch verschiedene Systeme und legten schließlich den Kernbetrieb lahm.

Dieses Beispiel unterstreicht ein Schlüsselprinzip der Identitätsresilienz: Organisationen müssen darauf vorbereitet sein, identitätsbasierte Angriffe schnell zu erkennen und einzudämmen, den vertrauenswürdigen Zugriff wiederherzustellen und den Betrieb ohne längere Unterbrechung wiederaufzunehmen.

Der Angriff verursachte dem Unternehmen Verluste von über 100 Millionen Dollar aufgrund von Systemausfällen – sowie 45 Millionen Dollar an Sammelklagen im Zusammenhang mit dem Angriff und einem Datenleck aus dem Jahr 2019.[9]

Kunden äußerten Bedenken hinsichtlich der Sicherheit und der operative Zuverlässigkeit.[10]

Der Vorfall löste behördliche Prüfungen und Untersuchungen im Zusammenhang mit den Melde- und Reaktionspraktiken aus.[10]

9 Die Aufzeichnung
10 Inszone Versicherungsdienstleistungen

DIE LÖSUNG: AUFBAU VON IDENTITÄTSRESILIENZ

WESENTLICHE BESTANDTEILE EINER STRATEGIE ZUR IDENTITÄTSRESILIENZ

Identitätsresilienz ist die Fähigkeit, Identitätsangriffe und andere Vorfälle schnell zu erkennen, einzudämmen und sich davon zu erholen, während gleichzeitig ein sicherer und zuverlässiger Zugriff für Benutzer und Anwendungen gewährleistet wird.

Zu den Kernelementen einer umfassenden Strategie zur Stärkung der Identitätsresilienz gehören:

Proaktive Risikobewertung zur Identifizierung und Priorisierung von Risiken und die Sicherheitslage zu stärken.

Echtzeit-Überwachungs- und Rollback-Funktionen ermöglichen eine schnellere Erkennung und Reaktion auf identitätsbasierte Angriffe.

Nachgewiesene Fähigkeit zur Wiederherstellung der Identitätsinfrastruktur schnell und zuverlässig in einen vertrauenswürdigen Zustand.

Transparenz, Reaktion und Wiederherstellung sowohl lokale und cloudbasierte Identitätsanbieter.

WIE COMMVAULT® UMFASSENDE IDENTITÄTSRESILIENZ BIETET

Der Aufbau von Resilienz im Identitätsbereich erfordert einen modernen, einheitlichen Ansatz. Commvault Cloud unterstützt Unternehmen dabei, Identitätssysteme – einschließlich AD, Entra ID und Okta – vor Bedrohungen wie Datenbeschädigung, versehentlichem Löschen und Ransomware zu schützen und schnell wiederherzustellen.

Mit einem umfassenden Ansatz zur Identitätsresilienz unterstützt Commvault Unternehmen dabei, Risiken proaktiv zu bewerten, Bedrohungen in Echtzeit zu erkennen und einzudämmen sowie ihre Identitätsanbieterumgebungen schnell und sicher in einen vertrauenswürdigen Zustand zurückzuversetzen.

Schwachstellenanalysen

Unterstützt Sie bei der Identifizierung von Fehlkonfigurationen und Sicherheitslücken in Ihrer AD-Umgebung – wie z. B. übermäßige Berechtigungen und nicht ablaufende Anmeldeinformationen – und ermöglicht Ihnen die Priorisierung von Risiken mit klaren, umsetzbaren Abhilfemaßnahmen, sodass Sie Ihre Sicherheitslage verbessern und Risiken reduzieren können.

Granulare Wiederherstellung

Hilft dabei, genau das wiederherzustellen, was benötigt wird, bis hin zu bestimmten Benutzern, Gruppen, Organisationseinheiten und sogar individuellen Attributen, ohne die Gesamtumgebung zu beeinträchtigen.

Unveränderbarer Schutz

Hilft dabei, Identitätssicherungen in manipulationssicheren Speichern zu schützen, die so konzipiert sind, dass Änderungen oder Löschungen durch kompromittierte Zugangsdaten verhindert werden.

Automatisiert, orchestrierte Wiederherstellung im großen Maßstab

Hilft Ihnen bei der Wiederherstellung ganzer AD-Forests, mehrerer Domänen und Domänencontroller durch koordinierte, automatisierte Arbeitsabläufe, die für komplexe, verteilte Umgebungen entwickelt wurden.

Echtzeit-Überprüfung und -Erkennung

Unterstützt die kontinuierliche Überwachung von Identitätsänderungen, einschließlich Rechteausweitung, Persistenztechniken und anomalem Verhalten, sodass Sie böswillige oder unautorisierte Änderungen untersuchen und sofort zurücksetzen können.

Integrierte Wiederherstellungstests

Hilft Ihnen, Vertrauen in Ihre Bereitschaft zur Abwehr von Cyberangriffen zu gewinnen, indem regelmäßige Test- und Wiederherstellungsabläufe durchgeführt werden, die Ihnen helfen, Ihre Wiederherstellungspläne zu validieren und Ihre Widerstandsfähigkeit zu verbessern.

ÜBER DIE IDENTITÄT HINAUS: DIE KOMPLETTE CYBER ERHOLUNGSSTRATEGIE

Die Konfrontation mit einem Cyberangriff oder einer Ransomware-Erpressung ist eine erschütternde Erfahrung. Die Wiederherstellung der Identitätssysteme ist in den meisten Fällen der erste Schritt. Die Automatisierung dieses ansonsten zeit- und ressourcenintensiven Prozesses kann die Wiederherstellung beschleunigen und den Geschäftsbetrieb schnell wiederaufnehmen. Noch besser ist es, wenn die Identitätswiederherstellung auf derselben Plattform basiert wie die übrige Cybersicherheitslösung.

Echte Identitätsresilienz geht über den Schutz von Identitätsanbietern hinaus.– Es lässt sich problemlos in Ihre umfassendere Cyber-Wiederherstellungsstrategie integrieren.

Die Vereinheitlichung des Cyber-Wiederherstellungs- und Wiederaufbauprozesses auf einer gemeinsamen Plattform ermöglicht eine einfache Koordination, Automatisierung und Orchestrierung, die über die reine Identitätswiederherstellung hinausgeht – Sie können die Wiederherstellung von Anwendungen, Daten, Clouds und Infrastruktur orchestrieren.

Dies wird Ihren Teams helfen, zusammenzuarbeiten, um Ihre Systeme nach Cyberangriffen und Katastrophen wiederaufzubauen und eine Widerstandsfähigkeit zu schaffen, die ein kontinuierliches Geschäft ermöglicht.

Erfahren Sie mehr über Commvault® Identity Resilience

commvault.com | 888.746.3849 | get-info@commvault.com