REPORT

Identity Security Report 2026

Das sagen 5.000 IT- und Cybersicherheitsexperten aus 17 Ländern

SOPHOS

Einleitung

Identitäten sind der Perimeter der Cybersecurity. Dieser Perimeter weitet sich immer weiter aus, da KI-Systeme kontinuierlich und immer umfassender über E-Mail, Dateien, SaaS-Anwendungen sowie menschliche und nicht-menschliche Identitäten auf Geschäftsdaten zugreifen. Dadurch werden immer mehr sensible Informationen offengelegt, da diese nun leichter zugänglich und leichter zu verbreiten sind.

Da Unternehmen Cloud-Lösungen, Remote-Arbeit und Anwendungen und Services, die auf Maschine-zu-Maschine-Verbindungen basieren, immer mehr und schneller einsetzen, ist die Zahl digitaler Identitäten – sowohl menschlicher als auch nicht-menschlicher Art – explosionsartig angestiegen. Jede Benutzeranmeldeinformation, jeder API-Schlüssel, jedes Servicekonto und jedes OAuth-Token stellt ein potenzielles Einfallstor für Angreifer dar. Dies macht Identitätssicherheit zu einem der kritischsten und anspruchsvollsten Bereiche der modernen Cyberabwehr.

Angreifer haben diesen Wandel erkannt. Gestohlene Zugangsdaten, kompromittierte Servicekonten und Social-Engineering-Angriffe auf Mitarbeiter zählen mittlerweile zu den häufigsten ersten Zugriffsvektoren bei Sicherheitsverletzungen weltweit. Angreifer nutzen KI und Automatisierung, um sich schneller und auf mehr Systemen fortzubewegen. Die Folgen reichen von Datendiebstahl und Erpressung bis hin zu umfassenden Ransomware-Angriffen, die den Geschäftsbetrieb für Tage oder Wochen lahmlegen können.

Um das wahre Ausmaß und die Auswirkungen von identitätsbezogenen Bedrohungen zu verstehen, gab Sophos eine unabhängige Umfrage unter 5.000 IT- und Cybersicherheitsverantwortlichen in 17 Ländern in Auftrag. Im Rahmen dieser Umfrage sollten deren Erfahrungen und Auswirkungen in puncto Identitätsbedrohungen im Jahr 2025 ermittelt werden. In diesem Report werden die Ergebnisse präsentiert. Darüber hinaus werden die Häufigkeit von Identitätsangriffen, die Fähigkeit von Unternehmen, diese zu erkennen und zu stoppen, die daraus resultierenden Konsequenzen, die Hauptursachen erfolgreicher Angriffe, die finanziellen Kosten und der Stand der Einhaltung von Sicherheitsvorgaben untersucht.

Die Ergebnisse zeichnen ein düsteres Bild: Identitätsbedrohungen sind allgegenwärtig, haben weitreichende Folgen und sind eng mit Ransomware verknüpft. Unternehmen, die nicht in Identitätssicherheit investieren, setzen sich einem erheblichen Risiko für ihren Betrieb, ihre Finanzen und ihren Ruf aus.

5.000

IT- und Security-Verantwortliche aus 17 ändern nahmen an einer herstellerunabhängigen globalen Umfrage teil

Wichtigste Erkenntnisse auf einen Blick

- **71 % der Unternehmen waren in den letzten 12 Monaten von mindestens einer identitätsbezogenen Sicherheitsverletzung** betroffen, mit durchschnittlich 3 Angriffen pro betroffenem Unternehmen.
- **14 % der betroffenen Unternehmen waren nicht in der Lage, den bedeutendsten Identitätsangriff zu erkennen und zu stoppen,** bevor Schaden entstand.
- **Die durchschnittlichen Kosten für die Behebung eines Identitätsangriffs beliefen sich auf 1,64 Millionen $.** Der Medianwert liegt bei 750.000 $.
- **Datendiebstahl (49 %) und Ransomware (48 %) waren die häufigsten Folgen** von erfolgreichen Identitätsangriffen.
- **Zwei Drittel der von Ransomware betroffenen Unternehmen (67 %) gaben an, dass der Ransomware-Vorfall auch der bedeutendste Identitätsangriff war.** So wird ein klarer Weg von der Identität zur Ransomware erkennbar.
- **Mangelhaftes Management nicht-menschlicher Identitäten (NHIs) wurde in 41 % der Identitätsangriffe angeführt.** Damit ist es nach menschlichen Fehlern (43 %) die zweithäufigste Einzelursache.
- **Unternehmen mit schwachem Management nicht-menschlicher Identitäten sind mit 22 % höherer Wahrscheinlichkeit von Finanzdiebstahl und mit 24 % höherer Wahrscheinlichkeit von Erpressung betroffen.** Sie geben Wiederherstellungskosten von insgesamt fast 150.000 $ über dem Durchschnitt an.
- **Lediglich jedes dritte Unternehmen (34 %) rotiert oder prüft regelmäßig Servicekonten und nicht-menschliche Identitäten.** Nur 11 % tun dies kontinuierlich – wodurch Sicherheitslücken entstehen, die Angreifer ausnutzen können.
- **Nur 24 % der Unternehmen prüfen kontinuierlich auf ungewöhnliche Anmeldeversuche** und mehr als die Hälfte überprüft alles alle drei Monate oder seltener.
- **Am häufigsten waren Energie-, Öl-/Gas- und Versorgungsunternehmen (80 %) sowie Bundesbehörden (78 %) von Identitätsangriffen betroffen.** Die niedrigsten Werte wiesen hingegen die Bereiche IT, Technologie und Telekommunikation (63 %) sowie das Gesundheitswesen (63 %) auf.
- **Bei kleineren Unternehmen (100–250 Mitarbeiter) war die Wahrscheinlichkeit, Identitätsangriffe zu erkennen, 72 % geringer** im Vergleich zu Unternehmen mit 1.001–3.000 Mitarbeitern (19 % vs. 11 %).

Detaillierte Ergebnisse

Häufigkeit von Identitätsangriffen

Die Umfrage zeigt, dass identitätsbezogene Angriffe keine Randerscheinung sind, sondern die Regel. Mehr als sieben von zehn Organisationen (70,9 %) waren in den letzten 12 Monaten von mindestens einer identitätsbezogenen Sicherheitsverletzung betroffen. Lediglich 22,6 % gaben definitiv an, keine Sicherheitsverletzung erlebt zu haben, während 6,4 % einräumten, dass Verletzungen möglicherweise ohne ihr Wissen stattgefunden haben.

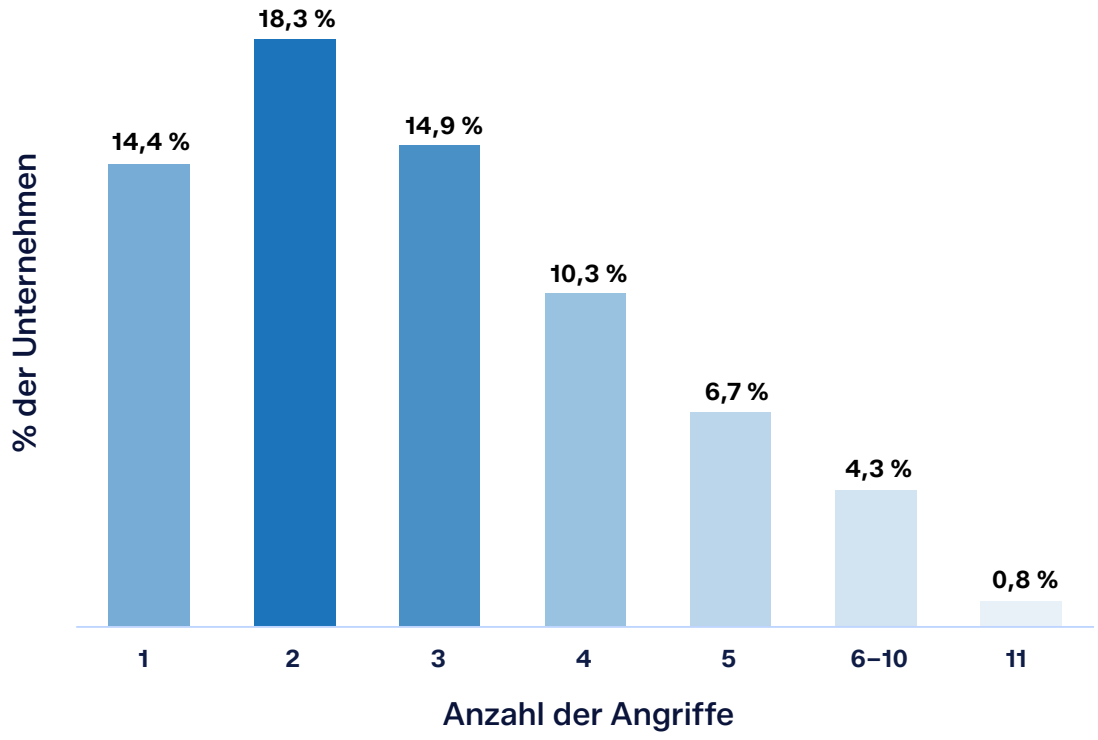
Bei den betroffenen Unternehmen lag die durchschnittliche Anzahl der Vorfälle bei 3,1, was darauf hindeutet, dass Identitätsangriffe selten einmalige Ereignisse sind. 5 % der Befragten berichteten von sechs oder mehr Angriffen im vergangenen Jahr.

67 %

aller Vorfälle, die im Jahr 2025 von Sophos Incident Response und Sophos MDR untersucht wurden, hatten ihren Ursprung in identitätsbasierten Angriffen.

Sophos X-Ops Insight

Häufigkeitsverteilung von Angriffen



War Ihr Unternehmen in den letzten 12 Monaten von identitätsbezogenen Sicherheitsvorfällen betroffen? Falls ja, wie viele? n=5.000

Ein Blick auf einzelne Länder

Bei der Angriffsrate pro Land gibt es große geografische Unterschiede. Die Schweiz (88,7 %) verzeichnete die höchste Rate, 18 Prozentpunkte über dem globalen Durchschnitt, gefolgt von Mexiko (83,3 %) und Italien (80,0 %). Deutschland (62,6 %), Kolumbien (62,7 %) und Japan (64,7 %) waren am seltensten betroffen, wobei selbst die niedrigsten Werte über 60 % lagen.

Land	Angriffsrate	im Vergleich zu Weltweit (70,9 %)
Schweiz	88,7 %	+17,8 Prozentpunkte
Mexiko	83,3 %	+12,4 Prozentpunkte
Italien	80,0 %	+9,1 Prozentpunkte
Australien	79,7 %	+8,8 Prozentpunkte
Indien	76,8 %	+5,9 Prozentpunkte
Südafrika	75,0 %	+4,1 Prozentpunkte
Brasilien	74,0 %	+3,1 Prozentpunkte
VAE	73,3 %	+2,4 Prozentpunkte
Singapur	72,0 %	+1,1 Prozentpunkte
Spanien	70,0 %	-0,9 Prozentpunkte
Chile	66,7 %	-4,2 Prozentpunkte
USA	66,1 %	-4,8 Prozentpunkte
Frankreich	66,0 %	-4,9 Prozentpunkte
UK	65,3 %	-5,6 Prozentpunkte
Japan	64,7 %	-6,2 Prozentpunkte
Kolumbien	62,7 %	-8,2 Prozentpunkte
Deutschland	62,6 %	-8,3 Prozentpunkte

War Ihr Unternehmen in den letzten 12 Monaten von identitätsbezogenen Sicherheitsvorfällen betroffen? Falls ja, wie viele? n=5.000.

Ein Blick auf die Branchen

Bei einem Blick auf die Daten je nach Branche wiesen die Bereiche Energie, Öl/Gas und Versorgungsunternehmen (80,3 %) sowie Bundesbehörden (78,4 %) die höchste Angriffsrate auf. Am wenigsten betroffen waren die Bereiche IT/Technologie/Telekommunikation (63,1 %) und Gesundheitswesen (63,4 %), was möglicherweise darauf zurückzuführen ist, dass es in diesen Sektoren einen höheren Reifegrad in puncto Sicherheitsinvestitionen gibt.

Branche	Angriffsrate
Energie, Öl/Gas und Versorgungsunternehmen	**80,3 %**
Bundesbehörden	78,4 %
Bauwesen und Immobilien	76,1 %
Fertigung und Produktion	73,6 %
Einzelhandel	72,0 %
Grund- und weiterführende Schulen	71,1 %
Finanzdienstleistungen	71,0 %
Medien, Freizeit & Unterhaltung	70,9 %
Behörden auf Landes- und Kommunalebene	69,6 %
Vertrieb und Transport	67,6 %
Hochschulen	65,9 %
Unternehmens- & Fachdienstleistungen	64,5 %
Gesundheitswesen	63,4 %
IT, Technologie & Telekommunikation	63,1 %

War Ihr Unternehmen in den letzten 12 Monaten von identitätsbezogenen Sicherheitsvorfällen betroffen? Falls ja, wie viele? n=5.000.

Compliance als Indikator

Bei Unternehmen, die die Einhaltung von Compliance-Anforderungen als „sehr schwierig" bezeichneten, lag die Anzahl der Angriffe bei 82,4 %, ganze 14 Prozentpunkte höher als bei denjenigen, die Compliance als ein wenig oder gar nicht schwierig empfanden (68,3 %). Dies lässt darauf schließen, dass Probleme bei der Compliance ein früher Indikator für umfassendere Sicherheitsschwächen sind.

Grundlagen der Identitätssicherheit

Unternehmen müssen vier Identitätstypen verwalten

Jedes Unternehmen gewährt Zugriff auf unterschiedliche Arten von Identitäten. Jede dieser Optionen birgt ihre eigenen Risiken.

Kategorie 1 – Mitarbeiteridentitäten

Personen innerhalb der Organisation, die für die Ausübung ihrer Tätigkeit Zugriff auf Systeme und Daten benötigen.

- Mitarbeiter
- Auftragnehmer
- IT- und Informationssicherheitsadministratoren (Personen, deren Rolle einen erweiterten Systemzugriff erfordert)
- Führungskräfte (Personen, deren Rolle sie für einen Angreifer besonders wertvoll macht)

Kategorie 2 – Externe Identitäten

Personen außerhalb des Unternehmens, denen vorübergehend oder dauerhaft Zugang gewährt wird, um eine bestimmte und definierte Rolle oder Aufgabe zu erfüllen.

- Partner
- Zulieferer
- Kunden

Kategorie 3 – Nicht-menschliche Identitäten (NHIs)

Software, Systeme und automatisierte Prozesse, denen Zugriff gewährt wird, um Aufgaben ohne menschliches Eingreifen auszuführen.

- Servicekonten (z. B. geplante Backups)
- API-Schlüssel (z. B. für App-Integrationen)
- KI-Agenten (z. B. autonome Aufgaben)
- IoT-Geräte (z. B. Sensoren, Kameras)

Kategorie 4 – Privilegierte Identitäten (höchstes Risiko)

Jede Identität – sowohl menschlich als auch nicht-menschlich – mit erweiterten Berechtigungen, die einen tiefgreifenden Zugriff auf sensible Systeme und Daten ermöglichen.

- Super-Administratoren (d. h. Personen mit voller Systemkontrolle)
- Root-Konten (z. B. Cloud-Administratorzugriff)
- Gemeinsame Konten (z. B. Team-Logins)
- Notfallzugang (z. B. Notfallkonten)

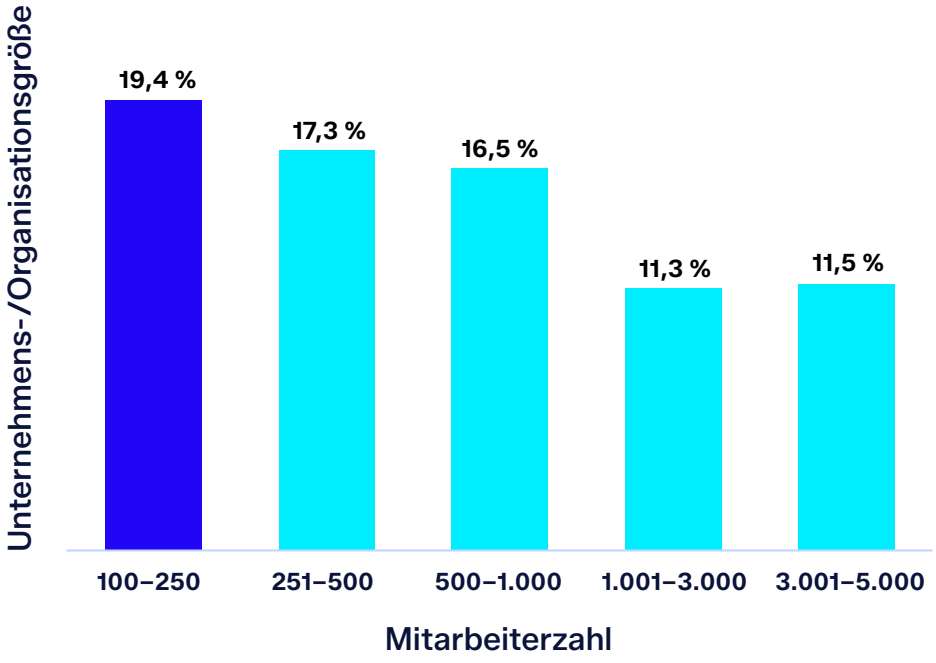
Jede Identität ist ein potenzieller Einstiegspunkt Zu den wichtigsten Maßnahmen, die ein Unternehmen für Sicherheit ergreifen kann, gehört zum einen die Kontrolle darüber, wer und was Zugriff auf Ihre Systeme hat. Unternehmen sollten zum anderen sicherstellen, dass dieser Zugriff angemessen ist und überwacht wird.

Kann das Unternehmen Identitätsangriffe erkennen und stoppen?

Von den 3.545 Befragten, die im Jahr 2025 von einem identitätsbezogenen Angriff betroffen waren, konnten 85,4 % den schwerwiegendsten Angriff erkennen und stoppen, bevor Schaden entstand. Dies zeigt zwar, dass für die Mehrheit eine Erkennung durchaus möglich ist. Für die 14,4 %, die den Angriff nicht stoppen konnten, stellt dieser jedoch ein erhebliches Risiko mit schwerwiegenden Folgen dar, wie spätere Erkenntnisse zeigen werden.

Erkennung aufgrund der Unternehmensgröße schwierig

Kleinere Unternehmen erkannten Angriffe deutlich seltener. Bei den kleinsten befragten Unternehmen (100–250 Mitarbeiter) konnten 19,4 % den Angriff nicht stoppen. Das ist fast doppelt so viel wie bei Unternehmen mit 1.001–3.000 Mitarbeitern (11,3 %). Diese Diskrepanz verdeutlicht die Ressourcen- und Kapazitätsherausforderungen, mit denen kleinere Unternehmen konfrontiert sind.



Wenn Sie an den bedeutendsten Identitätsangriff denken, von dem Ihr Unternehmen in den letzten 12 Monaten betroffen war: Konnten Sie den Identitätsangriff erkennen und stoppen, bevor Schaden entstanden ist? Basis: Bei dem Unternehmen kam es zu einem identitätsbezogenen Sicherheitsvorfall. n=3.545.

Mangelnde Erkennung nach Land

Brasilien (21,6 %) und die Schweiz (21,1 %) wiesen die höchsten Fehlerraten bei der Erkennung auf, während Großbritannien (7,1 %) und Mexiko (9,6 %) am besten abschnitten. Insbesondere die hohe Angriffsrate in der Schweiz in Verbindung mit einer hohen Fehlerrate bei der Erkennung macht sie zu einem besonders gefährdeten Markt.

Land	Nicht erkannt
Brasilien	**21,6 %**
Schweiz	21,1 %
Japan	19,6 %
Spanien	18,1 %
Chile	18,0 %
Singapur	17,6 %
Deutschland	17,4 %
Frankreich	14,6 %
Italien	14,6 %
Australien	13,8 %
Kolumbien	13,8 %
USA	12,8 %
VAE	11,8 %
Indien	11,2 %
Südafrika	10,7 %
Mexiko	9,8 %
UK	7,1 %

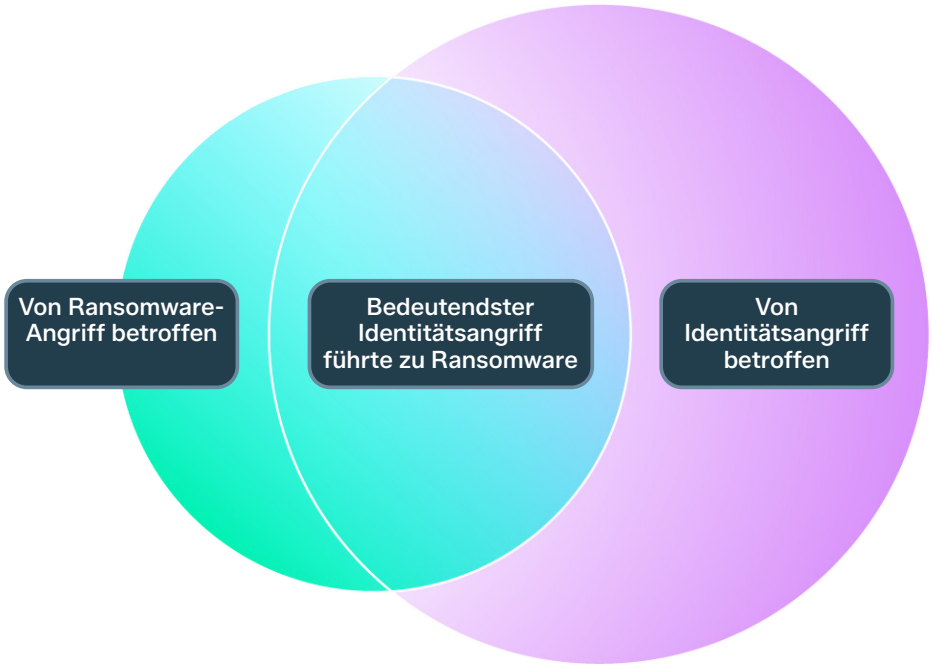
Wenn Sie an den bedeutendsten Identitätsangriff denken, von dem Ihr Unternehmen in den letzten 12 Monaten betroffen war: Konnten Sie den Identitätsangriff erkennen und stoppen, bevor Schaden entstanden ist? Basis: Bei dem Unternehmen kam es zu einem identitätsbezogenen Sicherheitsvorfall. n=3.545.

Mangelnde Erkennung nach Branche

Der Bereich Medien, Freizeit und Unterhaltung (22,4 %) wies die höchste Fehlerrate bei der Erkennung auf, gefolgt vom verarbeitenden Gewerbe (18,4 %) und dem Finanzdienstleistungssektor (17,9 %). Der Gesundheitssektor (8,1 %) schnitt bei der Erkennung am besten ab, was möglicherweise auf den regulatorischen Druck zurückzuführen ist, in Bedrohungsüberwachung zu investieren.

Verbindung zwischen Identität und Ransomware

Eines der auffälligsten Ergebnisse dieser Studie ist der direkte Zusammenhang zwischen Identitätsangriffen und Ransomware. Von den Unternehmen, die im Jahr 2025 von Ransomware betroffen waren, bestätigten zwei Drittel (66,5 %), dass es sich bei dem Ransomware-Vorfall um dasselbe Ereignis handelte wie bei ihrem bedeutendsten Identitätsangriff. Obwohl nicht alle Angriffe zu einer Datenverschlüsselung führten, belegt dies, dass die Kompromittierung der Identität ein zentrales Einfallstor zur Verbreitung von Ransomware ist.



War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? (n=5.000). War Ihr Unternehmen in den letzten 12 Monaten von identitätsbezogenen Sicherheitsvorfällen betroffen? Falls ja, wie viele? (n=5.000) [Falls beides zutrifft] Entsprach dieser Ransomware-Vorfall Ihrem bedeutendsten identitätsbezogenen Angriff?

Verbindung zwischen Ransomware und Identität nach Unternehmensgröße

Die Verbindung zwischen Identität und Ransomware war am stärksten in Unternehmen mit 1.001 bis 3.000 Mitarbeitern (71,6 %) und am schwächsten in solchen mit 100 bis 250 Mitarbeitern (62,4 %). Die Abweichungen könnten auf unterschiedlich komplexe Unternehmensinfrastrukturen, den Grad der Transparenz oder darauf zurückzuführen sein, ob der Angriffsvektor in den verschiedenen Segmenten mit dem Zielergebnis in Zusammenhang gebracht werden kann.

Unternehmensgröße	Ransomware = Identitätsangriff
100–250 Mitarbeiter	62,4 %
251–500 Mitarbeiter	68,2 %
501–1.000 Mitarbeiter	62,5 %
1.001–3.000 Mitarbeiter	**71,6 %**
3.001–5.000 Mitarbeiter	64,6 %

War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? (n=5.000). War Ihr Unternehmen in den letzten 12 Monaten von identitätsbezogenen Sicherheitsvorfällen betroffen? Falls ja, wie viele? (n=5.000) [Falls beides zutrifft] Entsprach dieser Ransomware-Vorfall Ihrem bedeutendsten identitätsbezogenen Angriff?

Brancheneinblicke

Die stärkste Verbindung zwischen Ransomware und Identität bestand im Hochschulwesen (76,8 %) und im Bereich Vertrieb/Transport (75,0 %), während die Werte im Finanzdienstleistungssektor (57,6 %) und im IT-, Technologie- und Telekommunikationssektor (61,1 %) niedriger lagen (wenn auch immer noch deutlich über der Mehrheitsschwelle).

Folgen unentdeckter Identitätsangriffe

Für die 510 Unternehmen, die den bedeutendsten Identitätsangriff nicht verhindern konnten, waren die Auswirkungen schwerwiegend und vielschichtig; die betroffenen Unternehmen berichteten im Durchschnitt von zwei Folgen des Vorfalls.

Auswirkung	Prozentsatz der betroffenen Unternehmen
Datendiebstahl – Angreifer stahlen sensible Daten	**48,8 %**
Ransomware – gestohlene Zugangsdaten, die zur Durchführung des Ransomware-Angriffs verwendet werden	48,4 %
Erpressung – Angreifer forderten Geld	43,9 %
Sabotage – Angreifer nutzten Zugangsdaten, um das Unternehmen zu schädigen	30,0 %
Finanzdiebstahl – umgeleitete Zahlungen	28,0 %
Finanzdiebstahl – Geld von Konten gestohlen	25,5 %
Zusammenfassung: Finanzdiebstahl (jeglicher Art)	**46,7 %**

Welche Folgen hatte dieser Identitätsangriff für Ihr Unternehmen? Basis: Das Unternehmen konnte die Sicherheitsverletzung nicht verhindern. n=510.

Bei fast der Hälfte der betroffenen Unternehmen kam es zu Datendiebstahl (48,8 %), und ein nahezu gleich großer Anteil erlebte einen Ransomware-Angriff (48,4 %). Fast die Hälfte (46,7 %) war von irgendeiner Form direkten finanziellen Diebstahls betroffen (umgeleitete Zahlungen, gestohlenes Geld oder beides). Zusammen mit Erpressung (43,9 %) verdeutlichen diese Ergebnisse, dass unentdeckte Identitätsangriffe fast immer zu schwerwiegenden Folgen führen.

Warum Unternehmen betroffen waren

Um Angriffe abwehren zu können, ist es unerlässlich zu verstehen, warum sie Erfolg hatten. Bei der Umfrage kristallisierte sich eine Mischung aus menschlichen, prozessbedingten und technischen Fehlern heraus, die dazu führten, dass Unternehmen von identitätsbasierten Angriffen betroffen waren. Darüber hinaus zeigt sich, dass es selten nur einen einzigen Grund gibt; die Befragten nennen im Durchschnitt zwei Hauptursachen, die zu dem Vorfall beigetragen haben.

Hauptursache	Prozentsatz der betroffenen Unternehmen
Menschliche Fehler – Mitarbeiter wurde zur Herausgabe von Zugangsdaten verleitet	**42,7 %**
Schwaches Management nicht-menschlicher Identitäten (z. B. im Code gespeicherte API-Schlüssel, statische Zugangsdaten, verwaiste Servicekonten, die zuvor Anwendungen mit Systemen verbunden waren, usw.).	40,6 %
Schwaches Management menschlicher Identitäten für Mitarbeiter	38,6 %
Mangelnde Transparenz hinsichtlich der Zugriffsrechte und Berechtigungen, die externen Anwendungen gewährt werden	35,7 %
Schwaches Management menschlicher Identitäten für Lieferanten/Auftragnehmer	31,4 %
Mangelnde Kontrolle über Zugriffsrechte und Berechtigungen, die externen Anwendungen gewährt werden	30,8 %
Böswilliger Insider – Mitarbeiter ermöglichte Angriff absichtlich	26,7 %
Zusammenfassung: Schwaches Management menschlicher Identitäten (jeglicher Art)	**60,2 %**
Zusammenfassung: Probleme mit dem Zugriff und den Berechtigungen, die externen Anwendungen gewährt wurden (jeglicher Art)	**56,1 %**

Warum war Ihr Unternehmen von dem identitätsbezogenen Angriff betroffen? Wählen Sie alle zutreffenden Antworten aus.
Basis: Das Unternehmen konnte die Sicherheitsverletzung nicht verhindern. n=510.

Menschliche Fehler waren mit 42,7 % der Nennungen der häufigste Einzelfaktor bei Identitätsangriffen. An zweiter Stelle steht das schwache Management nicht-menschlicher Identitäten (40,6 %), was besonders besorgniserregend ist, da es im Code gespeicherte API-Schlüssel, statische Zugangsdaten und verwaiste Servicekonten umfasst, die schwieriger zu prüfen und zu überwachen sind.

Bei über einem Viertel (26,7 %) der Angriffe wurde böswillige Insideraktivität festgestellt, bei der Mitarbeiter den Angriff absichtlich ermöglichten. Dies unterstreicht die Bedeutung von strengen internen Kontrollen und Wachsamkeit.

Insgesamt ist ein mangelhaftes Management menschlicher Identitäten (60,2 %) der häufigste Grund dafür, dass Unternehmen von identitätsbasierten Angriffen betroffen waren, während Probleme mit dem Zugriff und den Berechtigungen externer Anwendungen in 56,1 % der Vorfälle eine Rolle spielten.

59,5 %

MFA – eine jahrzehntealte Technologie – war in 59,5 % der MDR Fälle, die für den Sophos Active Adversary Report 2025 analysiert wurden, auf dem Zielsystem nicht verfügbar.

Sophos X-Ops Insight

Ein Blick auf die Unternehmensgröße

Größere Unternehmen haben in mehreren Bereichen der Identitätsüberwachung größere Schwierigkeiten als kleinere, was wahrscheinlich auf die umfangreichere Größe und Komplexität der Umgebungen zurückzuführen ist, die sie einsehen und sichern müssen.

Mehr als die Hälfte (55,6 %) der Unternehmen mit 1.001 bis 3.000 Mitarbeitern gaben menschliche Fehler als Hauptursache an, verglichen mit nur 29,0 % der Unternehmen mit 251 bis 500 Mitarbeitern. In ähnlicher Weise gaben 68,6 % der Unternehmen mit 3.001 bis 5.000 Mitarbeitern an, dass ein schwaches Management menschlicher Identitäten dazu beigetragen habe, dass sie von Angriffen betroffen waren, verglichen mit 58,5 % derjenigen mit 100 bis 250 Mitarbeitern.

Was sind nicht-menschliche Identitäten?

Eine nicht-menschliche Identität (NHI) ist eine digitale Berechtigung, die einer Software, einem System oder einem automatisierten Prozess gewährt wird, damit diese(r) ohne menschliches Eingreifen auf Ressourcen zugreifen kann. Anstelle von Passwörtern verwenden NHIs nicht-menschliche Zugangsdaten, um ihre Identität nachzuweisen, darunter:

- API-Schlüssel zur Verbindung von Anwendungen
- Servicekonten, die Backups ausführen
- OAuth-Token für SaaS-Integrationen
- KI-Agenten, die auf Datenbanken zugreifen

NHI-Zugangsdaten können auf ähnliche Weise gestohlen und missbraucht werden wie menschliche Anmeldedaten. Dies gestaltet sich umso problematischer, wenn Unternehmen die NHI-Berechtigungen, die sehr oft umfassend und bedeutend sind, nicht regelmäßig überprüfen.

NHIs sind deutlich zahlreicher als menschliche Identitäten vorhanden; bei manchen Unternehmen liegt das Verhältnis bei über 100:1. Agentische KI ist ein wichtiger Treiber dieses Anstiegs in den letzten Jahren.

In 96 %

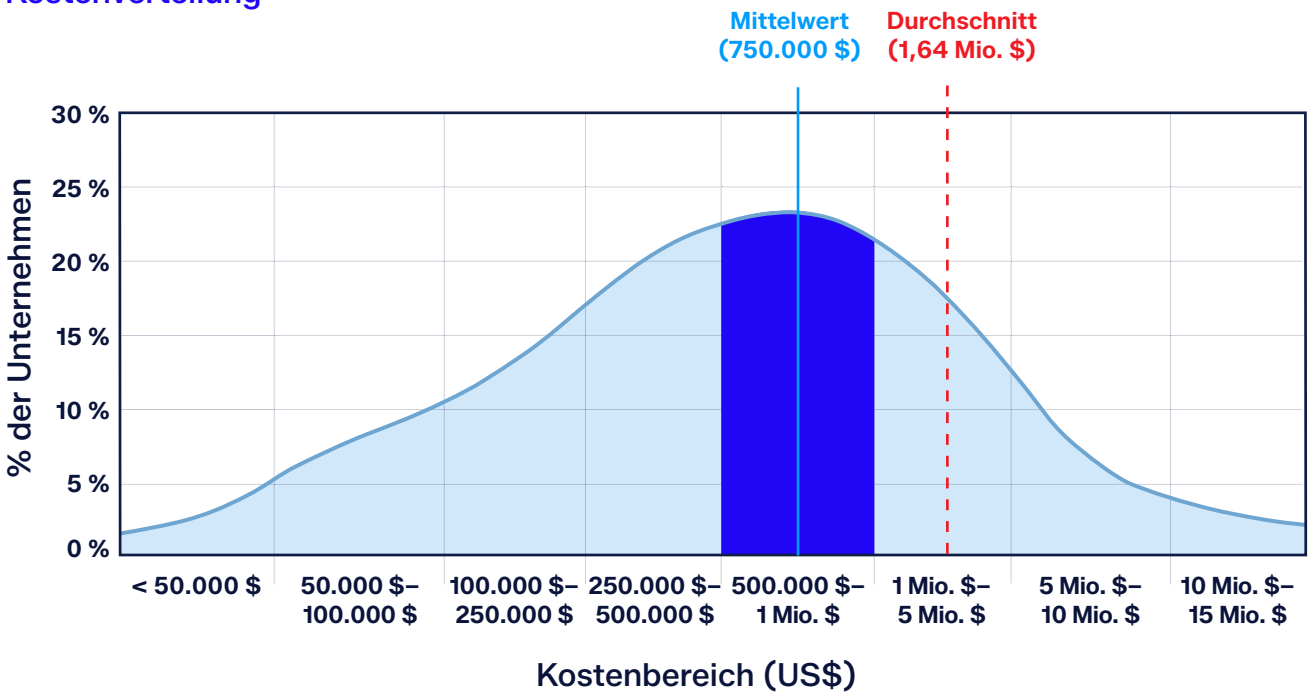
der ITDR-Kundenumgebungen von Sophos sind Multi-Tenant-Anwendungen vorhanden. Die Prüfung oder auch nur die Auflistung der an diesen Beziehungen beteiligten NHIs kann schwierig sein.

Sophos X-Ops Insight

Die finanziellen Folgen von Identitätsangriffen

Unternehmen, bei denen ein Identitätsangriff erfolgreich war, hatten erhebliche Wiederherstellungskosten. Die durchschnittlichen Wiederherstellungskosten weltweit beliefen sich auf 1.637.363 $, der Median lag bei 750.000 $. 73 % der betroffenen Unternehmen schätzten die Kosten auf 250.000 $ oder mehr, und fast ein Viertel (23,7 %) lag im Bereich von 500.000 bis 1 Million $.

Kostenverteilung



Wie hoch schätzen Sie die Gesamtkosten für Ihr Unternehmen ein, die durch die Behebung des Identitätsangriffs entstehen?
Basis: Das Unternehmen konnte die Sicherheitsverletzung nicht verhindern. n=510.

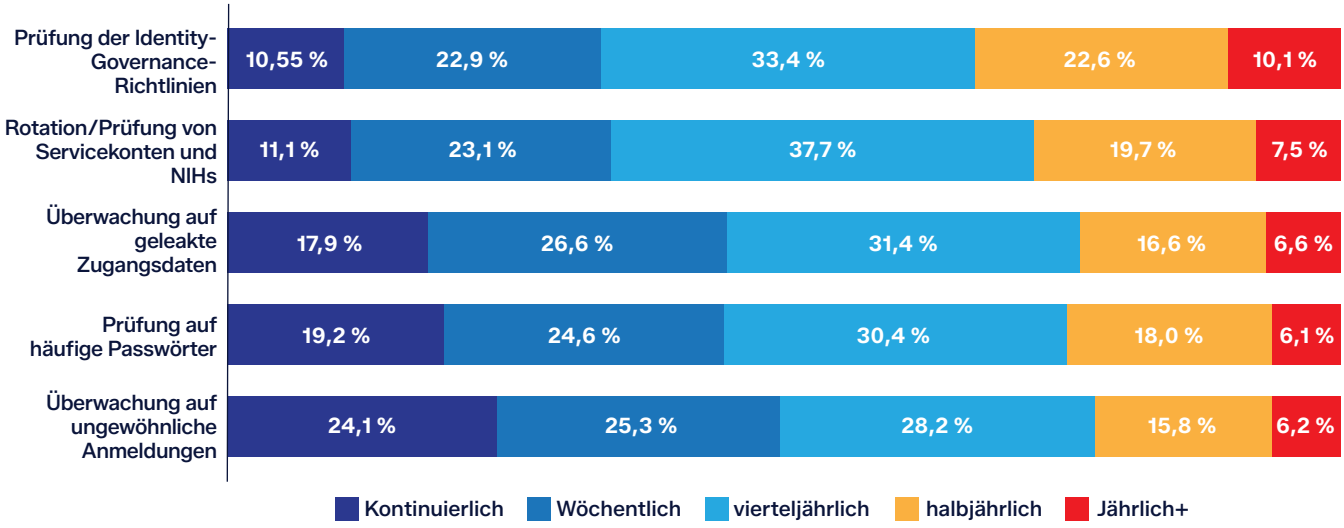
Kosten nach Unternehmensgröße

Unternehmensgröße	Mittlere Kosten	Durchschnittliche Kosten
100–250 Mitarbeiter	1.125.562 $	375.000 US$
251–500 Mitarbeiter	1.978.043 $	750.000 US$
501–1.000 Mitarbeiter	1.009.205 $	375.000 US$
1.001–3.000 Mitarbeiter	1.907.594 $	750.000 US$
3.001–5.000 Mitarbeiter	2.452.929 $	750.000 US$

Wie hoch schätzen Sie die Gesamtkosten für Ihr Unternehmen ein, die durch die Behebung des Identitätsangriffs entstehen?
Basis: Das Unternehmen konnte die Sicherheitsverletzung nicht verhindern. n=510.

Einhaltung der Sicherheitsvorgaben für Identitätssicherheit

In der Studie wurden fünf zentrale Aktivitäten im Bereich Identitätsmanagement untersucht und es wurde geprüft, wie häufig Unternehmen diese durchführen. Die Ergebnisse zeigen erhebliche Diskrepanzen zwischen Best Practices und der Realität auf – Diskrepanzen, die die Anfälligkeit für Identitätsangriffe erhöhen.



Wie häufig führt Ihr Unternehmen die folgenden Aktivitäten im Bereich Identitätsmanagement durch? n=5.000

Die Überwachung ungewöhnlicher Anmeldeversuche ist die am häufigsten in Echtzeit durchgeführte Aktivität (24,1 %, kontinuierlich), doch selbst hier überprüft mehr als die Hälfte der Unternehmen (50,6 %) nicht häufiger als alle drei Monate. Eine Rotation oder Überprüfung nicht-menschlicher Identitäten – eine kritische Aktivität, da dies die zweithäufigste individuelle Ursache für Sicherheitsverletzungen ist – führen nur 34,3 % dies wöchentlich oder häufiger durch.

Die Überprüfung von Identity-Governance-Richtlinien wird am seltensten auf kontinuierlicher Basis durchgeführt (10,5 %). Ein Drittel der Unternehmen (33,3 %) überprüft Richtlinien höchstens vierteljährlich und 22,6 % nur alle sechs Monate. Angesichts der Tatsache, dass sich Identitätsbedrohungen rasant weiterentwickeln, lassen jährliche, halbjährliche oder gar vierteljährliche Überprüfungen gefährliche Lücken entstehen.

Agentische KI: Beschleunigung des NHI-Problems

Agentische KI hat das NHI-Management exponentiell erschwert: mehr Identitäten, die schneller erstellt werden, mit breiterem Zugriff und weit weniger menschlicher Aufsicht. Zu den größten Herausforderungen bei NHIs gehören:

- **KI-Agenten vervielfachen NHIs automatisch**
  Jeder KI-Agent benötigt eine eigene Identität und eigene Zugangsdaten. Entscheidend ist, dass Agenten autonom neue Agenten starten können, um Teilaufgaben zu erledigen, wobei jeder Agent ohne menschliches Eingreifen oder Aufsicht weitere Zugangsdaten erzeugt.
- **KI-Agenten benötigen umfassenden und dauerhaften Zugriff**
  Um ihre Aufgaben zu erfüllen, müssen KI-Agenten auf viele Systeme zugreifen können: Kalender, Datenbanken, CRM-Systeme, Dateispeicher und APIs. Im Gegensatz zu menschlichen Konten laufen diese Zugriffsrechte nur selten ab und werden nur selten überprüft.
- **KI-Agenten sind schwieriger zu überwachen als traditionelle NHIs**
  Ein Backup-Servicekonto führt jede Nacht zur gleichen Zeit die gleiche Aufgabe aus, was die Überwachung erleichtert. KI-Agenten hingegen treffen autonome Entscheidungen, handeln unvorhersehbar und sind rund um die Uhr im Einsatz, sodass es sehr schwierig ist, zu erkennen, dass etwas schiefgelaufen ist.
- **KI-Agenten von Drittanbietern übernehmen unbekannte Risiken**
  Wenn Unternehmen die Funktionen von KI-Agenten von Drittanbietern nutzen, übernehmen sie laut Forschungsergebnissen alle Zugangsdaten und Zugriffsberechtigungen dieser Agenten, allerdings mit begrenzter Transparenz darüber, wie sicher diese erstellt wurden oder worauf sie zugreifen können.
- **Sicherheitsregeln wurden nicht für KI-Agenten geschrieben**
  Die meisten Frameworks für Identitätssicherheit wurden für menschliche Benutzer und einfache Maschinen entwickelt. Sie berücksichtigen keine Agenten, die selbstständig eigene Zugangsdaten während eines Workflows erstellen, delegieren und außer Kraft setzen können, wodurch eine erhebliche Governance-Lücke entsteht.

Agentische KI ist ein wesentlicher Grund dafür, dass die Sicherheit von NHIs ganz oben auf die Agenda der CISOs gerückt ist.

Folgen eines schwachen Managements nicht-menschlicher Identitäten

Wie bereits erwähnt, war ein mangelhaftes Management nicht-menschlicher Identitäten (NHI) in 40,6 % der Fälle eine Hauptursache für erfolgreich durchgeführte Angriffe. Eine genauere Analyse der Daten zeigt, dass kompromittierte NHIs die finanziellen Folgen des Angriffs drastisch verschärfen.

Besonders auffällig ist, dass Unternehmen mit schwachem NHI-Management mit +27,9 % über dem Durchschnitt deutlich anfälliger für Finanzdiebstahl (bei dem Angreifer Zahlungen von Konten umleiten) und mit +24,4 % über dem Durchschnitt deutlich anfälliger für Erpressung (bei der Angreifer Geld fordern) sind. Die einzigen Kategorien, in denen Unternehmen mit schwachem NHI-Management etwas besser als der Durchschnitt abschnitten, waren Datendiebstahl und Ransomware, wobei diese Unterschiede jedoch marginal sind.

Auswirkung	% aller betroffenen Unternehmen	% der betroffenen Unternehmen mit schwachem Management nicht-menschlicher Identitäten	Prozentuale Veränderung bei schwachem Management nicht-menschlicher Identitäten
Datendiebstahl – Angreifer stahlen sensible Daten	48,8 %	47,8 %	-2,1 %
Ransomware – gestohlene Zugangsdaten, die zur Durchführung des Ransomware-Angriffs verwendet werden	48,4 %	46,4 %	-4,1 %
Erpressung – Angreifer forderten Geld	43,9 %	**54,6 %**	**+24,4 %**
Sabotage – Angreifer nutzten Zugangsdaten, um das Unternehmen zu schädigen	30,0 %	33,8 %	+12,7 %
Finanzdiebstahl – umgeleitete Zahlungen	28,0 %	**35,8 %**	**+27,9 %**
Finanzdiebstahl – Geld von Konten gestohlen	25,5 %	29,9 %	+15,7 %
Zusammenfassung: Finanzdiebstahl (jeglicher Art)	**46,7 %**	**57,0 %**	**+22 %**

Welche Folgen hatte dieser Identitätsangriff für Ihr Unternehmen? Basis: Das Unternehmen konnte die Sicherheitsverletzung nicht verhindern. n=510 (alle Angriffe), n=207 (Angriffe im Zusammenhang mit NHIs)

Angesichts der zunehmenden finanziellen Auswirkungen schwacher NHIs ist es nicht verwunderlich, dass Unternehmen mit schwachem NHI-Management deutlich höhere Gesamtkosten für die Wiederherstellung nach Identitätsangriffen meldeten, wobei die typischen Kosten fast 150.000 $ über dem Durchschnitt liegen.

Durchschnittliche Kosten für die Wiederherstellung nach Identitätsangriffen

Es besteht ein klarer Zusammenhang zwischen mangelnder Einhaltung der Sicherheitsvorgaben für NHIs und der Wahrscheinlichkeit eines NHI-bedingten Angriffs. Während ein Drittel (34 %) aller Unternehmen ihre Servicekonten und NHIs kontinuierlich oder wöchentlich rotieren oder prüfen, sinkt dieser Anteil bei denjenigen, bei denen der Angriff auf kompromittierte NHIs zurückzuführen ist, auf ein Viertel (24 %).

Fazit

Angesichts der Ergebnisse dieser Umfrage sollten sich Unternehmen nicht auf Erfolgen ausruhen. Im vergangenen Jahr waren mehr als 7 von 10 Unternehmen von Identitätsangriffen betroffen, im Durchschnitt ereigneten sich mehr als drei Vorfälle pro betroffenem Unternehmen. Dies ist also kein theoretisches Risiko oder ein Problem, das auf bestimmte Branchen oder Regionen beschränkt ist. Es handelt sich um eine universelle, allgegenwärtige Bedrohung, die Unternehmen jeder Größe, Branche und Region betrifft. Die Daten zeigen, dass Identitätsangriffe das Einfallstor für Ransomware, Datendiebstahl und Erpressung in Unternehmen darstellen: Bei 67 % der von Ransomware betroffenen Unternehmen war der Vorfall direkt auf einen Identitätsangriff zurückzuführen.

Wenn Identitätsangriffe erfolgreich sind, sind die Auswirkungen schwerwiegend und vielschichtig. Bei fast der Hälfte der betroffenen Unternehmen kam es zu Datendiebstahl oder Ransomware-Angriffen, und die durchschnittlichen Bereinigungskosten von 1,64 Millionen $ machen jeden Vorfall zu einem bedeutenden finanziellen Problem.

Die Hauptursachen weisen auf systemische Schwächen hin: Menschliche Fehler (42,7 %), mangelhaftes Management nicht-menschlicher Identitäten (40,6 %) und unzureichende Transparenz hinsichtlich der Berechtigungen von Drittanbieteranwendungen (35,7 %) sind allesamt behebbar, jedoch nur mit nachhaltigen Investitionen und Aufmerksamkeit. Dass kleinere Unternehmen Angriffe fast doppelt so häufig nicht erkennen wie größere, verdeutlicht eine Lücke in der Cybersecurity, die die Aufmerksamkeit der Sicherheits-Community erfordert.

Am besorgniserregendsten ist wohl der aktuelle Stand bei der Einhaltung von Sicherheitsvorgaben. Nur etwa ein Viertel der Unternehmen überwacht kontinuierlich ungewöhnliche Anmeldeaktivitäten, und weniger als ein Drittel wechselt regelmäßig nicht-menschliche Zugangsdaten aus – genau die Schwachstellen, die Angreifer ausnutzen.

Unternehmen müssen erkennen, dass Identitätssicherheit kein einmaliges Projekt, sondern ein kontinuierlicher operativer Prozess ist. Wer dies erkennt und entsprechend vorgeht, wird weitaus besser gerüstet sein, sich gegen die Bedrohungen zu verteidigen, die das Jahr 2025 geprägt haben und sich im Jahr 2026 und darüber hinaus weiter verschärfen werden.

Empfehlungen

Wie die Umfrage gezeigt hat, ist eine starke Identitätssicherheit wesentlicher Bestandteil einer effektiven Strategie zur Minderung von Cyber-Risiken. Um die Gefahr durch identitätsbasierte Angriffe zu verringern, sollten Unternehmen mehrschichtige Abwehrmaßnahmen sowohl für menschliche als auch für nicht-menschliche Identitäten implementieren. Beginnen Sie mit den wesentlichen Schritten und arbeiten Sie im Rahmen eines kontinuierlichen Verbesserungsprogramms auf die empfohlenen Maßnahmen hin.

Wesentliche Schritte

Menschliche Identitäten

- Erzwingen Sie Multi-Faktor-Authentifizierung (MFA) für alle Benutzerkonten.
- Verwenden Sie unterschiedliche Zugangsdaten für privilegierte und nicht privilegierte Vorgänge.
- Implementieren Sie Kontosperrung und Schutz vor Brute-Force-Angriffen.
- Zentralisieren Sie das Identitätsmanagement mit Single Sign-On (SSO).
- Stellen Sie sicher, dass Ihr Benutzer-Awareness-Training die neuesten Techniken für Phishing und Harvesting von Zugangsdaten berücksichtigt.

Nicht-menschliche Identitäten

- Erstellen Sie ein Inventar aller nicht-menschlichen Identitäten und klassifizieren Sie sie.
- Verwenden Sie kurzlebige Zugangsdaten anstelle von langlebigen Geheimnissen.

Menschliche und nicht-menschliche Identitäten

- Wenden Sie Zugriffsrechte nach dem Prinzip der minimalen Berechtigung an.
- Sichern und verwalten Sie Zugangsdaten ordnungsgemäß.
- Inaktive Identitäten sollten umgehend deaktiviert oder entfernt werden.
- Setzen Sie einen formellen Offboarding-Prozess durch, bei dem der Zugriff auf Arbeitgeberressourcen geprüft und gegebenenfalls deaktiviert wird.
- Sämtliche Authentifizierungsaktivitäten müssen protokolliert und überwacht werden. Die Protokolle sind mindestens 30 Tage lang aufzubewahren.

Empfohlene Schritte

Menschliche Identitäten

- Implementieren Sie Richtlinien für bedingten Zugriff und risikobasierte Richtlinien.
- Setzen Sie Passkeys (entweder Hardware oder Software) als primäre Authentifizierungsmethode ein.
- Bündeln Sie Identitäten mithilfe weithin akzeptierter Identitätsprotokolle wie Security Assertion Markup Language (SAML) oder dem neueren OpenID Connect (OIDC).

Nicht-menschliche Identitäten

- Verwenden Sie Identity Federation für Workloads anstelle von statischen Geheimnissen.
- Führen Sie eine Geheimnismanagementplattform für NHIs im richtigen Umfang ein.
- Aktivieren Sie das Scannen von Geheimnissen auf unterstützten Plattformen (GitHub, GitLab).

Menschliche und nicht-menschliche Identitäten

- Implementieren Sie eine Privileged Access Management-Lösung (PAM).
- Führen Sie ein Zero-Trust-Sicherheitsmodell ein.
- Führen Sie regelmäßige Zugriffsüberprüfungen und erneute Berechtigungszertifizierungen durch.
- Implementieren Sie Funktionen zur Identity Threat Detection and Response (ITDR).
- Segmentieren Sie Netzwerkzugriff nach Identität und Rolle.
- Definieren und testen Sie ein oder mehrere Playbooks zur Identity Incident Response, die sich mit identitätsbezogenen Vorfällen wie den in diesem Report beschriebenen befassen.

Mehr erfahren

Lesen Sie unseren Leitfaden zu Best Practices für Identitätssicherheit.

Methodologie

Diese Umfrage wurde von Vanson Bourne im Auftrag von Sophos im ersten Quartal 2026 durchgeführt. 5.000 IT- und Cybersecurityverantwortliche in 17 Ländern wurden befragt: USA, Brasilien, Chile, Kolumbien, Mexiko, Großbritannien, Frankreich, Deutschland, Italien, Spanien, Schweiz, Australien, Indien, Japan, Singapur, Südafrika und Vereinigte Arabische Emirate. Die Befragten stammten aus Unternehmen mit 100 bis 5.000 Mitarbeitern in 15 Branchen.

SOPHOS

Wenn Sie Ihre Anforderungen an Identitätssicherheit besprechen und erfahren möchten, wie Sophos Ihnen dabei helfen kann, besuchen Sie unsere Website oder sprechen Sie mit einem Berater.

Sales DACH
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2026-05-08 DE (TA) CRE-5312