Insight

Identitätssicherheit: Ein strategischer Leitfaden

Inhaltsverzeichnis

Identitätssicherheit: Strategischer Käuferleitfaden

In modernen Unternehmen stellt jeder Benutzer-Login, jedes Servicekonto und jede Drittanbieter-Verbindung ein potenzielles Risiko dar. Während hybrides Arbeiten, Cloud-Anwendungen und KI das Unter-nehmen neu gestalten, greifen Angreifer zunehmend Identitäten – nicht Firewalls – an. Aus Sicht eines Angreifers: Warum sich mühsam hinein hacken, wenn man einfach eine Identität stehlen und sich ein-loggen kann? Der Schutz digitaler Identitäten ist zu einer der effektivsten Methoden geworden, um Sicherheitsverletzungen zu verhindern, den Zugriff zu kontrollieren und Vertrauen zu bewahren. Tatsächlich ist die Identität zum primären Angriffs-vektor für Unternehmen geworden -

93% der Organisationen erlebten im vergangenen Jahr mindestens **zwei identitätsbezogene Angriffe**.*

Für Sicherheitsverantwortliche bedeutet dies, dass der Schutz von Identitäten nun geschäftskritisch ist. Dieser Leitfaden erklärt zentrale Konzepte der Identity Security – IAM, IGA, PAM, ITDR, Multi-Faktor-Authentifizierung usw. – und erläutert, warum jedes davon für Ihr Unternehmen wichtig ist. Er zeigt zudem auf, wie Insight als führender Lösungsanbieter mit tiefgehenden Microsoft-Partnerschaften dabei helfen kann, ein umfassendes Identity-Security-Programm aufzubauen.

*https://investors.cyberark.com/news/news-details/2024/Report-93-Of-Organizations-Had-Two-or-More-Identity-Related-Breaches-in-the-Past-Year/)

Warum Identitätsicherheit wichtig ist

Moderne Unternehmen sehen sich mit einer Explosion digitaler Identitäten konfrontiert – von Mitarbeitern und Kunden bis hin zu Software-Bots und Cloud-Diensten. Jede Identität stellt einen potenziellen Einstiegspunkt für Angreifer dar, insbesondere da hybrides Arbeiten und Cloud-Nutzung die traditionelle Netzwerkgrenze auflösen. Techniken wie Social Engineering und der Diebstahl von Zugangsdaten zielen nicht nur auf Benutzer, sondern auch auf Maschi-nenkonten und Anwendungsidentitäten. Schwache oder gestohlene Zugangsdaten sind bei der Mehrheit der Sicherheitsverletzungen ein Faktor – was die Dringlichkeit starker Identitätsschutzmaßnahmen unterstreicht.

Schätzungen zufolge sind **86%** der **Sicherheitsverletzungen mit gestohlenen Zugangsdaten** verbunden**

Neben der unmittelbaren Bedrohung durch Sicherheitsverletzungen bergen schlechte Identitätspraktiken weitere Geschäftsrisiken: unbefugter Zugriff auf sensible Daten, Nichteinhaltung gesetzlicher Vorschriften, Betriebsunterbrechungen und Vertrauensverlust bei Kunden. Im Gegensatz dazu ermöglicht ein robustes Identity-Security-Programm die Umsetzung von „Zero Trust"-Prinzipien („never trust, always verify") und stellt sicher, dass nur die richtigen Personen (oder Systeme) unter den richtigen Bedingungen den richtigen Zugriff erhalten. Darüber hinaus verbessert es die Benutzererfahrung, indem es Chaos (mehrfache Logins, manuelle Zugriffsprozesse) durch einen schlanken, sicheren Zugriff ersetzt – so wird Produktivität ermöglicht, ohne die Sicherheit zu opfern. Kurz gesagt: Der Fokus auf Identity Security hilft Organisationen, Risiken zu reduzieren, Compliance-Anforderungen zu erfüllen und das Unternehmen durch sicheren, vertrauenswürdigen Zugriff auf Technologie-Ressourcen zu stärken.

**https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

Die zentralen Säulen der Identitätssicherheit

Um ein Unternehmen zu schützen, muss Identity Security mehrere Bereiche abdecken. Sie ist kein einzelnes Produkt, sondern ein miteinander verbundenes Set an Fähigkeiten, das gemeinsam grundlegende Fragen beantwortet: Wer (oder was) kann auf was, wann und wie zugreifen? Das untenstehende Diagramm zeigt die gesamte Landschaft der Identity-Security-Funktionen – von der Verwaltung von Identitäten und Berechtigungen bis hin zur Bedrohungsüberwachung.

Insight Identity Strategy Framework

Identität & Zugang
Wer kann auf was zugreifen?

Identitäts-grundlagen
- Verzeichnisdienste
- Föderation / B2B
- Bereitstellung und Entzug von Zugriffsrechten (Provisioning & De-Provisioning)
- Kundenidentität / B2C

Autorisierung
einschließlich MFA, phishing-resistenter MFA und passwortloser Authentifizierung

Autorisierung

Single Sign-On

Benutzer-Self-Service

Identitätsverwaltung & Administration (IGA)
Sollten sie weiterhin Zugriff haben?

Identitäts-verwaltung
- Zugriffsüberprüfung & Zertifizierungen
- Compliance-Management
- Auditing (Prüfungen)

Identitäts-Admin
- Workflow Management

Privilegierter Zugriff
- Erkennung privilegierter Konten
- Verwaltung von Zugangsdaten
- Aufzeichnung von Sitzungen
- Verwaltung von Rechteerweiterung & Delegation für privilegierte Zugriffe

Identitätsbedrohungserkennung & -reaktion (ITDR)
Werden wir angegriffen?

Bedrohungs-erkennung
- Anomalieerkennung & Analyse des Benutzer- und Entitätenverhaltens (UEBA)

Bedrohungs-reaktion
- Konto sperren oder Passwortzurücksetzung erzwingen
- erneute Autorisierung oder "Step-up"-Autorisierung erzwingen

Identitäts- und Zugangsmanagement (IAM)

Identitäts- und Zugangsmanagement - Identity and Access Management (IAM) - ist die Grundlage einer Identity-Security-Strategie. Der Schwerpunkt liegt auf der Einrichtung und Verwaltung digitaler Identitäten (für Mitarbeiter, Partner, Kunden und sogar Softwarekonten) sowie auf der Kontrolle ihres Zugriffs auf Ressourcen. IAM umfasst die Erstellung von Benutzeridentitäten in Verzeichnisdiensten, die Bereitstellung von Konten für Anwendungen und Authentifizierungsdienste wie Single Sign-On. Es „legt die Grundlage fest, wer oder was auf welche Ressourcen zugreifen darf" in der Organisation. In der Praxis ermöglichen IAM-Lösungen (wie Microsoft Entra ID, ehemals Azure AD) es Benutzern, sich sicher und bequem anzumelden, Passwortrichtlinien oder passwortlose Anmeldungen durchzusetzen und den Zugriff auf verschiedene Systeme zentral zu verwalten.

Warum es wichtig ist: Eine solide IAM-Basis (Identity and Access Management) stellt sicher, dass nur authentifizierte und autorisierte Benutzer auf sensible Assets zugreifen können und reduziert so das Risiko unbefugter Zugriffe. Zentralisiertes IAM verbessert die Sicherheit und die Benutzererfahrung, indem es die Passwortflut beseitigt und Geschäftsanwendern den benötigten Zugriff ermöglicht (z. B. über Single Sign-On zu Cloud-Anwendungen). Es schafft zudem die Grundlage für die Durchsetzung von Sicherheitsrichtlinien wie Multi-Faktor-Authentifizierung und bedingtem Zugriff im gesamten Unternehmen. Ohne effektives IAM kämpfen Organisationen oft mit uneinheitlichen Zugriffskontrollen und isolierten Identitäten („Silos"), was zu Sicherheitslücken, frustrierten Nutzern und negativen Audit-Ergebnissen führt.

Kurz gesagt: IAM ist entscheidend für Produktivität und Sicherheit und bildet die erste Verteidigungslinie gegen den Missbrauch von Identitäten.

Typische IAM-Funktionen umfassen: Verzeichnisdienste zur Speicherung und Überprüfung von Benutzeridentitäten | Authentifizierungsmechanismen (von Passwörtern bis zu biometrischen Verfahren und MFA) | Föderation für Partner- oder Kunden-Logins (B2B/B2C) | Bereitstellungs- und Entzugsprozesse, um Zugriffsrechte zu vergeben oder zu entziehen, wenn Personen dem Unternehmen beitreten, sich intern bewegen oder es verlassen.

Modernes IAM legt Wert auf starke Authentifizierung und kontextabhängigen Zugriff (weiter unten erläutert), da Angreifer zunehmend Anmeldedaten ins Visier nehmen.

Identitätsverwaltung & -steuerung (IGA)

Identitätsverwaltung und -steuerung baut auf Identity and Access Management (IAM) auf, indem es steuert, wer über die Zeit hinweg auf welche Ressourcen zugreifen darf. Während IAM Identitäten und Zugriffsrechte einrichtet, stellt IGA sicher, dass diese Zugriffsrechte auch bei Veränderungen in der Organisation und den Rollen weiterhin angemessen und konform bleiben. Es „stellt sicher, dass der Zugriff im Laufe der Zeit angemessen bleibt, indem Berechtigungen verwaltet, Zugriffsüberprüfungen durchgeführt und richtlinienbasierte Kontrollen durchgesetzt werden“. In der Praxis umfasst IGA Prozesse wie: Regelmäßige Zertifizierung der Zugriffsrechte von Nutzern durch ihre Vorgesetzten | Genehmigungs-Workflows für Zugriffsanfragen | Trennung von Aufgaben (Segregation of Duties), um gefährliche Berechtigungskombinationen zu verhindern und Prüfung und Auditierung von Identitätsdaten.

Warum es wichtig ist: IGA ist entscheidend für Compliance, Sicherheit und Effizienz. Ohne Governance sammeln Nutzer im Laufe der Zeit zu viele Berechtigungen an oder behalten Zugriff auf Systeme, die sie nicht mehr benötigen (z. B. nach einem Rollenwechsel oder nach dem Ausscheiden aus dem Unternehmen). Dieser sogenannte „Privilege Creep“ führt zu Sicherheitslücken und kann zu Audit- oder Compliance-Verstößen führen.
IGA hilft Organisationen, das Prinzip der minimalen Rechtevergabe („Least Privilege“) durchzusetzen – jede Identität erhält nur den Zugriff, der unbedingt erforderlich ist – und liefert Nachweise für gesetzliche Vorgaben (wie DSGVO und NIS2), dass der Zugriff auf sensible Daten ordnungsgemäß kontrolliert und überprüft wird.
Durch die Automatisierung von Zugriffsüberprüfungen und Genehmigungen reduziert IGA zudem die manuelle Belastung für IT und Führungskräfte und macht das Zugriffsmanagement skalierbarer.

Kurz gesagt, IGA beantwortet fortlaufend die Frage:
„Soll diese Identität diesen Zugriff weiterhin haben?“
und mindert dadurch Insider-Bedrohungen und Fehler, während die Organisation auditbereit und sicher bleibt.

Verwaltung privilegierter Zugriffsrechte (PAM)

Privileged Access Management (PAM) ist ein spezialisierter Bereich der Identitätssicherheit, der sich auf besonders kritische Konten – die „Schlüssel zum Königreich" – konzentriert. Privilegierte Konten (wie Systemadministratoren, Domain-Admins, Eigentümer von Cloud-Plattformen oder Servicekonten mit weitreichenden Berechtigungen) verfügen über Fähigkeiten, die bei Missbrauch oder Kompromittierung verheerend sein können. PAM konzentriert sich auf den Schutz von hochriskanten Zugangsdaten und Administrator-Berechtigungen, egal ob diese einem menschlichen Administrator oder einem Servicekonto gehören, das Produktionssysteme steuert.

Zu den wichtigsten PAM-Kontrollen gehören:

- ✓ Sichere Speicherung privilegierter Zugangsdaten (z. B. in verschlüsselten Tresoren)
- ✓ Just-in-Time-Zugriff (Erteilung erhöhter Berechtigungen nur bei Bedarf und für eine begrenzte Zeit)
- ✓ Mehrfaktor-Authentifizierung für privilegierte Aktionen
- ✓ Sitzungsüberwachung und -aufzeichnung
- ✓ Automatisches Abmelden oder Rotieren von Zugangsdaten nach der Nutzung.

Warum das wichtig ist: Privilegierte Konten sind ein häufiges Ziel von Cyberangriffen – Angreifer suchen gezielt danach, da sie den höchsten Zugriff gewähren. Ohne PAM kann ein einziges gestohlenes Administrator-Passwort zu einem katastrophalen Sicherheitsvorfall führen, der es einem Eindringling ermöglicht, Systeme zu stören oder große Datenmengen zu stehlen.

PAM-Lösungen verringern dieses Risiko erheblich, indem sie die unkontrollierte Nutzung mächtiger Konten verhindern. Sie stellen sicher, dass Administratoren eindeutige, starke Zugangsdaten verwenden (oft nur für die Dauer einer Aufgabe ausgegeben) und dass alle privilegierten Akti-vitäten nachvollziehbar sind. Dies wehrt nicht nur externe Angreifer ab, sondern reduziert auch Insider-Bedrohungen oder versehentlichen Missbrauch durch IT-Mitarbeiter. Für die Organisation bedeutet die Implementierung von PAM, dass kritische Systeme und Daten wesentlich besser vor Missbrauch geschützt sind. Zudem verlangen viele Compliance-Vorgaben ausdrücklich Kontrollen für administrativen Zugriff – PAM erfüllt diese Anforderungen durch verpflichtende Aufsicht und Prüfpfade.

Kurz gesagt: PAM fügt eine essentielle Sicherheitsschicht um die sensibelsten Zugriffe hinzu und begrenzt drastisch den Schaden, der entstehen kann, wenn eine Identität gehijackt oder missbraucht wird.

Starke Authentifizierung und Zugriffssteuerung

Eine wirksame Authentifizierung bildet die Grundlage für alle oben genannten Identitätsbereiche. Authentifizierung ist der Prozess, mit dem überprüft wird, ob ein Benutzer oder ein System tatsächlich derjenige ist, der er vorgibt zu sein. Schwache Authentifizierung (wie die ausschließliche Verwendung von Passwörtern) ist ein bekannter Schwachpunkt – Passwörter können erraten, ge-stohlen oder durch Phishing erlangt werden.
Starke Authentifizierung bedeutet den Einsatz mehrerer Faktoren (MFA) oder moderner Methoden, die Angreifer nicht leicht umgehen können. Für menschliche Benutzer können dies einmalige Passcodes, Smartphone-Authentifizierungs-Apps, physische Sicherheitsschlüssel oder biometrische Verfahren sein – zusätzlich zu oder anstelle eines Passworts. Für Systemidentitäten (wie APIs oder Servicekonten) bedeutet starke Authentifizierung den Verzicht auf statische Passwörter und die Verwendung von Zertifikaten oder token-basierten Methoden mit sicherem Schlüsselmanagement.

Warum das wichtig ist: Laut Microsoft kann Multi-Faktor-Authentifizierung 99,9 % aller Kontoübernahme-Angriffe auf Benutzerkonten verhindern. Durch die Implementierung von MFA in der gesamten Organisation sinkt das Risiko unbefugten Zugriffs drastisch – selbst wenn ein Passwort gestohlen wird, kann der Angreifer den zweiten Faktor nicht ohne Weiteres bereitstellen.
Aus geschäftlicher Sicht gehört starke Authentifizierung zu den Sicherheitsmaßnahmen mit dem höchsten Return on Investment (ROI): Sie schützt direkt vor häufigen Angriffen wie Phishing und Credential Stuffing und verhindert dadurch kostspielige Sicherheitsvorfälle.
Zusätzlich stärken Techniken wie Conditional Access (eine Zugriffspolitik, die sich basierend auf Kontext und Risiko anpasst) die Authentifizierung weiter. Beispielsweise kann das System bei einem Anmeldeversuch aus einem ungewöhnlichen Standort oder von einem Gerät mit schlechtem Sicherheitsstatus zusätzliche Überprüfung verlangen oder den Zugriff blockieren.
Dies gewährleistet Sicherheit, ohne legitime Benutzer unnötig zu behindern. Durch das Prinzip „niemals standardmäßig vertrauen“ und die kontinuierliche Identitätsprüfung (ein Kernprinzip von Zero Trust) können Organisationen Remote-Arbeit und Cloud-Nutzung sicher ermöglichen.

Unternehmen und schaffen gleichzeitig Flexibilität – Mitarbeiter, Partner und Kunden können sich von überall verbinden, jedoch zu den Bedingungen der IT und mit minimaler Reibung.

Erkennung und Reaktion auf Identitätsbedrohungen (ITDR)

Selbst mit vorbeugenden Maßnahmen sollten Organisationen davon ausgehen, dass einige Identitätsverletzungen auftreten werden (z. B. wenn eine Phishing-E-Mail einen Mitarbeiter täuscht oder ein Altkonto kompromittiert wird). Identity Threat Detection and Response (ITDR) ist eine aufstrebende Säule der Sicherheit, die sich darauf konzentriert, identitätszentrierte Angriffe in Echtzeit zu erkennen und zu entschärfen. ITDR „überwacht die missbräuchliche Nutzung und Kompromittierung von Identitäten" und achtet auf ungewöhnliche Muster, die auf eine Identitätsübernahme oder unbefugte Nutzung von Zugangsdaten hindeuten. Dazu gehören Werkzeuge, die das Anmeldeverhalten auf Anomalien analysieren (z. B. Impossible Travel, ungewöhnliche Uhrzeiten, Änderungen bei Gerät oder IP-Muster), Angriffe auf Verzeichnisinfrastrukturen erkennen (wie Privilegienausweitung in Active Directory oder Missbrauch von SSO-Tokens) und sich in die übergreifenden Sicherheitsoperationen integrieren, um auf Bedrohungen zu reagieren, die auf Identitäten abzielen.

Warum das wichtig ist: Traditionelles Sicherheitsmonitoring hat sich auf Endpunkte und Netzwerke konzentriert, doch moderne Angreifer umgehen diese oft, indem sie Identitätsschwachstellen ausnutzen – etwa durch die Verwendung gültiger Zugangsdaten, um sich einzuloggen und anschließend unbemerkt Privilegien zu erhöhen. ITDR-Lösungen schließen diese Lücke, indem sie speziell für die Erkennung von Identitätsangriffen entwickelt wurden, die in klassischen Endpunkt- oder Netzwerksicherheits-Tools keine Alarme auslösen würden. Gartner und Branchenführer betonen ITDR als entscheidende Komponente einer Zero-Trust-Strategie, um sicherzustellen, dass verdächtiges Verhalten durch oder gegen eine Identität frühzeitig erkannt wird. Beispiel: Wenn ein Angreifer Zugriff auf ein inaktives Konto erhält und beginnt, auf sensible Daten zuzugreifen, kann ITDR diese ungewöhnliche Aktivität erkennen und automatisch reagieren (z. B. durch Widerruf von Tokens oder Anforderung einer erneuten Authentifizierung). Microsofts Ansatz zu ITDR betont die Vereinheitlichung von Identitätsschutz und Sicherheitsoperationen – durch den Austausch von Signalen zwischen Identitätssystemen und dem Security Operations Centre (SOC), damit An-griffe schnell gestoppt werden können. Aus geschäftlicher Sicht reduzieren ITDR-Funktionen die Wahrscheinlichkeit, dass eine Identitätsverletzung zu einem vollumfänglichen Sicherheitsvorfall eskaliert. Sie helfen, den „Blast Radius" einer Identitätskompromittierung zu begrenzen, indem sie diese schnell erkennen und reagieren (oft automatisiert), bevor

ein Angreifer tiefer in Systeme eindringen kann. Als Teil eines ausgereiften Identitätssicherheitsprogramms gibt ITDR CISOs und CIOs mehr Vertrauen, dass selbst wenn präventive Kontrollen versagen, ein Sicherheitsnetz vorhanden ist, um identitätsbasierte Bedrohungen abzufangen und einzudämmen.

Aufbau eines umfassenden Programms zur Identitätssicherheit

Das Verständnis der einzelnen Komponenten ist ein Anfang – doch wie bringt man sie strategisch zusammen? Erfolgreiche Identitätssicherheit hängt ebenso sehr von Menschen und Prozessen ab wie von Technologie. Hier sind zentrale Schritte und Best Practices für die Umsetzung eines ganzheitlichen Programms:

Bewerten und Inventarisieren aller Identitäten und Zugriffe: Man kann nur schützen, was man kennt. Beginnen Sie mit einer gründlichen Erfassung aller menschlichen und nicht-menschlichen Identitäten in Ihrer Organisation (Mitarbeiterkonten, Servicekonten, Cloud-Rollen usw.) sowie deren Zugriffsrechte. Identifizieren Sie besonders risikobehaftete Identitäten (wie Domain-Administratoren oder Konten externer Dienstleister) sowie „verwaiste" Konten, die keinem aktuellen Besitzer zugeordnet sind. Diese Bewertung deckt Lücken auf – etwa Benutzer mit übermäßigen Berechtigungen oder Anwendungen ohne MFA – und hilft, Prioritäten zu setzen. Mit den richtigen Tools lässt sich dieser Prozess von mühsamer Tabellenkalkulation in einen wiederholbaren und automatisierten Ablauf verwandeln.

Starke Authentifizierung überall durchsetzen: Machen Sie Multi-Faktor-Authentifizierung (MFA) für alle Benutzer verpflichtend – insbesondere für privilegierte und Remote-Zugriffe. Ziehen Sie in Betracht, schrittweise fortschrittliche Methoden wie passwortlose Authentifizierung (z. B. biometrische Verfahren oder FIDO2-Sicherheitsschlüssel) einzuführen, um Sicherheit und Benutzerfreundlichkeit zu verbessern. Nutzen Sie Conditional Access-Richtlinien, um sich an das jeweilige Risiko anzupassen – beispielsweise MFA nur für sensible Anwendungen oder bei erkannten Risikofaktoren (ungewöhnliche Anmeldeorte, „Impossible Travel") verlangen. So bleiben Sicherheitsmaßnahmen wirksam, ohne Benutzer zu ermüden.

Least Privilege über IAM- & IGA-Prozesse umsetzen: Nutzen Sie Ihre Identity and Access Management (IAM)- und Identity Governance and Administration (IGA)-Tools, um das Prinzip durchzusetzen, dass jede Identität nur den minimal erforderlichen Zugriff erhält. Etablieren Sie rollenbasierte Zugriffskontrollen (RBAC), sodass Standardrollen vordefinierte Zugriffsrechte haben und Ad-hoc-Berechtigungen reduziert werden. Implementieren Sie einen Identitätslebenszyklus-Prozess: Wenn Personen neu hinzukommen, Rollen wechseln oder das Unternehmen verlassen, sollte ihr Zugriff umgehend angepasst oder entfernt werden. Führen Sie regelmäßig Zugriffsüberprüfungen (Attestations) für kritische Systeme durch – nutzen Sie IGA-Lösungen, damit Manager oder Systemverantwortliche bestätigen, wer weiterhin Zugriff haben sollte. Dieser Governance-Zyklus verhindert Privilege Creep (schleichende Ausweitung von Berechtigungen) und stellt langfristig die Compliance sicher.

Privilegierten Zugriff sichern und überwachen: Falls noch nicht geschehen, sollten Sie in eine Privileged Access Management (PAM)-Lösung investieren oder Cloud-Funktionen für privilegierte Verwaltung nutzen (z. B. Microsoft Entra Privileged Identity Management für Azure AD-Rollen). Speichern Sie alle administrativen Passwörter in einem Tresor und verwenden Sie Auscheck-Prozesse mit Genehmigungen für jede Person, die erhöhte Zugriffsrechte erhält. Aktivieren Sie Just-in-Time-Erhöhungen, sodass Administratorrechte automatisch ablaufen, wenn sie nicht genutzt werden. Überwachen Sie alle administrativen Sitzungen (zeichnen Sie bei kritischen Systemen Tastatureingaben oder Befehle auf, sofern möglich) und richten Sie Warnmeldungen für ungewöhnliche privilegierte Aktivitäten ein (z. B. wenn unerwartet ein neuer Benutzer zur Gruppe der Domain-Admins hinzugefügt wird). Behandeln Sie Ihre Verzeichnisinfrastruktur (z. B. Active Directory oder Entra ID) als Tier-0-Asset – sichern Sie sie mit den höchsten Sicherheitskontrollen, da jeglicher andere Zugriff von ihrer Integrität abhängt.

Identitätssignale in die Bedrohungserkennung integrieren: Speisen Sie Aktivitätsprotokolle zu Identitäten (aus IAM-Systemen, Active Directory, Cloud-Verzeichnissen, SSO usw.) in Ihre Security-Operations-Workflows (SIEM/SOC) ein. Setzen Sie Tools zur Erkennung von Identitätsbedrohungen ein – beispielsweise Microsoft Entra ID Protection und Microsoft Defender for Identity – die sich auf die Erkennung von Angriffen auf Zugangsdaten oder anomale Nutzung spezialisiert haben. Stellen Sie sicher, dass bei der Erkennung einer möglichen Kompromittierung Playbooks für eine schnelle Reaktion vorhanden sind: Automatisieren Sie das Deaktivieren von Konten oder das Zurücksetzen von Passwörtern bei Verdacht auf kompromittierte Konten und nutzen Sie Conditional Access, um riskante Sitzungen dynamisch zu blockieren oder zusätzliche Authentifizierungsschritte zu erzwingen. Simulieren Sie regelmäßig Szenarien von Identitätsverletzungen, um Ihre Erkennung und Reaktion zu testen (führen Sie z. B. eine Phishing-Übung durch und prüfen Sie, ob das SOC die Nutzung eines geleakten Test-Zugangsdatenpaars erkennt).

Eine sicherheitsbewusste Unternehmenskultur fördern: Technologie allein reicht nicht aus. Schulen Sie Mitarbeiter in guter Identitätshygiene – etwa beim Erkennen von Phishing-Versuchen, der Nutzung genehmigter Passwortmanager und dem Grundsatz, Zugangsdaten niemals zu teilen. Führen Sie Richtlinien und Schulungen ein, damit jeder versteht, dass der Schutz seiner Anmeldedaten Teil seiner Verantwortung ist (z. B. verlorene Geräte sofort melden oder MFA-Aufforderungen nicht ignorieren). Bauen Sie eine enge Zusammenarbeit zwischen Ihren Identitätsadministratoren und dem Sicherheitsteam auf: Sie sollten Hand in Hand arbeiten, da Identität heute eine zentrale Verteidigungslinie darstellt. Wenn IT- und Sicherheitsteams kooperieren (wie in Microsofts Referenzarchitektur empfohlen), können Bedrohungen schneller adressiert und Richtlinien kontinuierlich verbessert werden.

Fazit: Durch die Umsetzung dieser Praktiken schaffen Organisationen mehrere Verteidigungsschichten rund um Identitäten, während der Zugriff flexibel bleibt. Ziel ist eine adaptive, widerstandsfähige Identitätssicherheitsstrategie – eine, die nicht nur gegen heutige Angriffe auf Zugangsdaten schützt, sondern sich auch an neue Bedrohungen und Geschäftsanforderungen anpassen kann.

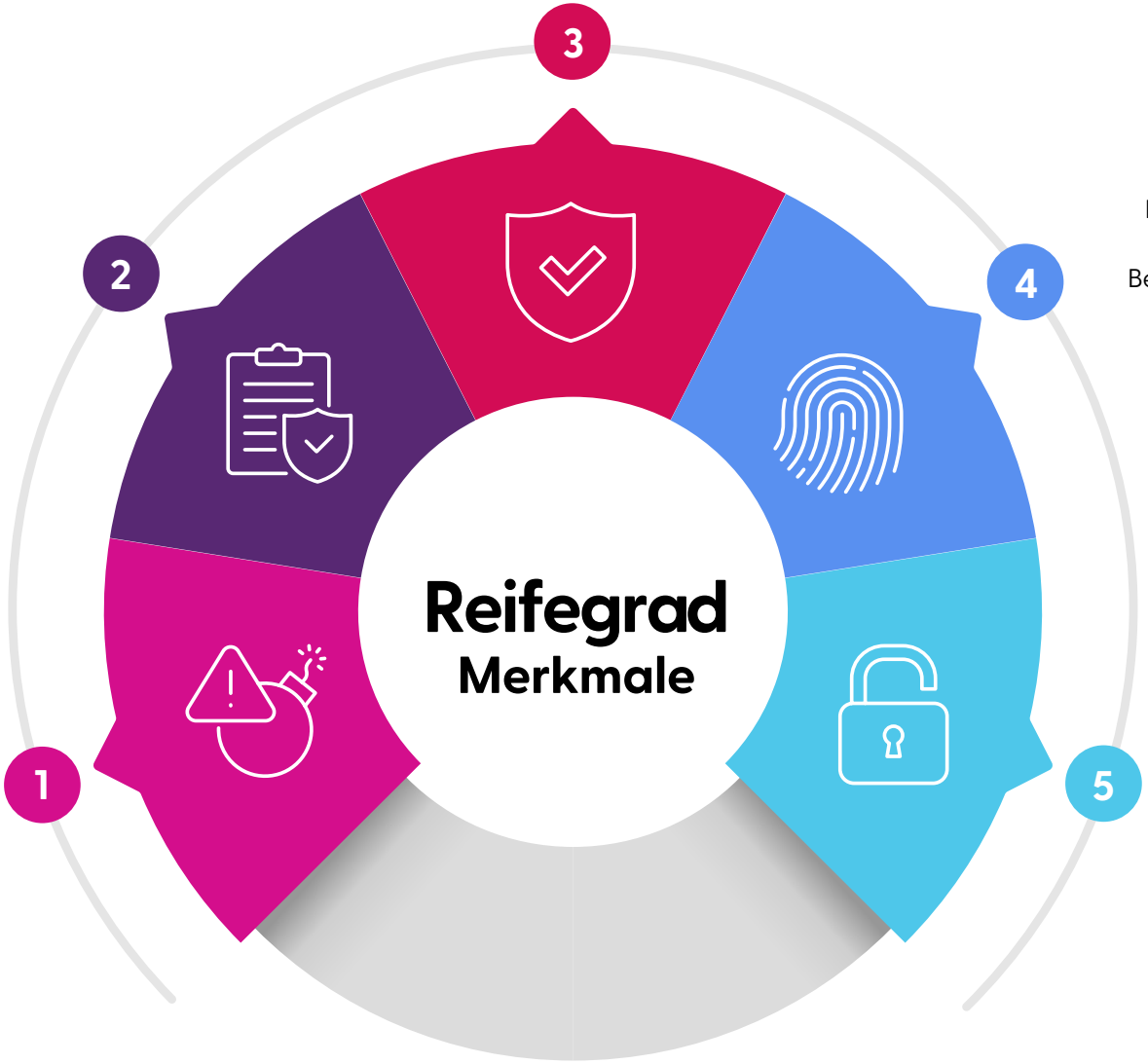
Identitätsreife

Managed

Automatisierte Bereitstellung, Single Sign-On (SSO) für wichtige Anwendungen, Kontrolle privi-legierter Zugriffe, regelmäßige Zugriffsüberprüfungen

Baseline

Zentralisierte Verzeichnisse, MFA für einige Benutzer, grundlegender rollenbasierter Zugriff, gelegentliche Audits



Optimised

Bedingte Zugriffsrichtlinien, identitätsbasierte Bedrohungserkennung, starke Governance-Prozesse

Adhoc

Nicht verbundene Systeme, schlechte Passworthygiene, manuelle Benutzerbe-reitstellung, kaum oder keine Multi-Faktor-Authentifizierung (MFA)

Adaptive

Risikobasierter Zugriff, passwortlos, KI-gestützte Erkennung, ausgerichtet auf Zero Trust und Geschäftsergebnisse

Die Zukunft der Identitätssicherheit

Identitätssicherheit geht längst über die reine Zugangskontrolle zu Systemen hinaus. Sie entwickelt sich zu einer dynamischen, intelligent gesteuerten Grundlage, die sichere Zusammenarbeit, dezentralen Zugriff und Automatisierung im großen Maßstab ermöglicht. Mit der zunehmenden Nutzung von Cloud-Technologien, hybriden Arbeitsmodellen und KI-gestützten Betriebsabläufen wandelt sich die Rolle der Identität von reaktiver Zugangskontrolle hin zu proaktiver Verteidigung und Geschäftsförderung. Vorausschauende Organisationen bereiten sich bereits auf diesen Wandel vor.

Hier sind die Trends, die die Zukunft der Identitätssicherheit prägen – und was sie für Ihre Organisation bedeuten:

Dezentralisierte Identität & verifizierbare Anmeldedaten

Dezentrale Identität (DID) ermöglicht es Nutzern, ihre eigenen Identitätsdaten zu verwalten und zu kontrollieren, ohne auf eine zentrale Instanz angewiesen zu sein. Identitäten basieren auf verifizierbaren Anmeldedaten, die außerhalb der Blockchain („off-chain“) in sicheren digitalen Wallets gespeichert und mithilfe von Public-Key-Kryptografie oder verteilten Ledgern validiert werden. Microsoft investiert in diesem Bereich mit Entra Verified ID und unterstützt damit den Wandel hin zu einer selbstbestimmten Identität (Self-Sovereign Identity).

Warum das wichtig ist:
Dieses Modell verringert die Abhängigkeit von Identitätsanbietern und ermöglicht es Organisationen, Identitätsattribute (z. B. Beschäftigungsstatus, Zertifizierungen, Gesundheitsstatus) zu überprüfen, ohne personenbezogene Daten zu speichern. In Branchen wie Bildung, öffentlicher Sektor und Gesundheitswesen verbessert es den Datenschutz, verhindert Identitätsbetrug und erleichtert die Einhaltung von Vorschriften wie der DSGVO. Mit wachsender Verbreitung werden Organisationen Strategien benötigen, um dezentrale Anmeldedaten sicher und im großen Maßstab auszustellen, zu verifizieren und zu nutzen.

Identität-als-Code und richtlinienbasierter Zugriff

In Anlehnung an Infrastructure-as-Code behandelt Identity-as-Code Identitätskonfigurationen (Rollen, Richtlinien, Berechtigungen) als versionskontrollierten Code, der in CI/CD-Pipelines integriert ist. Tools wie Microsoft Entra Permissions Management und Terraform-basierte Governance-Frameworks bringen dieses Konzept in gängige Unternehmensumgebungen. **Warum das wichtig ist:**
Die Definition von Identitätsrichtlinien als Code ermöglicht schnellere und konsistentere Bereitstellungen sowie eine bessere Prüfbarkeit. Sicherheits- und Plattformteams können über DevSecOps-Workflows zusammenarbeiten, wodurch Fehlkonfigurationen und menschliche Fehler reduziert werden. Wenn Organisationen auf Multi-Cloud- und hybride Umgebungen skalieren, stellt Identity-as-Code sicher, dass Zugriffskontrollen sich parallel zur Infrastruktur weiterentwickeln – nicht erst im Nachhinein.

Rasanter Anstieg von Maschinenidentitäten

Nicht-menschliche Identitäten – APIs, Container, IoT-Geräte, Microservices – übertreffen mittlerweile in den meisten Unternehmen die Anzahl menschlicher Benutzer. Jede dieser Identitäten benötigt Anmeldedaten (Tokens, Secrets, Zertifikate) und Zugriffskontrollen. Dennoch behandeln viele Organisationen sie immer noch als Nebensache – mit fest im Code hinterlegten Zugangsdaten, schlechter Rotation oder fehlendem Lebenszyklus-Management.
Warum das wichtig ist:
Maschinenidentitäten sind ein Hauptziel für Angreifer, die dauerhaften und verdeckten Zugriff suchen. Ihre effektive Verwaltung erfordert spezielle Kontrollen – einschließlich automatisierter Geheimnisrotation, Sichtbarkeit ungenutzter oder überprivilegierter Servicekonten sowie Integration mit Tools zur Geheimnisverwaltung (z. B. Azure Key Vault, HashiCorp Vault). In zukunftsfähigen Identitätsprogrammen werden menschliche und maschinelle Identitäten mit gleicher Sorgfalt verwaltet.

KI-gestützte Identitätssicherheit

Microsoft Entra ID Protection und Defender for Identity nutzen bereits KI, um Anomalien im Anmeldeverhalten zu erkennen – etwa unmögliche Reisebewegungen, Token-Wiederverwendung oder MFA-Ermüdungsangriffe. Diese Fähigkeiten entwickeln sich weiter, um kontextbezogene, autonome Entscheidungsprozesse zu ermöglichen. **Warum das wichtig ist:**
Statische Regeln halten mit der Geschwindigkeit und Kreativität moderner Angreifer nicht Schritt. KI-gestützter Schutz ermöglicht Echtzeit-Risikobewertung, adaptive Richtlinien und automatisierte Gegenmaßnahmen – verkürzt Reaktionszeiten und begrenzt Kompromittierungen. Mit besseren KI-Modellen werden Identitätsplattformen zunehmend Erkennung, Entscheidung und Handlung autonom übernehmen und nur schwerwiegende oder unklare Vorfälle an Analysten weiterleiten.

Insight & Microsoft: Ihre Partner für herausragende Identitäts-sicherheit

Die Umsetzung des gesamten Spektrums der Identitätssicherheit kann komplex sein. Genau hier macht der richtige Partner den entscheidenden Unterschied. Insight ist als führender Anbieter von Identitätssicherheitsdiensten positioniert – unterstützt durch eine außergewöhnlich starke Partnerschaft mit Microsoft. Das Expertenteam von Insight verfügt über tiefgehende, praxisnahe Erfahrung mit Microsofts Identitäts- und Sicherheitstechnologien – von Azure Active Directory (jetzt Microsoft Entra ID) bis hin zu den neuesten Tools für Identitäts-Governance und Bedrohungsschutz. Tatsächlich gehört Insight zu Microsofts weltweit führenden Sicherheitspartnern: Wir halten alle vier Microsoft Security Advanced Specialisations, darunter die Spezialisierung für Identity and Access Management sowie Spezialisierungen in Cloud Security, Information Protection und Threat Protection. Insight ist zudem Mitglied der Microsoft Intelligent Security Association (MISA) und arbeitet eng mit Microsofts Sicherheitsteams zusammen.

Was bedeuten diese Qualifikationen für Sie als Kunden? Kurz gesagt: Insight bringt nachweisliche Expertise mit, um eine auf Ihre Organisation zugeschnittene Identitätssicherheitsstrategie zu entwerfen und umzusetzen – unter Nutzung der besten Microsoft-Technologien. Ob Sie Ihre lokale Identitätsinfrastruktur stärken oder die vollständige Microsoft Entra-Suite für cloudbasierte Identität einführen – Insight verfügt über mehr als 1.500 Microsoft-zertifizierte Architekten und Sicherheitsingenieure, die bereit sind zu helfen. Unsere Experten haben Unternehmen weltweit dabei unterstützt: Mehrfaktor-Authentifizierung einzuführen | Single Sign-On über Tausende von Apps zu aktivieren | Den Identitätslebenszyklus mit Tools wie Microsoft Entra ID Governance zu automatisieren | Identitätssignale in Bedrohungserkennungsplattformen zu integrieren. Wir stimmen diese Lösungen mit Ihren Geschäftsziele ab, sodass Sicherheitsverbesserungen auch Produktivität und Benutzerfreundlichkeit fördern.

Dank der engen Partnerschaft mit Microsoft sind wir stets an der Spitze neuer Entwicklungen in der Identitätssicherheit. Als Microsoft beispielsweise Identity Threat Detection & Response-Funktionen und KI-gestützte Sicherheitsanalysen einführte, gehörte Insight zu den ersten, die diese in unsere Managed Services integrierten. (Insight war eines der ersten Unternehmen, das den verifizierten Managed XDR-Status von Microsoft erreichte – ein Beweis für unsere Fähigkeit, Identitätsbedrohungserkennung mit 24/7-Reaktionsoperationen zu verbinden.) Wir folgen zudem der Microsoft Security Reference Architecture – einer bewährten Best-Practice-Architektur – um sicherzustellen, dass alle Komponenten der Identitätssicherheit in Ihrer Umgebung nahtlos zusammenarbeiten. Das Ergebnis ist eine integrierte Gesamtlösung, keine isolierten Einzeltools.

Am wichtigsten ist: Insight betrachtet Identitätssicherheit als strategischen Enabler für Ihr Geschäft. Wir setzen nicht nur Technologie um – wir arbeiten mit Ihren Stakeholdern zusammen, um Richtlinien, Governance-Modelle und Benutzerakzeptanzstrategien zu entwickeln, die die Lösungen effektiv machen. Wie das Sicherheitsteam von Insight UK sagt: „Digitale Identität ist der Schlüssel zum Herzen jeder Organisation und muss daher mit derselben Priorität geschützt werden wie Daten oder Infrastruktur. Microsoft bietet eine umfassende Architektur, aber echte Wirkung entsteht erst durch die Kombi-nation mit Kultur, Prozessen und organisatorischem Engagement.“ Insight hilft, dieses Gesamtbild zu vervollständigen. Wir bieten Leistungen von ersten Assessments und Workshops über praktische Implementierungen bis hin zu Managed Identity Security Operations. Ganz gleich, wo Sie sich auf Ihrer Reifegradkurve für Identitätssicherheit befinden – Insight hat die Expertise, Sie weiterzubringen.

Mit Insight als Partner gewinnen Sie ein Team, das nicht nur technisch versiert ist, sondern auch tief in Ihren Erfolg investiert. Wir messen unseren Erfolg daran, dass Sie Sicherheitsverletzungen verhindern, Compliance-Ziele erreichen und neue Technologien sicher einführen – alles unter dem Schutz eines robusten Identitätssicherheitsrahmens. Mit Insight und Microsoft an Ihrer Seite wird Identitätssicherheit von einer Sorge zu einer geschäftlichen Stärke.

Microsoft

Fazit

Identitätssicherheit ist mehr als ein Punkt auf einer Checkliste – sie ist eine strategische Notwendigkeit in der modernen Bedrohungslandschaft. Durch das Verständnis und die Integration der zentralen Säulen (IAM, IGA, ITDR) können Organisationen ihre kritischen Werte schützen und ihre Mitarbeitenden befähigen, effizient und sicher zu arbeiten.

Der Weg mag komplex erscheinen, aber Sie müssen ihn nicht allein gehen. Mit einem vertrauenswürdigen Partner wie Insight – ausgestattet mit branchenführenden Microsoft-Lösungen und unvergleichlicher Expertise – können Sie ein Identitätssicherheitsprogramm aufbauen, das Ihr Unternehmen heute schützt und zugleich auf das vorbereitet, was als Nächstes kommt.

Glossar

Begriff	Definition
Zugriffskontrollrichtlinien	Richtlinien und Technologien, die festlegen, wer auf bestimmte Systeme, Daten oder Dienste zugreifen darf – und unter welchen Bedingungen.
Authentifizierung	Der Prozess zur Überprüfung der Identität eines Benutzers, Geräts oder Systems mithilfe von Faktoren wie Passwörtern, biometrischen Daten oder Sicherheitsschlüsseln.
Autorisierung	Der Prozess, der bestimmt, welche Aktionen oder Zugriffe einer authentifizierten Identität erlaubt sind.
Bedingter Zugriff	Dynamische Zugriffsrichtlinien, die Risikosignale (wie Gerätestatus oder Standort) auswerten, bevor der Zugriff gewährt wird.
Dezentralisierte Identität (DID)	Ein Identitätsmodell, bei dem Einzelpersonen ihre eigenen Identitätsdaten und Anmeldedaten kontrollieren, verifiziert durch verteilte Technologien.
Verzeichnisdienste	Zentralisierte Systeme zur Verwaltung von Identitätsinformationen, wie Microsoft Entra ID oder Active Directory.
Identitäts- und Zugriffsmanagement (IAM)	Grundlegende Systeme und Richtlinien zur Verwaltung digitaler Identitäten und zur Kontrolle des Zugriffs auf Ressourcen.
Identität-als-Code	Die Behandlung von Identitätskonfigurationen (Rollen, Richtlinien) als Code, um Automatisierung, Prüfbarkeit und Integration in DevOps-Pipelines zu ermöglichen.
Identitätsverwaltung und -administration (IGA)	Werkzeuge und Prozesse zur Verwaltung des Lebenszyklus von Identitätszugriffen, einschließlich Überprüfungen, Genehmigungen und Richtliniendurchsetzung.
Identitätslebenszyklus	Der vollständige Prozess der Aufnahme, Änderung und Aussonderung von Identitäten während ihrer Zugehörigkeit zur Organisation.
Erkennung und Reaktion auf Identitätsbedrohungen(ITDR)	Funktionen zur Überwachung und Reaktion auf identitätsbasierte Bedrohungen wie Missbrauch, Eskalation oder Anomalieerkennung.

Begriff	Definition
Just-in-Time Zugriff (JIT)	Gewährung privilegierter Zugriffsrechte nur vorübergehend und nur bei Bedarf, um bestehende Risiken zu minimieren.
Prinzip der minimalen Rechte (Least Privilege)	Ein Grundsatz, der sicherstellt, dass Benutzer und Systeme nur die Zugriffsrechte haben, die für ihre Arbeit erforderlich sind – nicht mehr.
Maschinenidentität	Nicht-menschliche Konten, die von Software, APIs, Diensten oder Geräten genutzt werden und Identitätskontrollen sowie Governance erfordern.
Mehrstufige Authentifizierung (MFA)	Ein Authentifizierungsansatz, der zwei oder mehr Formen der Verifizierung erfordert und die Widerstandsfähigkeit gegen Kontoübernahmen verbessert.
Passwortlose Authentifizierung	Anmeldemethoden, die Passwörter überflüssig machen, z. B. durch biometrische Verfahren, Gerätevertrauen oder kryptografische Schlüssel.
Privilegiertes Zugriffsmanagement (PAM)	Kontrollen und Werkzeuge, die Administrator- und andere sensible Konten durch Passwort-Tresore, Überwachung und JIT-Zugriff absichern.
Rollenbasierte Zugriffskontrolle (RBAC)	Eine Methode zur Vergabe von Zugriffsrechten basierend auf der Funktion oder Rolle eines Benutzers.
Selbstbestimmte Identität (SSI)	Ein Modell, bei dem Benutzer ihre digitalen Identitäten unabhängig von zentralen Behörden besitzen und verwalten.
Dienstkonto	Eine digitale Identität, die von Systemen oder Software zur Ausführung automatisierter Aufgaben genutzt wird und oft erhöhte Berechtigungen benötigt.
Einmalanmeldung Single Sign-On (SSO)	Ein System, das es Benutzern ermöglicht, sich einmal anzumelden und anschließend Zugriff auf mehrere Systeme oder Anwendungen zu erhalten.
Tokenbasierte Authentifizierung	Authentifizierung, die auf sicheren Tokens (z. B. JWTs) basiert, anstatt Benutzernamen und Passwörter erneut einzugeben.
Zero Trust	Eine moderne Sicherheitsphilosophie, bei der Zugriff niemals vorausgesetzt, sondern stets überprüft wird – basierend auf Kontext und kontinuierlicher Bewertung.

Die nächsten Schritte

Kontaktieren Sie Insight, um Ihr umfassendes Identitätssicherheitsprogramm aufzubauen. Da Identität mittlerweile der primäre Angriffsvektor für Unternehmen ist, ist die Absicherung jedes Benutzers, jedes Servicekontos und jeder Verbindung geschäftskritisch. Unser ganzheitlicher Ansatz schützt Ihre digitalen Identitäten, reduziert Risiken und ermöglicht die Umsetzung von Zero Trust-Prinzipien.
Wir helfen Ihnen sicherzustellen, dass nur die richtigen Personen den richtigen Zugriff erhalten – und gleichzeitig die Produktivität optimiert wird. Vertrauen Sie auf Insights tiefgehende Expertise und die enge Partnerschaft mit Microsoft, um Ihre Identitätssicherheit von einer komplexen Herausforderung in einen geschäftlichen Erfolgsfaktor zu verwandeln.

- **at.insight.com**
- **ch.insight.com**
- **de.insight.com**