WHITEPAPER von PATECCO

April 2026

Top-Risiken im IAM, die jede Organisation kennen sollte

- Warum Organisationen IAM-Risiken aktiv adressieren sollten
- Typische IAM-Risiken und wie man sie verhindert
- Stärkung des IAM durch proaktives Risikomanagement

Inhaltsverzeichnis:

❖ Einführung

Das Verwalten von Benutzeridentitäten und Zugriffsrechten wird zunehmend komplexer. Mit dem Wachstum von Remote-Arbeit und der zunehmenden Nutzung cloudbasierter Systeme wird es immer wichtiger, den Überblick darüber zu behalten, wer auf welche Ressourcen zugreifen kann. An dieser Stelle spielt das Identity and Access Management (IAM) eine entscheidende Rolle.

IAM stellt sicher, dass die richtigen Personen zum richtigen Zeitpunkt auf die richtigen Systeme zugreifen können. Man kann es sich wie einen digitalen Torwächter vorstellen: IAM schützt sensible Informationen, indem es reguliert, wer auf welche Ressourcen zugreifen und mit ihnen interagieren darf. Gleichzeitig gehen mit dieser Verantwortung signifikante Risiken einher, die Organisationen verstehen und proaktiv angehen müssen.

In diesem Whitepaper werden wir einige der häufigsten IAM-Risiken und deren potenzielle Konsequenzen beleuchten. Darüber hinaus geben wir praktische Strategien zur Risikominimierung an die Hand, um die Sicherheit zu erhöhen, die Compliance zu gewährleisten und die wertvollsten digitalen Assets einer Organisation zu schützen. Durch das Verständnis und das proaktive Management dieser Herausforderungen können Unternehmen nicht nur Datenpannen verhindern, sondern auch eine stärkere und resilientere IT-Umgebung aufbauen.

❖ Warum Organisationen IAM-Risiken aktiv adressieren sollten

In der heutigen digitalen Umgebung ist das Identitäts- und Zugriffsmanagement (IAM) ein zentraler Bestandteil des Risikomanagements in Unternehmen. Da Unternehmen auf Cloud-Plattformen, hybride Arbeitsmodelle und miteinander verbundene Systeme setzen, nimmt die Anzahl der Identitäten, Rollen und Zugriffspunkte kontinuierlich zu. Ohne proaktive Überwachung können Lücken in der Identitätsverwaltung schnell zu Sicherheitsrisiken, Compliance-Problemen und betrieblichen Ineffizienzen führen.

Durch einen präventiven Ansatz für IAM-Risiken können Unternehmen Transparenz gewährleisten, einheitliche Richtlinien durchsetzen und die Wahrscheinlichkeit von Vorfällen verringern, bevor diese eskalieren. Die frühzeitige Behebung von Schwachstellen schützt nicht nur sensible Daten, sondern stärkt auch die Geschäftskontinuität und das Vertrauen der Stakeholder.

Wichtige Gründe, IAM-Risiken proaktiv zu managen, sind unter anderem:

- **Reduzierung finanzieller Risiken**
  Die frühzeitige Identifikation von Zugriffsschwachstellen hilft dabei, kostspielige Sicherheitsvorfälle, regulatorische Strafen und Aufwendungen für die Wiederherstellung zu verhindern.
- **Schutz der Reputation der Organisation**
  Starke Identitätskontrollen stärken das Vertrauen von Kunden und Partnern und minimieren die reputationsschädigenden Auswirkungen von Sicherheitsvorfällen.
- **Sicherstellung der operativen Effizienz**
  Gut verwaltete Zugriffsrechte verhindern Unterbrechungen von Arbeitsabläufen, reduzieren den administrativen Aufwand und unterstützen die Produktivität.
- **Einhaltung gesetzlicher Vorschriften**
  Proaktive IAM-Governance unterstützt die Einhaltung sich entwickelnder Datenschutz- und Branchenvorschriften und reduziert somit Prüfungsrisiken.
- **Stärkung des Sicherheitsrahmens**
  Kontinuierliche Überwachung und Verbesserung der Identitätskontrollen ermöglichen eine schnellere Erkennung und Abwehr von Bedrohungen.

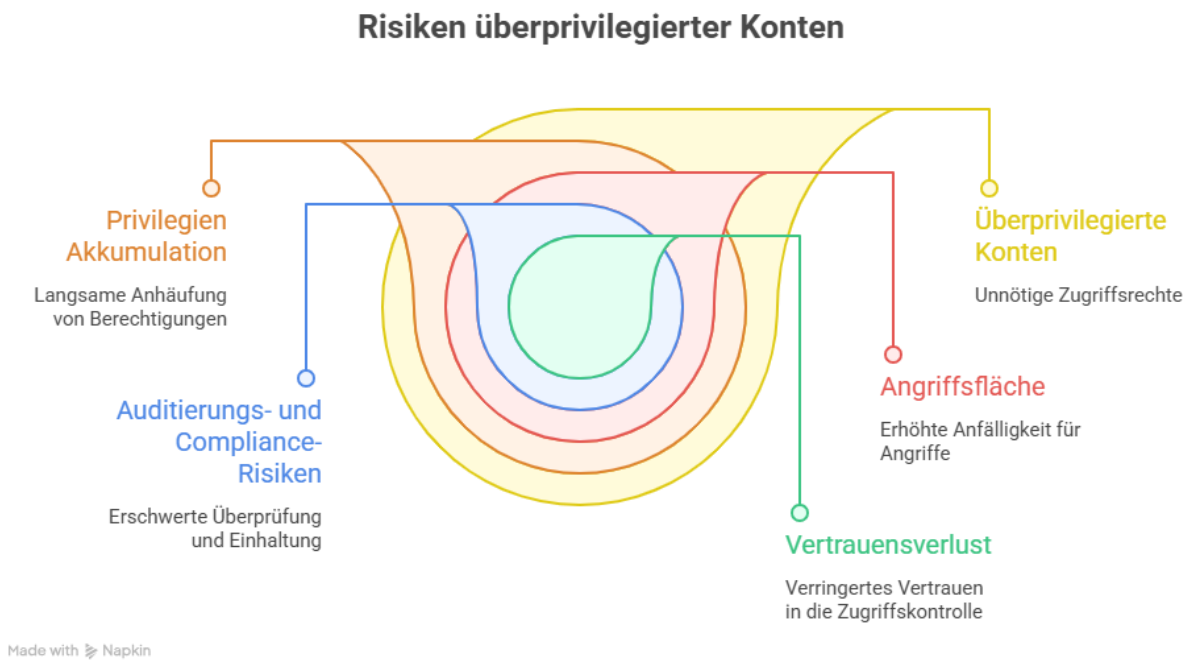
Durch die Einbettung des IAM-Risikomanagements in die strategische Planung, anstatt sich nur dann damit zu befassen, wenn Probleme auftreten, positionieren sich Unternehmen so, dass sie sicher arbeiten, die Compliance-Anforderungen erfüllen und sich selbstbewusst an die sich wandelnden digitalen Herausforderungen anpassen können.

❖ Typische IAM-Risiken und wie man sie verhindern

1.Überprivilegierte Konten

Übermäßige Zugriffsrechte entstehen, wenn Benutzer, Anwendungen oder Systeme Berechtigungen erhalten, die über das für ihre Aufgaben erforderliche Maß hinausgehen. Dies ist häufig das Ergebnis einer “Privilegien Akkumulation“, bei den Berechtigungen im Laufe der Zeit gewährt, aber nicht regelmäßig überprüft oder entfernt werden. Obwohl dies zunächst praktisch erscheint, vergrößert eine solche Überversorgung die Angriffsfläche und kann von externen Angreifern oder internen Akteuren ausgenutzt werden.

In komplexen IT-Umgebungen entstehen überprivilegierte Zugriffsrechte häufig durch Rollenwechsel, temporäre Projektzuweisungen oder inkonsistente Prozesse im Identitätslebenszyklus. Wenn Berechtigungen nicht dem Prinzip der minimalen Rechte (“Least Privilege“) entsprechen, riskieren Organisationen, die Kontrolle darüber zu verlieren, wer auf sensible Daten zugreifen oder kritische Aktionen ausführen kann. Im Laufe der Zeit erschweren diese unkontrollierten Berechtigungen die Auditierung, erhöhen die Compliance-Risiken und verringern das Vertrauen in die Praktiken der Zugriffskontrolle.



Auswirkung:

Erhöhte Schadensanfälligkeit, falls Anmeldeinformationen kompromittiert oder intern missbraucht werden, was potenziell zu Datenverlust, Betriebsunterbrechungen oder Verstößen gegen Compliance-Vorgaben führen kann.

Minderungsstrategien:

- Rollenbasierte Zugriffskontrolle (RBAC) anwenden, um Berechtigungen an klar definierte Rollen anzupassen
- Regelmäßige Überprüfungen der Zugriffsberechtigungen durchführen (Access Certification Reviews)
- Automatisierte Überwachungstools einsetzen, um Privilegien Erweiterungen frühzeitig zu erkennen
- Dokumentierte Begründungen für alle erhöhten Zugriffsrechte pflegen

2. Unzureichende Passwortverwaltung

Unzureichende Passwortstandards bleiben eine anhaltende Schwachstelle in der Cybersicherheit. Trotz Fortschritten bei Authentifizierungstechnologien verlassen sich viele Organisationen weiterhin stark auf Passwörter, ohne robuste Richtlinien durchzusetzen. Probleme wie zu geringe Mindestlängen, seltene Passwortwechsel oder die Akzeptanz vorhersehbarer Muster schwächen die allgemeine Sicherheit erheblich.

Da Bedrohungsakteure zunehmend automatisierte Angriffe auf Zugangsdaten durchführen, wie etwa Brute-Force-Versuche, Password-Spraying oder Phishing-Kampagnen, erhöht schwaches Passwort- und Zugriffsmanagement die Wahrscheinlichkeit unbefugter Zugriffe erheblich. Passwortbezogene Schwachstellen stellen ein signifikantes Risiko in Umgebungen dar, in denen mehrschichtige Authentifizierungsmechanismen oder Programme zur Sensibilisierung der Nutzer fehlen. Die Stärkung der Passwort-Governance ist daher ein grundlegender Schritt, um die Resilienz des IAM zu erhöhen und identitätsbezogene Risiken zu reduzieren.

Auswirkung:

Schwache Zugangsdaten bieten Bedrohungsakteuren leicht nutzbare Einstiegspunkte und erhöhen die Wahrscheinlichkeit unbefugter Systemzugriffe oder Übernahmen von Benutzerkonten.

Minderungsstrategien:

- Strenge Richtlinien zu Passwortkomplexität, -länge und -wiederverwendung durchsetzen
- Multi-Faktor-Authentifizierung (MFA) in allen Umgebungen aktivieren
- Sichere Passwortverwaltungs-Tools fördern und einsetzen
- Regelmäßige Schulungs- und Sensibilisierungsprogramme für Mitarbeiter durchführen

3. Limitierte Zugriffsüberwachung und -transparenz

Effektive IAM-Kontrolle erfordert eine kontinuierliche Überwachung von Zugriffsverhalten, Anomalieerkennung und die Auditierbarkeit von Änderungen. Ohne ausreichende Transparenz wird es sehr schwierig, unbefugte Zugriffe zu erkennen oder verdächtige Aktivitäten nachzuvollziehen. Diese Sichtbarkeitslücke ist besonders riskant in dynamischen, integrierten IT-Umgebungen, in denen Identitäten über mehrere Plattformen und Dienste hinweg interagieren.

Begrenzte Überwachungsmöglichkeiten können die Erkennung von Sicherheitsvorfällen verzögern und die Untersuchung erschweren. Wenn Organisationen keinen konsolidierten Überblick über Identitätsaktivitäten haben, fällt es ihnen schwer, Frühwarnzeichen wie ungewöhnliche Anmeldeaktivitäten, Missbrauch von Berechtigungen oder Anomalien beim Datenzugriff zu erkennen. Die Stärkung von Überwachung und Sichtbarkeit ermöglicht es Sicherheitsteams, proaktiv statt reaktiv zu reagieren.

Auswirkung:

Eine verzögerte Erkennung böswilliger oder unbefugter Aktivitäten erhöht die Schwere des Vorfalls und kann die Gefährdung verlängern, bevor Abhilfemaßnahmen ergriffen werden.

Minderungsstrategien:

- Security Information and Event Management (SIEM)-Plattformen implementieren
- Funktionen zur Benutzer- und Entitätenverhaltensanalyse (UEBA) nutzen
- Automatisierte Warnmeldungen für anomales Verhalten konfigurieren
- Umfassende Protokollierung sicherstellen und regelmäßige Überprüfungen durchführen

4. Unzureichende Zugriffskontrollen

Unzureichende Zugriffskontrollen entstehen, wenn Mechanismen zur Vergabe, Einschränkung und Überwachung von Benutzerberechtigungen keine angemessenen Grenzen durchsetzen. Dies kann auftreten, wenn Zugriffsrichtlinien schlecht definiert sind, Rollenzuweisungen zu weit gefasst sind oder die Durchsetzung über verschiedene Systeme hinweg inkonsistent erfolgt. Selbst Organisationen mit ausgereiften IAM-Programmen können aufgrund von Altsystemen, Cloud-Integrationen oder dezentraler Administration entsprechende Lücken aufweisen.

Eine schwache Durchsetzung von Zugriffskontrollen erhöht das Risiko unbefugter Zugriffe auf sensible Informationen und kritische Systeme erheblich. Angreifer können solche Schwachstellen ausnutzen, um Berechtigungen auszuweiten, sich lateral durch Netzwerke zu bewegen oder vertrauliche Daten unentdeckt zu exfiltrieren. Ebenso können interne Nutzer unbeabsichtigt auf Ressourcen zugreifen, die über ihren Verantwortungsbereich hinausgehen, wodurch operative, Compliance- und Sicherheitsrisiken entstehen.

Die dynamische Natur moderner IT-Umgebungen - einschließlich Remote-Arbeit, Cloud-Diensten und Integrationen mit Drittanbietern - erschwert zusätzlich die konsistente Anwendung von Zugriffskontrollen und macht eine wirksame Aufsicht unerlässlich.

Organisationen mit unzureichender Durchsetzung von Zugriffskontrollen haben häufig Schwierigkeiten bei Audits und im Reporting. Ohne angemessene Kontrollen wird es herausfordernd, die Einhaltung von Vorschriften wie DSGVO, DORA oder NIS2 nachzuweisen. Der Mangel an granularen, durchsetzbaren Kontrollen reduziert die Effektivität von Überwachungssystemen und schränkt die Fähigkeit ein, abweichendes Verhalten oder Richtlinienverstöße in Echtzeit zu erkennen.

Auswirkung:

Die Nichtbeachtung strenger Zugriffskontrollen kann zu unbefugtem Datenzugriff, Betriebsstörungen, Verstößen gegen Compliance-Vorschriften und einer erhöhten Gefährdung durch interne oder externe Bedrohungen führen.

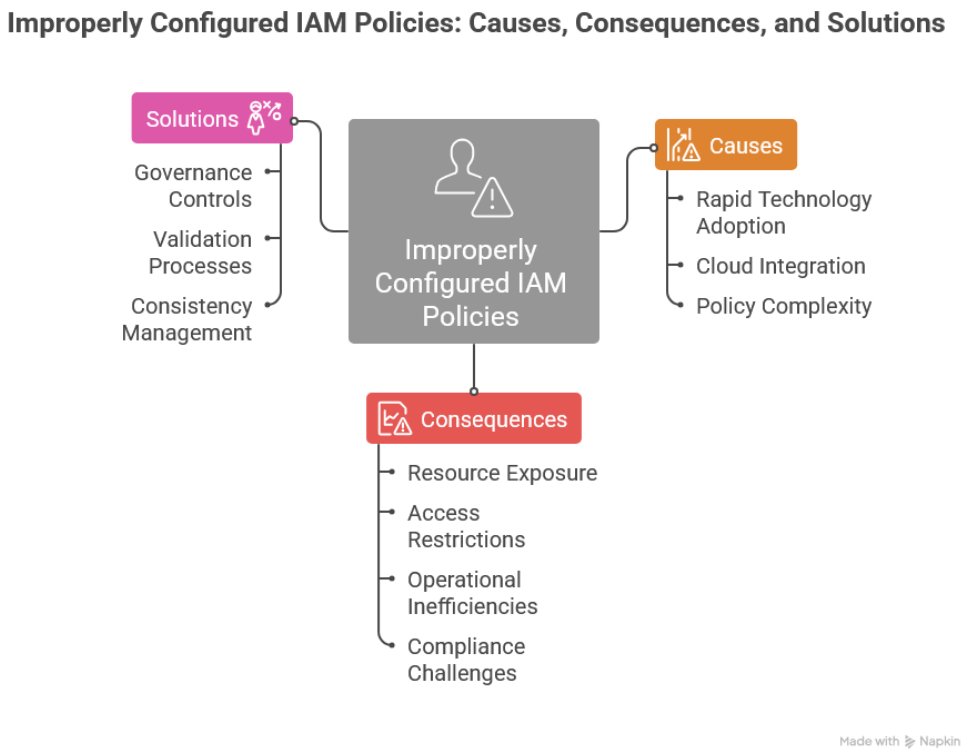
Minderungsstrategien:

- Granulare Zugriffskontrollen implementieren, die Berechtigungen an Aufgabenbereiche und geschäftliche Anforderungen anpassen
- Rollenbasierte und attributbasierte Zugriffsmodelle anwenden, um das Risiko überprivilegierter Zugriffe zu reduzieren
- Zugriffszuweisungen regelmäßig prüfen und auditieren, einschließlich temporärer oder erhöhter Berechtigungen
- Konsistente Kontrollen über alle Systeme hinweg durchsetzen, einschließlich Cloud-, SaaS- und On-Premises-Umgebungen
- Die Durchsetzung von Zugriffskontrollen mit kontinuierlichen Überwachungs- und Anomalie-Erkennung-Tools integrieren

5. Falsch konfigurierte Richtlinien im IAM

Die schnelle Einführung neuer Technologien - insbesondere Cloud-Integrationen - erhöht die Komplexität von Richtlinien und die Wahrscheinlichkeit von Konfigurationsfehlern. Fehlangepasste Konfigurationen können unbeabsichtigt sensible Ressourcen offenlegen oder legitimen Zugriff einschränken, was zu operativen Ineffizienzen und Herausforderungen bei der Compliance führt.

Da Identitätsrichtlinien immer komplexer werden, wird es zunehmend schwieriger, die Konsistenz über verschiedene Umgebungen hinweg zu gewährleisten. Kleine Konfigurationsfehler können sich weitreichend auswirken und mehrere Systeme oder Dienste gleichzeitig beeinträchtigen. Durch die Implementierung von Governance-Kontrollen und Validierungsprozessen kann sichergestellt werden, dass die Richtlinien weiterhin mit den Sicherheitsanforderungen und Geschäftszielen übereinstimmen



Auswirkung:

Fehlerhafte Richtlinien können zu unbefugter Offenlegung von Ressourcen oder zu Störungen legitimer Geschäftsprozesse führen, was sich potenziell auf die Verfügbarkeit von Diensten oder die Einhaltung regulatorischer Vorgaben auswirkt.

Minderungsstrategien:

- Automatisierte Tools zur Richtlinienvalidierung und Compliance nutzen
- Follow configuration governance best practices
- Beste Praktiken der Konfigurations-Governance befolgen
- Genaue Dokumentation von Richtlinienstrukturen und Änderungen pflegen

6. Schwache Kontrolle privilegierter Benutzerkonten

Privilegierte Konten - also solche mit administrativen oder erweiterten Zugriffsrechten - gehören zu den kritischsten Vermögenswerten im Identitäts-Ökosystem einer Organisation. Eine schwache Verwaltung dieser Konten erhöht das Risiko schwerwiegender Sicherheitsvorfälle erheblich. Zu privilegierten Konten zählen Systemadministratoren, Datenbankmanager, Service-Konten und Cloud-

Administratoren, die alle auf sensible Daten zugreifen, Konfigurationen ändern und standardmäßige Sicherheitskontrollen umgehen können.

In vielen Organisationen werden privilegierte Konten nur unzureichend überwacht, von mehreren Nutzern gemeinsam verwendet oder behalten dauerhaft erhöhte Rechte, die nicht regelmäßig überprüft werden. Dies eröffnet Möglichkeiten für böswillige Insider, kompromittierte Zugangsdaten oder externe Angreifer, laterale Bewegungen durchzuführen und Kontrolle über kritische Systeme zu erlangen. Die Auswirkungen eines kompromittierten privilegierten Kontos sind oft exponentiell größer als bei einem Standardbenutzerkonto, da Angreifer vorhandene Sicherheitsmechanismen umgehen und vertrauenswürdige Identitäten über längere Zeiträume ausnutzen können.

Die Herausforderung des Managements privilegierter Konten wird in hybriden und Cloud-Umgebungen noch verstärkt. Administratoren verwalten häufig mehrere Umgebungen mit inkonsistenten Richtlinien, temporäre Service-Konten nehmen zu, und Integrationen mit Drittanbieterdiensten schaffen neue Zugriffswege. Ohne zentrale Governance und kontinuierliche Überwachung verlieren Organisationen den Überblick darüber, wer über erhöhte Zugriffsrechte verfügt und ob diese angemessen genutzt werden.

Eine unzureichende Verwaltung privilegierter Konten erhöht zudem das regulatorische und Compliance-Risiko. Rahmenwerke wie NIST, ISO 27001 und PCI DSS betonen die strikte Kontrolle privilegierter Zugriffe, einschließlich regelmäßiger Überprüfungen, Trennung von Aufgabenbereichen und Audit-Logging. Das Versäumnis, diese Anforderungen durchzusetzen, kann zu Compliance-Verstößen, Strafen und Reputationsschäden führen.

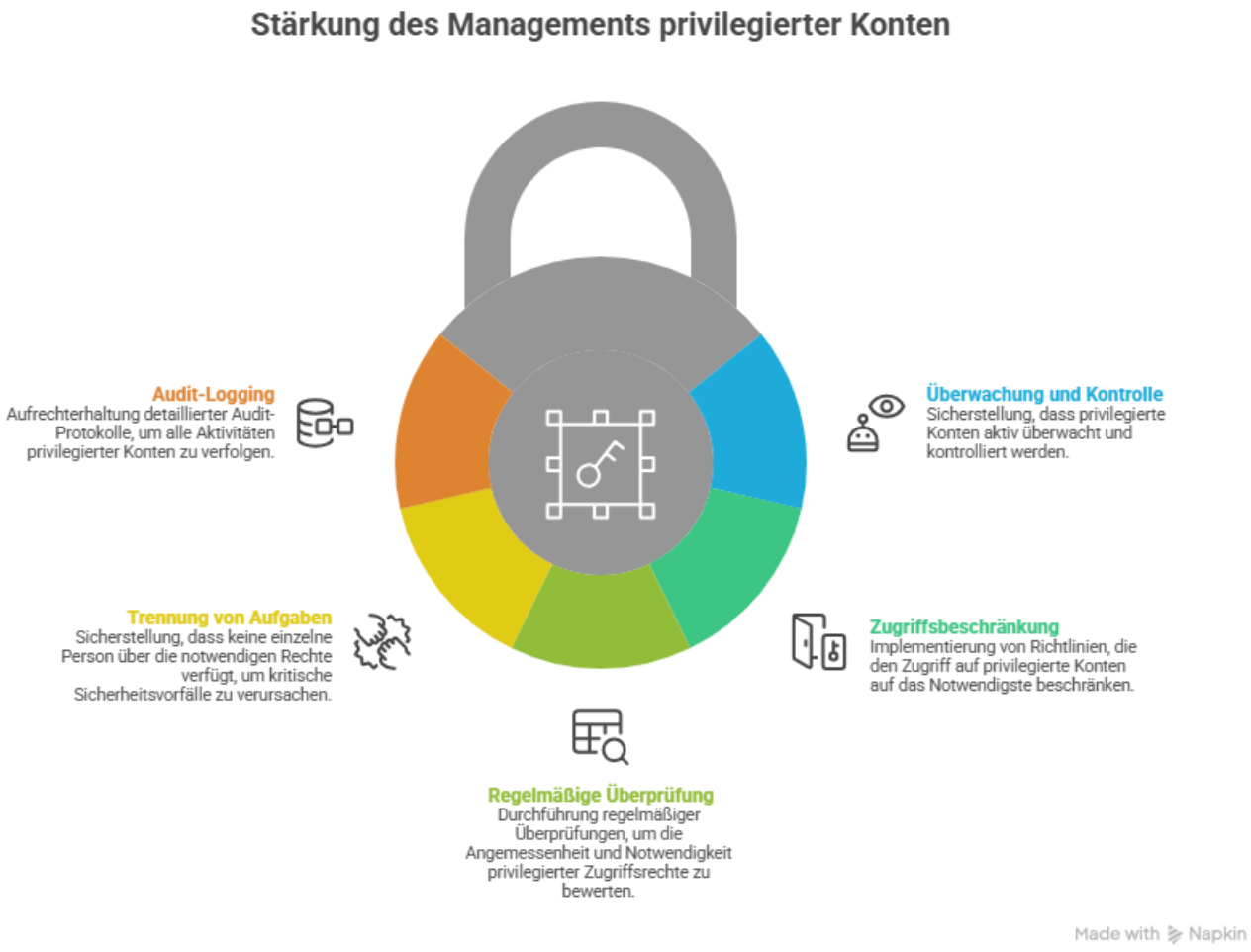
Auswirkung:

- Erhöhtes Risiko großflächiger Sicherheitsvorfälle durch kompromittierte privilegierte Konten
- Erhöhtes Potenzial für unbefugte Konfigurationsänderungen oder Datenexfiltration
- Erhöhte Wahrscheinlichkeit, regulatorische Audits oder Kontrollen nicht zu bestehen
- Eingeschränkte Fähigkeit, abweichendes Verhalten in Echtzeit zu erkennen oder darauf zu reagieren

Minderungsstrategien:

- Privileged Access Management (PAM)-Lösungen implementieren, um die Kontrolle zu zentralisieren und die Nutzung lückenlos zu überwachen.

- Das Prinzip der minimalen Rechte („Least Privilege“) durchsetzen, indem erhöhte Berechtigungen nur bei Bedarf und zeitlich begrenzt gewährt werden
- Zugangsdaten regelmäßig ändern und für jedes privilegierte Konto eindeutige Anmeldedaten verlangen
- Multi-Faktor-Authentifizierung (MFA) für alle privilegierten Konten aktivieren
- Detaillierte Audit-Logs führen und kontinuierliche Überwachung aller Aktivitäten privilegierter Konten durchführen
- Überwachung privilegierter Konten mit Security Information and Event Management (SIEM)- und Benutzerverhaltensanalyse-Plattformen (UEBA) integrieren, um Anomalien in Echtzeit zu erkennen



❖ Stärkung des IAM durch proaktives Risikomanagement

Identity and Access Management (IAM) ist entscheidend für den Schutz sensibler Daten und Systeme. Gleichzeitig sehen sich Organisationen zahlreichen Risiken ausgesetzt, darunter überprivilegierte Konten, schwache Passwort-Richtlinien, falsch konfigurierte Zugriffsrechte, Shadow IT sowie unzureichende Kontrollen privilegierter Konten. Jeder dieser Faktoren kann die Wahrscheinlichkeit von Sicherheitsverletzungen, Betriebsunterbrechungen und Compliance-Verstößen erhöhen.

Der Schlüssel zur Minimierung dieser Risiken liegt im proaktiven IAM-Management. Organisationen sollten klare Richtlinien durchsetzen, Zugriffsrechte regelmäßig überprüfen, starke Authentifizierung implementieren und die Benutzeraktivitäten kontinuierlich überwachen. Die Integration von IAM mit Tools wie SIEM und Privileged Access Management stellt sicher, dass Bedrohungen schnell erkannt und adressiert werden.

IAM ist nicht nur eine technische Funktion, sondern auch ein strategisches Sicherheitsinstrument. Durch eine effektive Verwaltung von Identitäten und Zugriffsrechten können Organisationen Daten schützen, Compliance sicherstellen, operative Risiken reduzieren und Vertrauen bei Mitarbeitern, Partnern und Kunden aufbauen. Wenn IAM als Priorität behandelt wird, trägt dies dazu bei, Sicherheitsvorfälle zu verhindern und ein sicheres, verlässliches Unternehmenswachstum in der heutigen digitalen Welt zu unterstützen.

Tel.: +49 (0) 23 23 - 9 87 97 96

Lothringer Straße 36, 44805 Bochum

E-Mail: info@patecco.com

www.patecco.com