CYBERARK®
The Identity Security Company

Least-Privilege-Prinzipien durch ein innovatives Identity Management stärken

Von Gil Rapaport

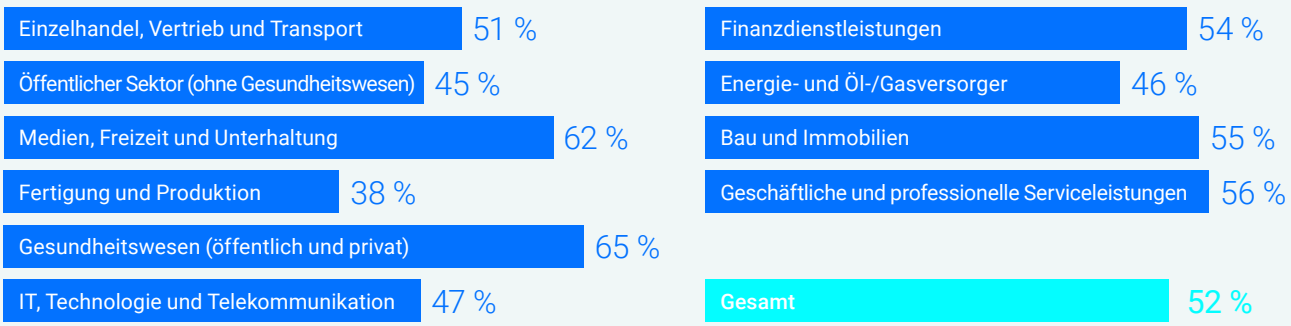
General Manager, Identity and Access, CyberArk

Die Definition von privilegierten Berechtigungen ändert sich, und das ändert alles.

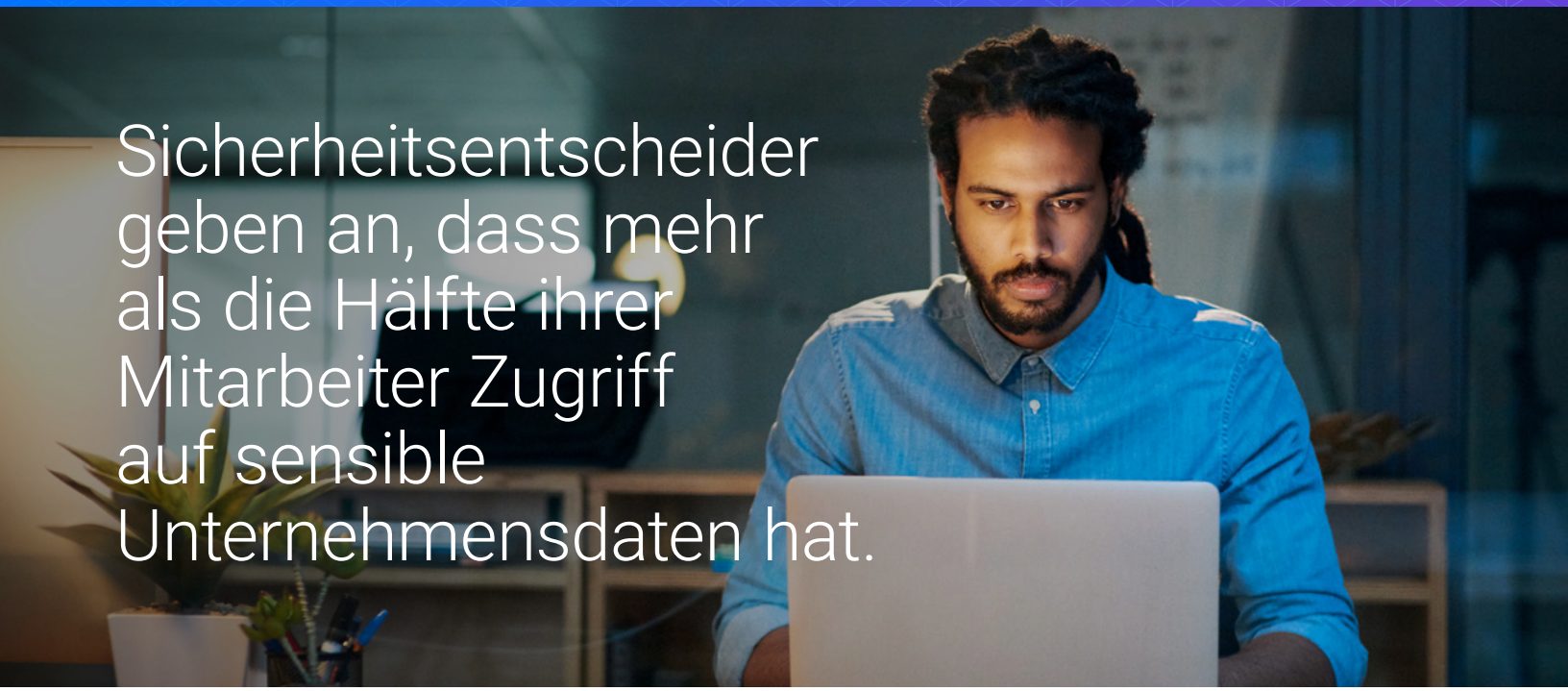
Identitäten aller Art – nicht nur Mitglieder des IT-Teams, sondern alle Mitarbeiter – erhalten Zugriff auf sensible Daten, Infrastruktur und Systeme, die Angreifer heute leicht ausnutzen können. Eine Befragung von 1.500 IT- und Sicherheitsentscheidern ergab, dass im Durchschnitt mehr als die Hälfte ihrer Mitarbeiter Zugriff auf sensible Unternehmensdaten hat.

Die Verwaltung digitaler Identitäten – von der Erteilung, Anpassung und dem Entzug von Berechtigungen bis hin zur Einhaltung von Audits – ist von entscheidender Bedeutung. Aber das ist nicht einfach. Die Anzahl der Identitäten, die Ihren Schutz erfordern, nimmt zu, da die digitalen und Cloud-Initiativen Ihres Unternehmens in Umfang und Größe zunehmen.

Aufteilung nach Branchen: Durchschnittlicher Prozentsatz der Mitarbeiter, die Zugriff auf sensible Unternehmensdaten erhalten



Quelle: Cyberark Identity Security Threat Landscape Report 2022



Sicherheitsentscheider geben an, dass mehr als die Hälfte ihrer Mitarbeiter Zugriff auf sensible Unternehmensdaten hat.

Wir arbeiten mit CIOs, CISOs und Sicherheitsentscheidern in Tausenden von Unternehmen in über 100 Ländern zusammen und wissen, dass Sie unter Druck stehen, Ihre Identitäten in einer Zeit zu verwalten und zu schützen, in der die folgenden als häufige Probleme genannt werden:

- **Viele Betriebe sind mit zeitaufwendigen manuellen Prozessen, veralteten Verfahren und Silos über Anwendungen, Directory-Stores und Datenrepositorys hinweg überfordert.**
- **Mit den zunehmenden Risiken steigen auch die Arbeitsbelastung, die Arbeitszeit und der Stresspegel.** Gleichzeitig verschärft der wirtschaftliche Druck die anhaltenden Ressourcen- und Qualifikationsdefizite.

Um Least-Privilege-Prinzipien wirklich durchzusetzen, benötigen IT- und Sicherheitsteams Kontrollen, die alle Arten von Identitäten mit leistungsstarkem Zugriff abdecken – von den IT-Administratoren der Welt bis hin zu Mitarbeitern mit erweiterten Privilegien. Das bedeutet, dass Unternehmen überdenken müssen, welche Bedeutung Identity Management hat – und was es leisten können muss. Sie benötigen Klarheit über den Zweck und die parktische Umsetzung.

1

2

3

IN DIESEM BEITRAG BESPRECHE ICH DIE SCHRITTE, DIE SIE UNTERNEHMEN KÖNNEN, UM DIE FÄHIGKEITEN IHRES TEAMS IN DREI BEREICHEN ZU STÄRKEN:

1 | Automatisierung und Orchestrierung von Zugriffsberechtigungen über den gesamten Identitätslebenszyklus hinweg

2 | Einrichtung unternehmensweiter Compliance-Kontrollen und Berichterstattung

3 | Erweiterung der Kontrollen, die Sie zur Sicherung privilegierter Benutzer verwenden, auf alle Identitäten

1. Automatisierung und Orchestrierung von Zugriffsberechtigungen über den gesamten Identitätslebenszyklus

Wie Sie wissen, umfasst die Durchsetzung der geringsten Privilegien nicht nur die Einschränkung des Zugriffs, sondern auch die Vergabe der minimalen Berechtigungen, die Benutzer für ihre Arbeit benötigen. Das Problem ist, dass manuelle, fehleranfällige Prozesse viele Unternehmen daran hindern können, den Identitätslebenszyklus ihrer Mitarbeiter sicher zu verwalten.

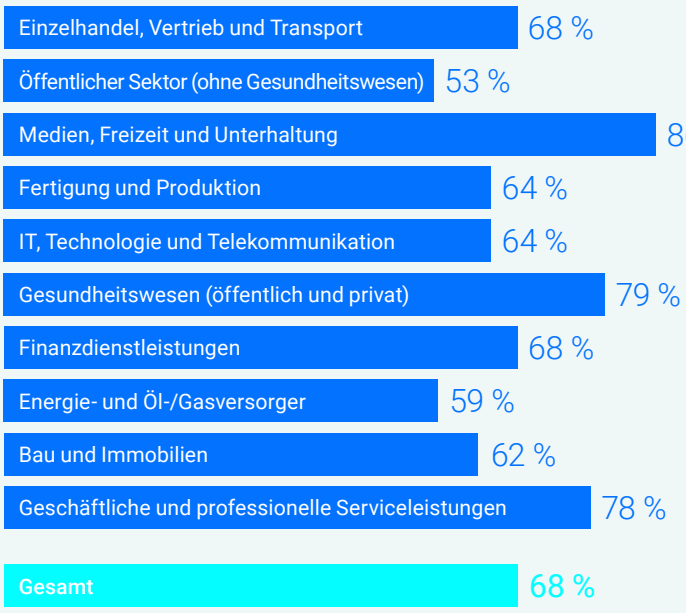
Zu Beginn warten neue Mitarbeiter oft Tage oder Wochen auf die Bereitstellung des Zugriffs auf die von ihnen benötigten Applikationen, Dienste und IT-Systeme. Irgendwann kann Ungeduld dazu führen, dass Arbeitnehmer nach anderen Wegen suchen, um Zugang zu erhalten, einschließlich der Einführung von Schatten-IT.

Aber überlegen Sie, was passieren könnte, wenn ein IT- oder Sicherheitsteammitglied einen kritischen Schritt in einem manuell ausgeführten Workflow vergisst. Wenn beispielsweise ein Mitarbeiter das Unternehmen verlässt, muss das IT-Team möglicherweise eine Checkliste mit Anwendungen durchgehen, bei denen er den Zugriff einzeln manuell entfernen muss.

Welche Risiken gibt es?

Ein verpasster Schritt lässt Bedrohungsakteuren die Tür offen, um falsch bereitgestellte, überprivilegierte oder verwaiste Konten auszunutzen – und Angreifer tun dies routinemäßig.

Aufteilung nach Branchen: IT- und Sicherheitsentscheider glauben, dass eine beschleunigte Mitarbeiterabwanderung und Fluktuation zu Sicherheitsproblemen geführt haben (z. B. durch Nichtentzug von Zugriffsrechten der Benutzer)



Quelle: Cyberark Identity Security Threat Landscape Report 2022

Die Daten für Anfang und Ende der Mitarbeitertätigkeit sind zwar wichtig, aber reichen nicht entfernt für ein kontinuierliches Identitätslebenszyklusmanagement. Um Least-Privilege-Prinzipien für Mitarbeiter während ihrer gesamten Betriebszugehörigkeit in Ihrem Unternehmen zu gewährleisten, ist Folgendes erforderlich:

- Monate, Jahre und sogar Jahrzehnte der Verfolgung und Neuzuweisung von Privilegien pro Benutzer.
- Bereitstellung und Sperrung von Zugriffen, wenn sich Jobrollen und Systeme ändern – und wenn die Anzahl der Applikationen wächst.
- Sicherstellen, dass das breite Spektrum der beteiligten Zielanwendungen synchron bleibt.

In einer Zeit, in der Privilegien überall vorhanden sind – einschließlich der Fähigkeit der Mitarbeiter, riskante Maßnahmen in Geschäftsanwendungen mit sensiblen Daten zu ergreifen – erfordern diese Identity Management-Grundlagen ein neues Konzept.

Der Grund dafür ist, dass die meisten Unternehmen in einem Muster verharren, bei dem die Punkte manuell miteinander verbunden und Skript-Integrationen zwischen Daten, Anwendungen, Ereignissen und Diensten vorgenommen werden. Und vielen Unternehmen fehlen formelle Verfahren oder konsistente Workflows für die Neubewertung, Anpassung oder Aufhebung der Zugriffe und Privilegien von Benutzern.

Hier sind einige Schritte, die Sie unternehmen können, um einen sicherheitsorientierten Ansatz für die Verwaltung von Identitäten vom Anfangsdatum eines Benutzers bis zum letzten Tag zu entwickeln:

Zentralisieren Sie Ihre Lebenszyklusmanagement-Richtlinien, -Kontrollen und -Fähigkeiten mithilfe automatisierter Arbeitsabläufe für:

- Onboarding und Offboarding von Mitarbeitern.
- Definition und Durchsetzung der individuellen Rollen, Verantwortlichkeiten, Zugriffsrechte und Berechtigungen jedes Benutzers.

Dieser Ansatz kann Ihr Team von sich wiederholenden, fehleranfälligen Aufgaben befreien. Durch die Integration dieser Prozesse in Ihre vertrauenswürdige HR-Software können Sie die Konsistenz und Genauigkeit zwischen den Plattformen aufrechterhalten.

Verbinden Sie Identitäten in Cloud- und On-Premise-Applikationen und -Systemen, damit Ihr Team:

- schnell Zugriff, wenn Benutzer ihn benötigen, ermöglichen kann.
- Anpassungen vornehmen kann, wenn sich Rollen oder Risiken ändern.
- Benutzer entfernen, wenn sie das Unternehmen verlassen.

Automatisierte Arbeitsabläufe können Ihnen dabei helfen, das Verschleiern von Privilegien und verwaisten Accounts zu verhindern, die Angreifer häufig ausnutzen, um Angriffe zu starten, Daten zu stehlen und vieles mehr.

Erhalten Sie Echtzeit-Einblicke in potenzielle Risiken – und die Fähigkeit, darauf zu reagieren – basierend auf automatisierten Tools, die Folgendes verfolgen:

- Verwendung von Anwendungen.
- Fehlgeschlagene Anmeldeversuche.
- Nicht genutzte Konten.
- Externe Bedrohungsdaten.

MEHR TUN, WENIGER CODIEREN

Viele Unternehmen, die ihr Identity Management automatisieren möchten, sind auf komplexes Coding und Skripting angewiesen, was spezielle Fähigkeiten zur Entwicklung und Instandhaltung erfordert.

Dieser Ansatz ist weder sicher noch nachhaltig. Die Aktualisierung der Codes kann spröde, veraltet und kostspielig sein, da der Autor mit einer überfüllten Warteschlange von IT-Anfragen konfrontiert ist.

Visuelle Editoren ohne Code mit vorkonfigurierten Konnektoren können Unternehmen helfen:

Orchestrieren Sie Identitätsereignisse.

Erstellen Sie Workflows, die Schutz und Produktivität ermöglichen.

Synchronisieren Sie Identitätsdaten über Applikationen, Directory-Speicher und Repositorys hinweg.

Dieses Konzept bietet Ihnen eine skalierbare Form der Transparenz und Kontrolle durch automatisierte Arbeitsabläufe, die darauf ausgelegt sind, riskante Handlungen von Benutzern und Angriffsversuche zu verhindern.

2. Einrichtung unternehmensweiter Compliance-Kontrollen und -Berichte

Zusätzlich zum Schutz des Unternehmens verwalten IT- und Sicherheitsteams häufig einen oder mehrere der folgenden Bereiche:

- Sicherstellen von Transparenz für interne Sicherheitsüberprüfungen
- Einhalten komplexer Branchen- und Regierungsvorschriften
- Entsprechen der Anforderungen von Audits und Compliance

Sicherstellen und Nachweisen von Compliance ist für viele Unternehmen ein Problem. Die Arbeit, die mit der Einhaltung von Vorschriften, der Erfüllung von Berichterstattungsanforderungen und der Vermeidung von Sanktionen verbunden ist, wächst, ähnlich wie Ihre Identitäten.

Dies führt uns zu einem Schlüsselelement der Durchsetzung von Least-Privilege-Prinzipien: die Verwaltung von zugriffsbezogenen Prüfungen und Zertifizierungen.

Die Risiken eines unkontrollierten Zugriffs, verwaister Konten und des Verschleierns von Privilegien sind weitreichend. Überlegen Sie sich nicht nur die Auswirkungen eines Verstoßes selbst, sondern auch, was die Nichteinhaltung von Vorschriften für Ihren Betrieb bedeuten kann. Allein die Europäische Union hat für Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) Geldbußen in Höhe von ca. 1,25 Milliarden Euro verhängt.

Wie erhalten Sie die Transparenz und Kontrolle, die Sie benötigen, um sicherzustellen, dass die Weiterentwicklung von Privilegien Ihr Unternehmen nicht gefährdet?

Diese Frage bezieht sich auf eine Vielzahl von Identitäten, darunter:

- Die potenziell riskanten Maßnahmen, die Mitarbeiter innerhalb von Applikationen mit sensiblen Daten ergreifen können.
- Die Berechtigungen, die Ihre privilegierten Benutzer haben, um auf Safes und privilegierte Konten zuzugreifen.
- Die Autorisierungen und Berechtigungen, die Ihre Entwickler und Operations Teams in Cloud-Umgebungen haben.

BERECHNUNG DER COMPLIANCE-HERAUSFORDERUNG

Die Sicherstellung und der Nachweis der Einhaltung globaler Vorschriften ist ein Kampf für Sicherheitsteams.

156

Staaten (80 % der Welt) haben Gesetze zur Bekämpfung der Cyberkriminalität erlassen.[1]

Mehr als 130

Staaten auf der ganzen Welt haben Datenschutzgesetze erlassen[2]

Nur 9 %

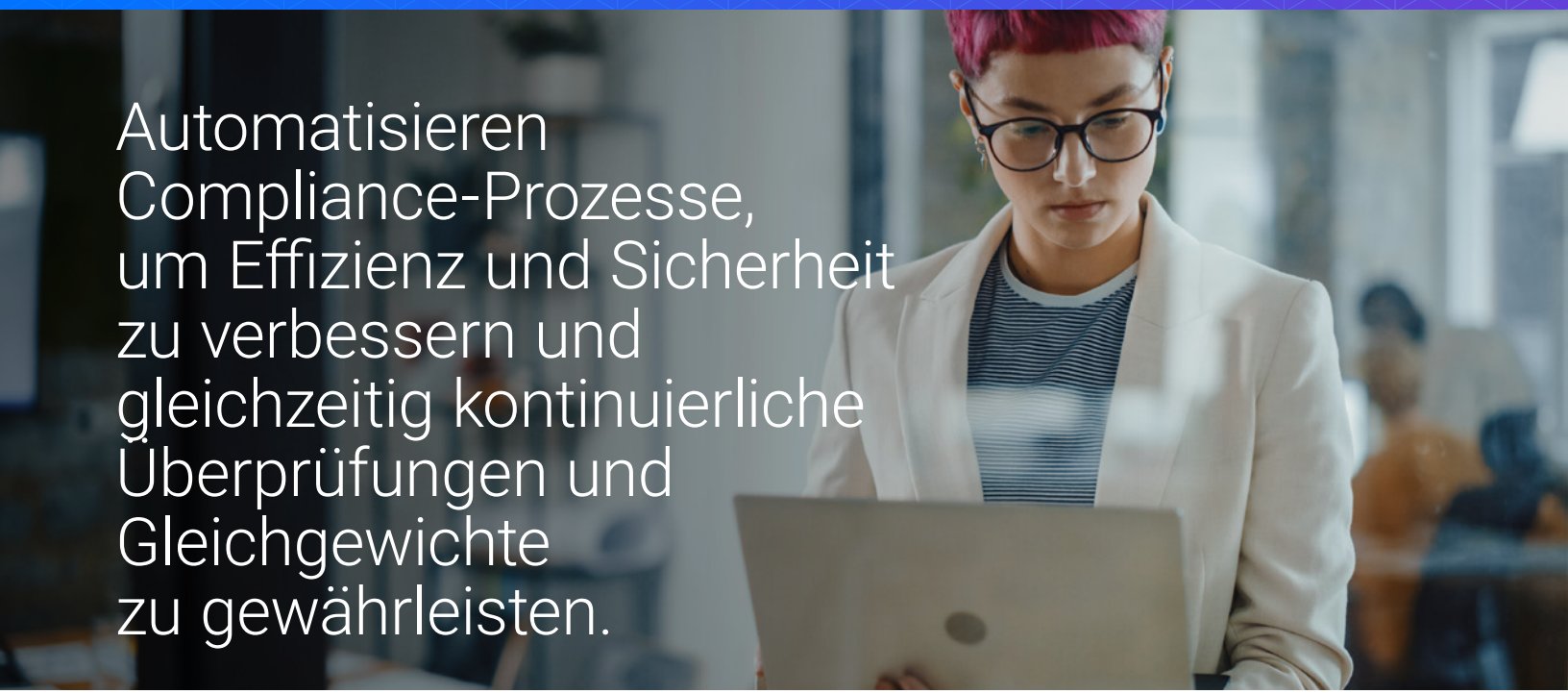
der Führungskräfte sind sehr zuversichtlich, dass sie alle Offenlegungsanforderungen effektiv erfüllen können. [3]

Mehr als die Hälfte (58 %) der Befragten sind sich nicht sicher, dass sie folgendes gewährleisten können:

Die geforderten Angaben zu wichtigen Vorfällen innerhalb der vorgeschriebenen Fristen zu liefern.[4]

Die Wesentlichkeit von Cyber-Vorfällen für die Berichterstattung zu beurteilen.[5]

[1] Cybercrime Legislation Worldwide, United Nations Conference on Trade and Development, 2022
[2] A Look Ahead at New Data Privacy Regulations: How Do They Compare to ISO/IEC 27701? ISACA, 2022
[3,4,5] Global Digital Trust Insights Survey, PWC, 2022



Automatisieren Compliance-Prozesse, um Effizienz und Sicherheit zu verbessern und gleichzeitig kontinuierliche Überprüfungen und Gleichgewichte zu gewährleisten.

Wenn es um Audits geht, gibt es viel zu beweisen – von den Richtlinien, die Sie verwenden, um Least-Privilege-Prinzipien durchzusetzen, bis hin zum Nachweis, dass Sie dies effektiv getan haben. Ein sicherheitsorientierter Ansatz kann helfen:

- **Schaffen** Sie eine einheitliche Übersicht darüber, wer Privilegien und Autorisierungen für welche Ressourcen hat, mit Möglichkeiten zur Erkennung, Anpassung, Zertifizierung und Entzug des Zugriffs.
- **Automatisieren** Sie Compliance-Prozesse, um die Effizienz und Sicherheit zu verbessern und gleichzeitig kontinuierliche Prüfungen und Abgleiche zu gewährleisten – zum Beispiel, um sicherzustellen, dass der Zugriff regelmäßig überprüft und zertifiziert wird.
- **Befähigen** Sie Ihr Team und Ihre Prüfer mit Analyse- und Berichtsfunktionen, um potenzielle Compliance-Probleme zu identifizieren, detaillierte Audit-Trails zu bieten und benutzerdefinierte Berichte zu ermöglichen.
- **Integrieren** Sie Compliance-Tools in Ihr gesamtes Framework für Identity Security, das dazu beitragen kann, Silos zu verhindern und die Compliance aller Identitäten, einschließlich privilegierter oder administrativer Konten, zu gewährleisten.

LEAST-PRIVILEGE-PRINZIP DURCH IDENTITY SECURITY ERREICHEN

Die in diesem Artikel besprochenen Best Practices sind alle Bestandteile eines ganzheitlichen Modells für Identity Security.

Identity Security konzentriert sich auf intelligente Privilegienkontrollen und kann menschliche und maschinelle Identitäten nahtlos sichern, die auf Applikationen, Infrastruktur und Daten zugreifen, und den Identitätslebenszyklus flexibel automatisieren – alles mit einem einheitlichen Konzept.

Identity Security ermöglicht Zero Trust, indem sie Least-Privilege-Prinzipien mit kontinuierlicher Erkennung und Schutz von Identitätsbedrohungen durchsetzt.

3. Erweiterung intelligenter Privilegienkontrollen auf Identity Management für alle Benutzer

Wie setzen Sie die geringsten Privilegien durch, wenn Privilegien überall vorhanden sind?

Zunächst einmal können Benutzer mit Zugriff auf privilegierte Konten zunehmen, wenn die Digital- und Cloud-Initiativen Ihres Unternehmens wachsen – zum Beispiel DevOps-Teams und Site Reliability Engineers. Da jedoch mehr Mitarbeiteridentitäten denn je Zugang zu Daten mit hohem Risiko erhalten, ist klar, dass die Identitäten aller Benutzer strengen Schutz benötigen.

Mit der Verbreitung von Identitäten nehmen auch die Bedrohungen zu, die sie gefährden. Was in vielen Fällen *nicht* wächst, sind die Mittel, die Sie für die Sicherung dieser Ressourcen bereitstellen können. Auch hier erfordert das Zusammentreffen von wirtschaftlichem Druck, angespannten Teams und schnell auftretenden Risiken einen neuen Ansatz.

Sie können diese Herausforderung angehen, indem Sie:

1. Intelligente Privilegienkontrollen, die Sie von Ihrem PAM-Programm kennen und denen Sie vertrauen, auf jede Art von Identität in Ihrem Unternehmen erweitern.
2. Neue Konzepte für das Identity Management anwenden, um die Compliance privilegierter Benutzer zu gewährleisten und die Bandbreite Ihres Teams durch die Automatisierung komplexer PAM-Aufgaben wiederherzustellen.

Die Best Practices, die wir in diesem Artikel besprochen haben, kommen alle ins Spiel. Ähnlich wie bei einem klassischen Defense-in-Depth-Framework können Sie Ihrem PAM-Programm zusätzliche Sicherheits- und Effizienzebenen hinzufügen, die Ihr Team an den bestmöglichen Ort bringen können, um Least-Privilege-Prinzipien durchzusetzen.

HIER SIND ZWEI BEREICHE, DIE SIE IM RAHMEN DES IDENTITY MANAGEMENTS UNTERSTÜTZEN KÖNNEN:

1 | Compliance: Stellen Sie die Compliance für privilegierten Zugriff im gesamten Unternehmen durch Fähigkeiten sicher, die wir im vorherigen Abschnitt untersucht haben. Suchen Sie nach Kontrollen und Tools, um Benutzer zu ermitteln, die Zugriff auf bestimmte Safes und privilegierte Konten in Ihrem PAM-Programm haben. Setzen Sie Least-Privilege-Prinzipien mit Überprüfungen und Zertifizierungen, die für wiederkehrende Daten geplant sind, kontinuierlich durch. Nachweis der Konformität mit detaillierten Analysen und Berichten.

2 | Workflow-Automatisierung: Vereinfachen Sie komplexe PAM-Prozesse, die Ihr Team ausbremsen. Suchen Sie nach Tools, die eine No-Code-Automatisierung bieten, nicht nur für das Lebenszyklusmanagement, sondern auch für Prozesse wie die Erstellung von Service Accounts mit Administratorrechten. Suchen Sie auch nach Möglichkeiten, das IT-Ticketmanagement zu automatisieren und eine skalierbare Erfüllung in ITSM-Tools zu ermöglichen.

Um das Beste aus Ihren PAM-Investitionen herauszuholen, müssen Sie auch bewährte Kontrollen zum Schutz der Anmeldedaten und Sessions privilegierter Benutzer durchführen und diese Kontrollen auf Ihre gesamte Belegschaft anwenden. Mit dem richtigen Ansatz und den richtigen Tools erreichen Sie:

- **Passwortsicherheit auf Unternehmensniveau:** Nutzen Sie Vaults und Just-in-Time-Zugriff, um sicherzustellen, wie Mitarbeiter Passwörter für Anwendungen speichern, abrufen und weitergeben, die nicht mit Single Sign-on integriert sind.
- **Session Protection für Geschäftsanwendungen:** Integrieren Sie Überwachungs-, Aufzeichnungs- und Audit-Fähigkeiten in die Sitzungen von Mitarbeitern, die riskante Maßnahmen in Geschäftsanwendungen mit sensiblen Daten ergreifen können.

Fazit:

Meine persönlichen Erfahrungen in der Zusammenarbeit mit dem CyberArk Team bei der Unterstützung von Kunden und der Entwicklung von Lösungen für den Schutz all ihrer Unternehmen sind die Grundlage für diese Empfehlungen.

Unternehmen benötigen Betriebseffizienz, um zu wachsen und sich zu transformieren. Sie brauchen Produktivität, um wettbewerbsfähig zu sein. Und sie benötigen eine hochwertige Benutzererfahrung, um sicherzustellen, dass die Benutzer nicht nur produzieren, sondern sich auch motiviert fühlen.

Aber ohne Sicherheit kann alles, an dem ein Unternehmen gearbeitet hat, durch einen einzigen Verstoß, einen Anschlag, eine Geldbuße oder einen Fehler bei etwas so Einfachem wie der Kodierung eines Arbeitsablaufs für die Bereitstellung verringert werden.

Wir möchten Ihnen helfen, erfolgreich zu sein, indem wir dazu beitragen, solche Ergebnisse zu verhindern, und indem wir einen Ansatz für Identity Security entwickeln, der Folgendes kann:

- Risiken messbar reduzieren
- Betriebseffizienz ermöglichen
- Anforderungen von Audits und Compliance entsprechen

SPRECHEN SIE MIT UNS

Wenn Sie mit einem Experten von CyberArk Kontakt aufnehmen möchten, um die Anforderungen Ihres Unternehmens beim Identity Management zu besprechen, wenden Sie sich an uns.

VEREINBAREN SIE EIN GESPRÄCH

MEHR ERFAHREN

Mehr über CyberArk Lösungen für das Identity Management erfahren Sie auf folgenden Seiten:

LEBENSZYKLUSMANAGEMENT

AUTOMATISIERUNG VON IDENTITY-WORKFLOWS

COMPLIANCE UND BERICHTERSTATTUNG

GIL RAPAPORT, General Manager, Identität und Zugriff, CyberArk

CYBERARK®
The Identity Security Company