Cyber Resilience in Zeiten des Identitätswildwuchses

So kann Ihnen eine vereinheitlichte Identitätssicherheit dabei helfen, kritische Sicherheitslücken zu schließen und Zero-Trust-Initiativen zu unterstützen

ONE IDENTITY by Quest

Sie sind CISO und Ihre Bedenken bezüglich der Cybersicherheit, die Sie dem Vorstand gegenüber zum Ausdruck gebracht haben, sind angesichts der gesamtwirtschaftlichen Herausforderungen, der Komplexität der Pipeline und der Notwendigkeit, den Remote-Zugriff drastisch zu erhöhen, größtenteils untergegangen.

Es ist Samstagmorgen und Ihr Diensthandy klingelt in Ihrem Homeoffice.

Warum schickt Ihnen der Leiter der IT-Sicherheit Textnachrichten und ruft Sie gleichzeitig an?

„Das kann nichts Gutes bedeuten", denken Sie sich.

Tut es auch nicht.

Es hat einen Cyberangriff gegeben. Das Ausmaß ist noch unbekannt, aber der Leiter der IT-Sicherheit erklärt Ihnen, dass seine Mitarbeiter den Vorfall untersuchen.

Ihnen schießen mehrere Fragen durch den Kopf:

- Wie sind die Angreifer hineingekommen?
- War ein interner Mitarbeiter an dem Angriff beteiligt?
- Auf wie viele vertrauliche Informationen wurde zugegriffen?
- Wie soll ich das dem Vorstand erklären?
- Wird sich dieser Vorfall positiv oder negativ auf das von mir vorgeschlagene Budget für Cybersicherheit für das nächste Finanzjahr auswirken?
- Muss ich meinen Lebenslauf auf den neuesten Stand bringen?

Es hat einen Cyberangriff gegeben. Das Ausmaß ist noch unbekannt, aber der Leiter der IT-Sicherheit erklärt Ihnen, dass seine Mitarbeiter den Vorfall untersuchen.

Das Risiko des Identitätswildwuchses

Ihr Unternehmen ist Opfer des Identitätswildwuchses geworden.
Es handelt sich um ein schleichendes Sicherheitsrisiko, das oft entsteht, wenn Unternehmen immer mehr Konten verwalten müssen. Immer mehr Konten entstehen, weil neue Technologien zur Unterstützung der Produktivität eingesetzt werden, die zahlreiche neue Benutzerkonten mit sich bringen.

Es schien eine gute Idee zu sein, das Unternehmen mit Ressourcen zu unterstützen, die die Ausführung der täglichen Aufgaben verbessern. Das Problem dabei: Jedes neue System, jede App oder Datenbank, mit der sich Ihre Benutzer verbinden, hat seine eigenen Anforderungen und bedarf eines spezifischen Umgangs mit Anmeldedaten. Manche haben strenge Vorgaben, andere weniger strenge. Manche sind sicher, andere weniger. Manche sind besser. Viele sind schlechter. Häufig hat man keinen Überblick, wer Zugriff hat und was damit getan wird.

Darüber hinaus kommt noch dazu, dass Administratoren privilegierten Remote-Zugriff auf die Systeme benötigen, und dass externe Benutzer verwaltet werden müssen, die sich mit jeglicher Art von Gerät oder Betriebssystem anmelden und dafür verschiedene Browser verwenden. So versucht man also immer mehr Konten, Identitäten und Kennwörter irgendwie unter Kontrolle zu bekommen.

Dieses Phänomen nennt sich Identitätswildwuchs.

Welche Maßnahmen ergreifen Sie, um diesen Wildwuchs zu kontrollieren, in den Griff zu bekommen und ein gesundes Gleichgewicht aus Produktivität und Sicherheit zu gewährleisten?

Im Folgenden finden Sie einen allgemeinen Überblick zum Thema Identitätswildwuchs. Er behandelt das Verschwinden des herkömmlichen Sicherheitsperimeters und Sie erfahren, wie Sie Cyber Resilience verbessern und ein Zero-Trust-Modell erfolgreich umsetzen können. Es geht um einen ganzheitlichen Ansatz und wie eine vereinheitlichte Plattform für Identitätssicherheit Ihr Unternehmen und seine Reputation schützen kann.

Gründe für den Identitätswildwuchs

Wie oben beschrieben, entwickelt sich die IT-Landschaft stetig weiter. Dies hat beträchtliche Auswirkungen darauf, wie Unternehmen sich schützen müssen, um Cyber Resilience zu erreichen. In dieser Situation ist es nicht leicht, immer auf dem Laufenden zu bleiben. Folgende Herausforderungen müssen Sicherheitsexperten jetzt bewältigen:

- Das rasante Verschwinden herkömmlicher Büros und Infrastrukturen
- Verteilte Arbeitsstandorte, denn sie sind keine vorübergehende Erscheinung. Immer mehr Mitarbeiter arbeiten von zu Hause aus oder an Remote-Standorten
- Den Einsatz von Partnern und Auftragnehmern zur Skalierung und Effizienzsteigerung
- Neue Plattformen und Technologien, die eingeführt werden, um Remote-Zugriff und ein unkonventionelles Arbeitsumfeld zu ermöglichen
- Einen Anstieg an Cloud-Computing und der Nutzung von Cloud-Services von verschiedenen Standorten aus
- Effizienz, Verfügbarkeit und Kosten sollen optimiert werden
- Erhöhte IT-Komplexität, um Datenschutzbestimmungen (wie DSGVO, HIPAA und CCPA) zu genügen und erforderliche Prozesse zur Absicherung des Datenaustauschs. Der Datenschutz und die Sicherheit muss gewährleistet werden.
- Den Anstieg von Robotic Process Automation (RPA), um ehemals manuelle und zeitaufwendige Prozesse zu optimieren

Diese Entwicklung steigert die Effizienz und verbessert die e Cyber Resilience. Aber sie bringen auch neue Problemstellungen mit sich. Warum ist das so? All diese Technologien bergen die Gefahr der explosionsartigen Zunahme von Identitäten. Mit anderen Worten: Immer mehr Mitarbeiter (intern wie extern), Roboter, Maschinen und Geräte benötigen Zugriff auf Unternehmensressourcen. Hinzu kommt, dass es immer mehr Benutzerkonten gibt, die zu diesen Identitäten gehören, denn Unternehmen arbeiten mit einer Vielzahl grundverschiedener Umgebungen und Systemarten in einer historisch gewachsenen IT-Landschaft. All dies zusammen führt zur wohl größten Herausforderung in der Cybersicherheit – dem Identitätswildwuchs.

Warum dem Wildwuchs ein Ende gesetzt werden muss

Wir alle wissen, dass Hacker Lücken in der Cybersicherheit ausnutzen – und das häufig im großen Stil. Das macht sich beim Identitätswildwuchs sofort bemerkbar, so werden in letzter Zeit deutlich mehr Diebstähle von Anmeldedaten verzeichnet.

Laut dem Data Breach Investigations Report (DBIR) von Verizon aus dem Jahr 2021 betrafen 63 % aller Sicherheitsverletzungen Anmeldedaten. CensusWide fand zudem heraus, dass knapp die Hälfte der befragten Unternehmen im letzten Jahr Opfer eines Diebstahls von Anmeldedaten von privilegierten Konten wurden.

Die verheerenden Folgen dieser Lücken in der Identitätssicherheit sorgen fast tagtäglich für Schlagzeilen. Der SolarWinds Hack, der Cyberangriff gegen Colonial Pipeline und die Sicherheitslücke im Exchange Server sind nur einige Beispiele für Vorfälle, die allgemein bekannt wurden. Diese Verstöße beeinträchtigten nicht nur die Sicherheit und möglicherweise die Existenzgrundlage vieler Menschen, sondern hatten auch negative Konsequenzen für die Unternehmen.

Dabei hätten einige Angriffe ganz einfach verhindert werden können. Experten für Cybersicherheit stellten in einem kürzlichen Bericht fest, dass beinahe die Hälfte aller Benutzer mehr Berechtigungen hat, als sie für ihre Arbeit benötigen. Deswegen stehen Identitäten und deren Berechtigungen nicht nur bei Großunternehmen im Mittelpunkt, sondern auch Regierungsbehörden weltweit sind sich ihrer Relevanz bewusst. In einem Memo-Entwurf vom September 2021 hob z. B. das US-amerikanische Office of Management and Budget (OMB) verschiedene Pflichtergebnisse hervor, die bis zum Abschluss des Finanzjahres 2024 zu erreichen sind. Dazu gehörte, dass Regierungsbehörden die Multi-Faktor-Authentifizierung einführen und unternehmensweite Identitätsverwaltungsprozesse einrichten müssen.

Damit Unternehmen diese Sicherheitslücke schließen können, müssen Sie den Identitätswildwuchs eindämmen – andernfalls drohen Bußgelder, Rechtsstreitigkeiten und der Verlust des Kundenvertrauens sowie Umsatzeinbußen.

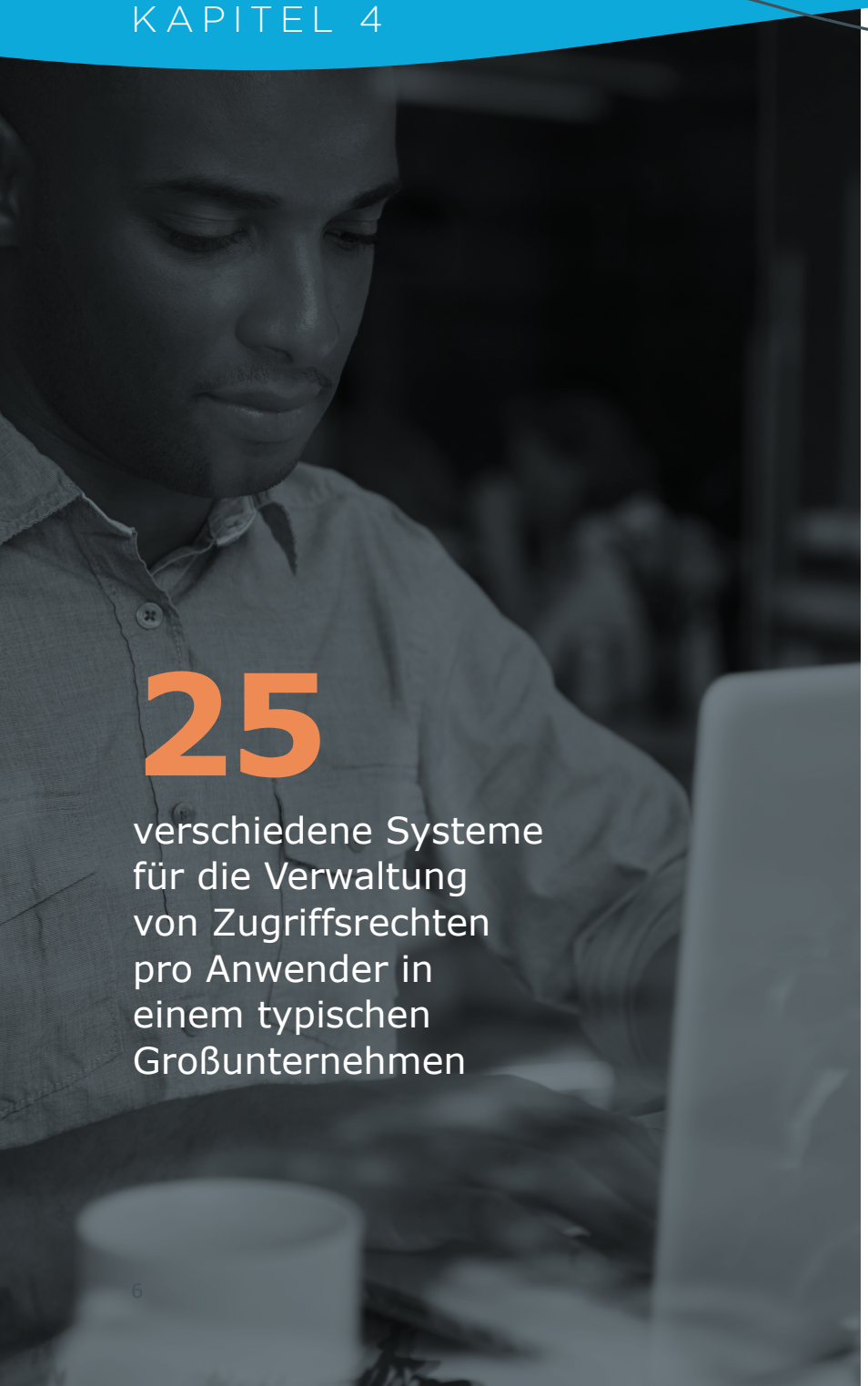
Die Identität als neuer Perimeter

Die Verwaltung von Identitäten wird immer wichtiger aber auch zunehmend komplexer, und so ist es nur logisch, dass der Sicherung von Identitäten eine größere Bedeutung zugemessen wird.

Der bisherige Perimeter bleibt weiterhin eine wichtige Verteidigungslinie gegen Cyberangriffe, er ist aber heutzutage nicht mehr ausreichend. Dieser infrastrukturbasierte Ansatz, der viele Jahre lang ein Eckpfeiler der Strategie für Cybersicherheit war, basiert auf der Annahme, dass innerhalb des Unternehmens alles geschützt werden kann. Um dieses ambitionierte Ziel zu erreichen, müssen Sie natürlich Ihre äußersten Verteidigungslinien stärken, nämlich dort, wo Angriffspunkte einem erhöhten Angriffsrisiko ausgesetzt sind.

Für diesen Ansatz ist der Perimeter unzureichend und nicht mehr zeitgemäß. Erfahrene Führungskräfte im Bereich IT-Sicherheit erkennen jetzt, dass sie um einen Kompromiss nicht herumkommen werden. Deshalb ist es eine pragmatischere Strategie, Maßnahmen zu ergreifen, um Angreifer draußen zu halten, aber gleichzeitig sicherzustellen, dass sie keinen Schaden anrichten können, wenn sie doch eindringen. Mithilfe dieses identitätsbasierten Ansatzes priorisieren vorausschauende Unternehmen das, was für sie am wichtigsten ist und prüfen genau, bevor sie entsprechenden Zugriff gewähren, wie z. B.: Wer ist der Benutzer? Worauf hat er Zugriff? Was macht er mit seinen Zugriffsberechtigungen, sind die Berechtigungen noch korrekt oder sollten sie geändert werden?

Kurz gesagt, der herkömmliche Perimeter verliert an Bedeutung und die Identität rückt in den Fokus.



25

verschiedene Systeme für die Verwaltung von Zugriffsrechten pro Anwender in einem typischen Großunternehmen

Die größten Hindernisse für Cyber Resilience

Identitätssicherheit ist ein wichtiger Faktor und viele Unternehmen arbeiten an ihrer Umsetzung, aber es ist nicht immer so einfach, wie man es sich wünscht. Das liegt vor allem daran, welche Arten von Identitäten vorhanden sind. In der Vergangenheit mussten sich Unternehmen hauptsächlich um interne Mitarbeiter kümmern, die für eine bestimmte Aufgabe eingestellt wurden, sich im Büro aufhielten und über ein einziges Gerät auf Ressourcen zugriffen. Bei den meisten Identitäten handelte es sich also um die Mitarbeiter.

Heutzutage sieht die Sache jedoch ganz anders aus. Sicherheitsexperten müssen sich nicht nur wegen interner Mitarbeiter Gedanken machen, sondern auch Identitäten von Auftragnehmern, Lieferanten und Partnern berücksichtigen. Mitarbeiter üben heutzutage nicht nur eine Aufgabe aus, sondern sie wechseln häufig ihre Arbeitsbereiche. Sie arbeiten nicht ausschließlich im Bürogebäude und greifen häufig von verschiedenen Standorten mit verschiedenen Geräten auf die benötigten Ressourcen zu. Sicherheitsexperten müssen neben Benutzern auch Anwendungen und Maschinen im Auge behalten. Benutzer können auch mehrere Identitäten und diese wiederum noch mehr Konten haben und: sie können Maschinen oder Roboter sein. Menschliche Benutzer verfügen oft über mehrere Geräte, die sich bei den unterschiedlichsten Anwendungen und Systemen on-premises oder in der Cloud anmelden. Und sie alle haben die Möglichkeit, von überall aus und über verschiedene physische Access Points und Systeme auf Ressourcen zuzugreifen.

Darüber hinaus verwalten die meisten Unternehmen heutzutage Zugriffsrechte in vielen getrennten Systemen. Laut dem dritten jährlichen Global Password Security Report nutzt ein Anwender in größeren Unternehmen durchschnittlichen 25 verschiedenen Systeme. Diese vielschichtige Umgebung erschwert es der IT-Sicherheit, die Übersicht über Berechtigungen und Benutzeraktivitäten zu gewinnen. Sie behindert außerdem eine vollständige Analyse des gesamten Kommunikationsprozesses. Aufgrund dieser Herausforderungen ergeben sich Informationslücken und Inkonsistenzen, die eine sorgfältige Prüfung vor Gewährung jeglicher Benutzerzugriffsrechte schwierig machen. Dabei spielen diese für die Implementierung eines modernen Sicherheitsansatzes eine wichtige Rolle.

Wenn Ihr Unternehmen diese Informationen nicht erhalten kann, kann es sich nicht auf Veränderungen von Benutzerrollen/Verantwortlichkeiten, Änderungen der IT-Infrastruktur und auf neue und aufkommende Bedrohungen einstellen. Verfolgt Ihr Unternehmen die Lösung dieser Problematik jedoch konsequent, wird es Ihre Cyber Resilience verbessern.

ONE IDENTITY by Quest

Argumente für einen ganzheitlichen Ansatz in der Identitätssicherheit

Identitätssicherheit kann auf verschiedene Weise umgesetzt werden und kann je nach Benutzerpopulation und -anforderungen, nach verwendeten Ressourcen, und abhängig vom Kerngeschäft eines Unternehmens andere Schwerpunkte haben. Aber der Schlüssel für eine erfolgreiche Umsetzung der Identitätssicherheit ist der Wechsel von einem fragmentierten zu einem ganzheitlichen Ansatz.

Viele Unternehmen betrachten jedoch die Kernaspekte der Identitätssicherheit getrennt wie z. B. Identity Governance and Administration (IGA), Identity Access Management (IAM), Privileged Access Management (PAM) sowie Active Directory Management and Security (ADMS) separat an. Innerhalb einer jeden Disziplin gibt es häufig mehrere Silos mit Benutzern, Anwendungen und Daten, die getrennt voneinander verwaltet werden. Diese Fragmentierung sorgt für hohe Reibungsverluste, verhindert eine Automatisierung der Administrationsprozesse und sorgt dafür, dass Unternehmen nur grob schätzen können, wann und wie Zugriffsrechte verwaltet werden sollten.

Der neue Ansatz ist umfassender und behandelt die wichtigsten Aspekte der Identitätssicherheit gemeinsam. Das bedeutet, Anwendungen greifen ineinander, Datensilos werden aufgelöst und Benutzer, Anwendungen und Daten ausgetauscht und abgeglichen. Mit diesem vereinheitlichten Ansatz zur Identitätssicherheit können Sie alle Identitäten korrelieren, Reibungsverluste aufgrund von Medienbrüchen und Dateninkonsistenzen durch verbesserte Integration vermeiden, die Angriffsfläche verringern und Ihre Cyber Resilience stärken.

ONE IDENTITY by Quest

Vereinheitlichte Identitätssicherheit als zentraler Baustein von Zero Trust

Mittlerweile ist gemeinhin bekannt, dass Zero Trust eine bewährte Vorgehensweise für die Implementierung einer robusten und zielgerichteten Sicherheit ist. Durch differenzierte und situationsabhängige Berechtigungszuweisung werden kritische Berechtigungen wie auch unnötiger und unverhältnismäßiger Zugriff ausgeschlossen. Unternehmen machen durch den Wechsel von einem fragmentierten zu einem ganzheitlichen Ansatz in der Identitätssicherheit bereits einen großen Schritt in Richtung IT-Sicherheit.

Zero Trust kann erfolgreich umgesetzt werden, wenn man den Blickwinkel erweitert. Sie sollten sich also nicht nur auf Identitäten von Personen konzentrieren, sondern auch auf Maschinenidentitäten. Nicht zu vernachlässigen sind auch all jene zusätzliche Konten, die durch die Erweiterung der historisch gewachsenen IT-Landschaft um Cloud oder hybride Infrastrukturen und durch Edge-Computing entstehen. Wenn Sie nicht alles im Blick behalten, könnte es sein, dass Hacker durch die Hintertür eindringen. Durch eine einheitliche Strategie zur Identitätssicherheit können Sie dieses Problem weitestgehend vermeiden.

Ein zweites wichtiges Element von Zero Trust ist die Bereitstellung einer flexiblen und konsistenten Zugriffsmethodik im gesamten Unternehmen. Der verbesserte Überblick und die Transparenz hilft Sicherheitsexperten dabei, Prozesse zu definieren, die Zugriffsrechte schneller und effizienter hinzufügen, entfernen und anpassen, „Just-in-Time". Dadurch kann der Zugriff der Benutzer auf das beschränkt werden, was für in diesem Moment für ihre Aufgabe nötig ist. Fehleranfällige manuelle Prozesse werden ausgeschlossen und die Arbeitsbelastung in der IT wird dadurch nicht höher.

Eine Schlüsselkomponente von Zero Trust ist Anpassbarkeit, die möglich ist, wenn eine einheitliche Strategie in der Identitätssicherheit umgesetzt wird. Durch die Nutzung dieses ganzheitlichen Ansatzes, der Kontextsensitivität und Verhaltensanalysen einbezieht, können Unternehmen schneller und effizienter neue Bedrohungen antizipieren, erkennen und darauf mit Korrekturmaßnahmen reagieren.

Best Practices für eine einheitliche Strategie in der Identitätssicherheit

Technologie kann erheblich bei der erfolgreichen Umsetzung eines einheitlichen Konzepts für die Identitätssicherheit in einem Unternehmen beitragen. Aber worauf sollten Sicherheitsexperten bei Lösungsanbietern achten, um bessere Ergebnisse zu erzielen? Für Ihre Auswahl sollten Sie diese fünf unverzichtbaren Funktionen berücksichtigen:

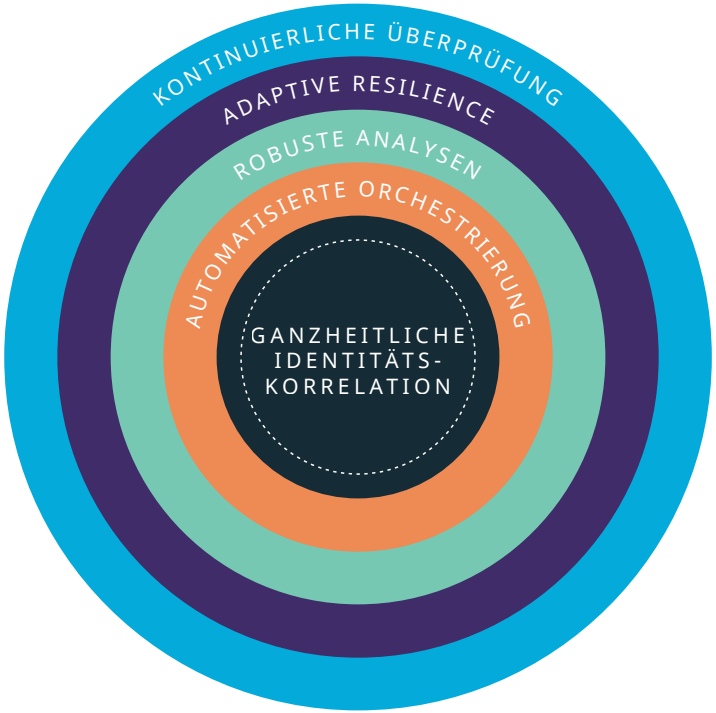
1. **Ganzheitliche Korrelation:** Unternehmen brauchen vor allem eine Lösung, die alle Identitäten und Konten vereint und dadurch den Überblick schafft, um fundierte Entscheidungen treffen zu können.

2. **Automatisierte Orchestrierung:** Ein zweites Kernelement der vereinheitlichten Identitätssicherheitsstrategie ist eine reibungslose Governance aller Identitäten und Zugriffsrechte. Dies erhöht nicht nur die Sicherheit, sondern verbessert Effizienz und Skalierbarkeit.

3. **Robuste Analysen:** Angesichts der Menge der zu berücksichtigen Elemente und deren Dynamik brauchen Unternehmen Lösungen für die Identitätssicherheit, die umfassende Einblicke liefern, durch die Bedrohungen antizipiert, erkannt und behoben werden können.

4. **Adaptive Cyber Resilience:** Sicherheitsexperten müssen sich bewusst sein, dass die Bedrohungslandschaft und das Unternehmen nicht mehr statisch sind. Deshalb sollten sie in der Lage sein, sich bei Bedarf schnell neu auszurichten und ihre Investitionen zukunftssicher zu machen.

5. **Kontinuierliche Überprüfung:** Eine vereinheitlichte Identitätssicherheit zeigt die größten Erfolge, wenn vor der Gewährung von Zugriffsrechten Überprüfungen durchgeführt werden können. Eine Technologie, die hierbei hilfreich ist, sollte die situative Sensibilität, Sitzungsüberwachung und Verhaltensanalysen einschließen und zusätzliche kontextbezogene Informationen berücksichtigen.



ONE IDENTITY by Quest

Hauptprobleme, die durch einen vereinheitlichten Identitätssicherheitsansatz gelöst werden können

Bisher wurden allgemeinen Herausforderungen und Vorteile beschrieben, die ein einheitlicher Ansatz für Identitätssicherheit mit sich bringt. Aber was sind die typischen Anwendungsfälle, die Experten für Cybersicherheit im Rahmen dieser Strategie abdecken können? Nachstehend finden Sie Beispiele für typische Ergebnisse:

Hauptprobleme	Anwendungsbeispiele	Ergebnisse
Absicherung des Unternehmens: **Schützen Sie Ihre Mitarbeiter, Anwendungen und Daten.**	• Zero Trust: Bieten Sie skalierbaren Schutz und reduzieren Sie das Risiko von Sicherheitsverletzungen, indem Sie ein adaptives Zero-Trust-Framework erstellen. • Privilegierter Remote-Zugriff: Stellen Sie sicher, dass Remote-Mitarbeiter und Auftragnehmer auf sichere Weise auf kritische Daten zugreifen können, auch ohne VPN. • Endpoint Privilege Management: Vereinheitlichen Sie die Sicherheit für AD/Azure AD-, Unix/Linux- sowie für Windows- und MacOS-Desktop-PCs. • Analyse des privilegierten Zugriffs und Sitzungsbeendigung: Erkennen Sie Risiken bei privilegiertem Zugriff und verhindern Sie, dass Ihr Unternehmen Schaden nimmt. • Verwaltung und Sicherheit eines Active Directory: Schränken Sie die Aufgabenbereiche der Administratoren auf das notwendige Mindestmaß ein und automatisieren Sie Standardabläufe, um Fehler in der manuellen Administration zu vermeiden. • Gesicherter privilegierter Zugriff für AD/Azure AD: Sichern und kontrollieren Sie interne und externe Zugriffe mit den gleichen Mechanismen, um eine maximale Absicherung Ihrer Ressourcen zu erreichen. • Password Vaulting: Vereinfachen und schützen Sie die Verwaltung von privilegierten Kennwörtern und Anmeldedaten.	• Schwachstellen beheben und Risiken minimieren • Zero Trust umsetzen • Vermeidung von Sicherheitsverletzungen • Vereinheitlichung von Identitäten in Cloud- und on-premises Umgebungen • Absicherung des privilegierten Zugriffs
Förderung betrieblicher Effizienz: **Zentralisieren Sie Sicherheitsprozesse.**	• Privilege Access Governance: Beziehen Sie privilegierte Benutzer in Ihre Governance-Prozesse ein. Andernfalls entstehen Lücken in der Einhaltung von Richtlinien mit negativen Auswirkungen auf die Sicherheit. • Active Directory Management and Security: Reduzieren Sie den Zugriff von Administratoren auf aufgabenspezifische Bereiche und optimieren Sie die Verwaltung von Benutzern und Gruppen durch Implementierung von Automationsprozessen. • Active Directory-Bridging: Vereinheitlichen Sie die Verwaltung über alle Betriebssysteme und Plattformen hinweg mittels zentral verwalteter Vorgaben und Richtlinien. • Fusionen und Übernahmen: Reagieren Sie schnell und ohne mühsame manuelle Prozesse auf komplexe Änderungen der Belegschafts- und Unternehmensstruktur.	• Vereinheitlichung von Richtlinien und Prozessen für die Identitätsverwaltung • Nachweisbare Verbesserung der Effizienz • Kontrolle des Zugriffs auf alle Ressourcen, Systeme und Plattformen • Automatisierung von Routineaufgaben, um die IT zu entlasten • Reibungslose Prozesse zur einfachen und automatisierten Verwaltung von Mitarbeitern bei Neueintritten, Abteilungswechsel und Ausscheiden (Joiner-Mover-Leaver)

Hauptprobleme	Anwendungsbeispiele	Ergebnisse
Audit- und Compliance-Anforderungen: **Dämmen Sie den Identitätswildwuchs ein und weisen Sie die Einhaltung von Richtlinien nach.**	• Identity Governance: Stellen Sie sicher, dass Richtlinien durchgesetzt, Benutzerzugriffe entsprechend den Anforderungen verwaltet und Nachweise dafür erbracht werden können. • Agentenlose Auditierung von Sitzungen: Schützen Sie Ihre kritischen Ressourcen und Benutzer durch Sitzungsaufzeichnungen und Analysen. Unterstützen Sie zudem forensische Untersuchungen und erfüllen Sie Compliance-Anforderungen an den privilegierten Zugriff. • Sofortige Compliance-Berichte: Erfüllen Sie Audit- und Compliance-Anforderungen durch Berichte zu allen Benutzern und Ressourcen sowie über alle Compliance-Maßnahmen.	• Erfüllung von Compliance-Anforderungen in der Berechtigungsverwaltung • Einhaltung von Richtlinien und Vorgaben zur Risikominimierung • Zuverlässige Audit Trails für alle Aktivitäten während privilegierter Sitzungen • Dedizierte Ereignisse können gesucht und Aufzeichnungen von privilegierten Sitzungen abgespielt werden • Erfüllen von Compliance-Anforderungen hinsichtlich der Überwachung des privilegierten Zugriffs
Absicherung Ihrer digitalen Transformation: **Schützen Sie Identitäten, während Sie den Funktionsumfang und den Zugriff erhöhen.**	• DevOps-Sicherheitsorchestrierung: Sorgen Sie für die Absicherung von DevOps- Prozessen mit identitätsbasierter Sicherheit. • Application Governance: Optimieren Sie Entscheidungen zum Zugriff auf Applikationen und geben Sie den Bereichsleitern die Möglichkeit, fundierte Entscheidungen zu treffen. • RPA-Sicherheitsoptimierung: Dämmen Sie Risiken im Zusammenhang mit der rasanten Zunahme von RPA-Identitäten ein. • Verwaltung komplexer Umgebungen: Reduzieren Sie den Verwaltungsaufwand für heterogene Umgebungen, um die Sicherheit und die Geschwindigkeit zu verbessern.	• Nahtlose Verwaltung von hybriden Umgebung • RPA sicher einsetzen • Vereinfachte Nutzung von DevOps Secrets • Klare Zuordnung von Mitarbeitern und Auftragnehmern • Weniger Fehler, erhöhte Sicherheit, optimierte Effizienz und geringere Komplexität

Fazit

Die Entwicklung schreitet ungebremst voran und mit ihr verändern sich Geschäftsbereiche und IT-Umgebung rasch, was zu einer weiteren Zunahme von Identitäten führt. Dieser Identitätswildwuchs wird täglich größer. Er birgt reelle Risiken in sich, die Experten für Cybersicherheit ernst nehmen müssen. Es ist Zeit, fragmentierten Ansätzen für die Verwaltung der Cybersicherheit ein Ende zu setzen.

Mit einem ganzheitlichen Ansatz für die Verwaltung von Zugriffsrechten können CISOs hinsichtlich der Cybersicherheit eine wichtige Lücke schließen. Sie können die Cyber Resilience ihres Unternehmens unterstützen und einen wichtigen Schritt unternehmen, um ein Zero-Trust-Modell umzusetzen, das sich schnell zu einer Notwendigkeit für Großunternehmen entwickelt.

Die Identität ist jetzt im Fokus. Eine einheitliche Sicherheitsstrategie für Identitäten ist die Lösung, um modernen Angriffsmethoden zu begegnen und Ihr Unternehmen für die Zukunft aufzustellen.

Wenn jetzt der Leiter der IT-Sicherheit anruft, können Sie sich darauf verlassen, dass Sie über alle Informationen verfügen, um den Zustand Ihrer Identitätssicherheit zu bewerten und zu ermitteln, und was in Ihrem Netzwerk geschehen ist.

Über One Identity

One Identity stellt vereinheitlichte Identitätssicherheitslösungen bereit, die Kunden dabei helfen, ihren Cybersicherheitsstatus zu stärken und Mitarbeiter, Anwendungen und Daten zu schützen, die für ihre Geschäfte von Bedeutung sind. Unsere vereinheitlichte Identitätssicherheitsplattform vereint erstklassige Lösungen für die Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) sowie Active Directory Management and Security (ADMS), mit denen Unternehmen von einem fragmentierten auf einen ganzheitlichen Ansatz für Identitätssicherheit umsteigen können. One Identity genießt weltweites Vertrauen und verwaltet über 250 Millionen Identitäten für mehr als 5.000 Unternehmen auf der ganzen Welt. Weitere Informationen finden Sie unter www.oneidentity.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:
www.quest.com/de-de/company/contact-us.aspx

eBook-UnifiedIdentitySecurity-KA-DE-WL-69156

ONE IDENTITY by Quest