COHESITY

KÄUFERLEITFADEN

EIN LEITFADEN FÜR FÜHRUNGSKRÄFTE ZUR BEWERTUNG VON LÖSUNGEN FÜR IDENTITÄTSRESILIENZ

Alles, was Sie wissen müssen, um Zugriffsrechte abzusichern, wertvolle Daten zu schützen und sich nach zerstörerischen Cyberangriffen schnell wieder zu erholen

Ihre Identitäts- und Zugriffsmanagementsysteme sind ein primäres Ziel für böswillige Akteure.

Warum?

9 von 10 Cyberangriffen betreffen Identitäts- und Zugriffsmanagementsysteme (IAM). Diese sind der am stärksten angegriffene Teil in der Infrastruktur jeder Organisation.

Ein Identitätssystem als führendes System ist ein hochwertiges Ziel, da seine Kompromittierung Angreifern Zugriff auf praktisch jede Ressource in der Organisation verschafft. Deshalb ist Identitätsresilienz ein Grundpfeiler jeder umfassenden Strategie für Cyber-Resilienz. Um ein minimal funktionsfähiges Unternehmen schnell wiederherzustellen, müssen Identitätsdienste zu den ersten Workloads gehören, die in einen vertrauenswürdigen Zustand zurückgeführt werden, da so viele kritische Systeme und Geschäftsprozesse von ihnen abhängig sind.

Für die meisten Organisationen ist das lokale Microsoft Active Directory (AD) das primäre IAM-System und die maßgebliche Quelle für andere Identitätsanbieter. Die Cyber-Wiederherstellung von AD, insbesondere in komplexen Umgebungen mit mehreren Forests, ist ein anspruchsvoller Prozess, der spezielles Fachwissen erfordert – sie ist nicht „nur eine weitere Workload“. Zusätzlich zu AD verwenden Sie höchstwahrscheinlich eine Mischung aus Entra ID und Okta.

Wenn Sie Ihre Abwehr gegen Cyberangriffe stärken möchten, müssen Sie sicherstellen, dass Sie über eine durchgängige Identitätsresilienz-Strategie für all Ihre kritischen Identitätsdienste verfügen.

> *„Keine Organisation kann zu 100 % vor Cyberangriffen geschützt sein – daher müssen Sie in Resilienz investieren, also in die Fähigkeit, sich von einem Sicherheitsvorfall zu erholen.“*

Identitätsresilienz stellt sicher, dass Ihr Unternehmen dazu in der Lage ist:

- **Identitätsbedrohungen zu erkennen und zu beheben:** Erkennen Sie laufende identitätsbasierte Angriffe und setzen Sie riskante Änderungen, die nicht auf menschliches Eingreifen warten können, automatisch zurück – mit Identity Threat Detection and Response (ITDR).
- **Identitätsdienste sauber wiederherzustellen und Vertrauen zurückzugewinnen:** Stellen Sie Ihre Identitätsdienste wieder her, ohne die Angreifer und/oder Hintertüren zurückzubringen, die zu einer persistenten Neuinfektion führen können.
- **Ausfallzeiten zu reduzieren:** Identität ist der Schlüssel für Zugriff und Authentifizierung. Wenn sie ausfällt, kommt der Betrieb zum Stillstand. Stellen Sie sicher, dass der Geschäftsbetrieb nach einem Identitätsangriff sicher und nahtlos wiederhergestellt werden kann, um Ausfallzeiten zu reduzieren.

Kein Unternehmen kann zu 100 % sicher vor Cyberangriffen sein – daher müssen Sie in Resilienz investieren, die Fähigkeit, sich nach einem Sicherheitsvorfall schnell zu erholen. Ihr Unternehmen sollte seine Identitätsresilienz verbessern und erweitern, indem es identitätsbasierte Angriffe kontinuierlich erkennt und behebt und eine bewährte Wiederherstellungsstrategie implementiert, die AD, Entra ID und Okta unter allen Umständen schnell und sauber wiederherstellt. Dieser Leitfaden hilft Ihnen, Lösungen zu bewerten, die richtigen Fragen zu stellen und eine souveräne Investitionsentscheidung zu treffen, um Ihre Identitätsinfrastruktur gegen moderne Bedrohungen abzusichern.

Worauf Sie bei einer Lösung für Identitätsresilienz achten sollten

Bei der Bewertung verschiedener Optionen ist es verlockend, Identität als einfach eine weitere Workload zu betrachten, die man sichert und bei Bedarf wiederherstellt. Aber das ist eine gefährlich veraltete Denkweise. Ein moderner Ansatz, der Cyber-Resilienz auf Identitäts- und Zugriffssysteme ausweitet, kombiniert erweiterte proaktive Sicherheit und saubere Wiederherstellung in jedem Schritt des Angriffslebenszyklus. Folgendes unterscheidet eine Identitätsresilienz-Lösung auf echtem Enterprise-Niveau vom Rest:

Erweiterte ITDR: Identitätsresilienz beginnt vor dem Sicherheitsvorfall. IAM-Systeme wie AD sind häufig die ersten Systeme, die Angreifer ins Visier nehmen, weil sie hier einen „Generalschlüssel" erhalten können. Es reicht nicht aus, einfach nur ein Backup zu erstellen. Ihre Lösung sollte in der Lage sein, durch Fähigkeiten im Bereich Identity Threat Detection and Response eine kontinuierliche Überwachung der Sicherheitslage Ihrer Identitätsumgebung bereitzustellen. Dies kann Sie dabei unterstützen, Schwachstellen zu erkennen, um Ihre Identitätsinfrastruktur abzuhärten und die Behebung von Vorfällen zu automatisieren. Automatisiertes Rollback und die Behebung böswilliger Änderungen, die nicht auf menschliches Eingreifen warten können, verringern die Chancen auf einen erfolgreichen Angriff. Durch die Implementierung dieser kontinuierlichen Bedrohungserkennung und Behebung sowie proaktiven Härtung können Sie sicherstellen, dass Angreifer auf Hindernisse stoßen, bevor sie Ihre Identitätssysteme zu einer Waffe machen können.

Ein Schutz, der Angriffen standhält: Wenn es zu einer Kompromittierung kommt, ist es wichtig, sicherzustellen, dass Ihre Identitätsinfrastruktur mithilfe sauberer Backup-Daten wiederhergestellt werden kann. Angreifer wissen, dass Backups die letzte Verteidigungslinie sind. Deshalb betreiben sie aktiv Double-Extortion-Methoden oder versuchen, sie zu verschlüsseln, zu verändern oder zu löschen – wodurch Sie weitgehend wehrlos werden und gezwungen sind, exorbitante Lösegelder zu zahlen. Ihre Lösung für Identitätsresilienz muss Unveränderlichkeit durch Design bieten – und sicherstellen, dass AD-Backups nicht manipuliert werden können, selbst wenn Angreifer an die Zugangsdaten von Domänenadministratoren gelangen. WORM-Speicher, Genehmigungen nach dem Vier-Augen-Prinzip und kryptografische Verifizierung sind entscheidende Fähigkeiten für resiliente Backups. Wenn Ihre Schutzschicht nicht standhält, wenn sich Angreifer bereits in Ihrem Netzwerk befinden, haben Sie keinen echten Schutz.

Schnelle, Malware-freie Wiederherstellung: Wenn Identitäten kompromittiert sind, breiten sich Ausfallzeiten auf alle Geschäftsfunktionen aus. Die Wiederherstellungsgeschwindigkeit ist wichtig, aber auch die Integrität der Wiederherstellung. Identitäten einfach wiederherzustellen, ohne ihren Vertrauensstatus zu validieren, birgt das Risiko, Malware oder Hintertüren erneut einzuschleusen, was zu wiederholten Infektionen und gefürchteten Doom-Loops führt. Eine effektive Lösung sollte die automatisierte, orchestrierte, schnelle Wiederherstellung von AD, Entra ID und Okta kombinieren. Speziell für AD sollten Wiederherstellungen vom Betriebssystem entkoppelt werden, um sicherzustellen, dass kompromittierte Zugangsdaten und Malware nicht zurückgebracht werden. So lassen sich Ausfallzeiten während eines Wiederherstellungsverfahrens reduzieren, indem persistente Infektionen verhindert werden – mit einer Wiederherstellung, der Sie vertrauen können.

Granulare Wiederherstellungsoptionen: Nicht jeder Identitätsvorfall erfordert eine vollständige Wiederherstellung. Eine granulare Wiederherstellung spart Zeit und reduziert Unterbrechungen, indem sie Ihnen Optionen für die Wiederherstellung auf Objekt-, Attribut- und Forest-Strukturebene anbietet. Wenn Sie Tools sowohl für die Forest- als auch für die granulare Wiederherstellung haben, ist sichergestellt, dass für Helpdesk-ähnliche Anfragen ebenso wie für ausgewachsene Cyberereignisse eine passende Lösung vorhanden ist.

Schutz über hybride Identität hinweg: Identität ist nicht mehr auf ein lokales AD beschränkt. Entra ID und Okta werden rasch zu einem entscheidenden Bestandteil der Identitätsarchitektur von Unternehmen, insbesondere für den Zugriff auf Cloud-Apps. Sie benötigen eine zukunftssichere Resilienzlösung, die nahtlos in hybriden Identitätsumgebungen läuft und sowohl AD, Entra ID als auch Okta schützt. Bei vielen Organisationen werden Entra ID und Okta mit AD synchronisiert, was bedeutet, dass Sie, um Entra ID und Okta erfolgreich und sicher wiederherzustellen, zuerst in der Lage sein müssen, AD zu schützen und wiederherzustellen. Entra ID und Okta sind von AD getrennte Anwendungen mit Einweg-Synchronisierungen vom lokalen System in die Cloud – ohne den lokalen Schutz besitzen Sie nur die zweite Hälfte einer Lösung. Ihre Lösung für Identitätsresilienz sollte auch Schutz- und Wiederherstellungsfähigkeiten umfassen, damit Entra ID und Okta sicher sind und sauber wiederhergestellt werden können, um die Kontinuität der Cloud-Identität sicherzustellen.

Post-Breach-Forensik zur Validierung des Vertrauens und zur Verhinderung zukünftiger Angriffe: Eine Wiederherstellung ohne Erkenntnisse macht Sie anfällig für wiederholte Vorfälle. Eine moderne Lösung sollte forensische Fähigkeiten integrieren, mit deren Hilfe Teams validieren können, ob eine Wiederherstellung sauber ist. Dies unterstützt nicht nur Post-Incident-Untersuchungen, sondern liefert entscheidende Informationen für Präventionsmaßnahmen – und hilft

Unternehmen, ihre Abwehrfähigkeiten zu stärken und Compliance- oder regulatorische Berichtspflichten zu erfüllen. Ohne die Due Diligence nach der Wiederherstellung riskieren Sie einen Folgeangriff. Forensik sollte keine untergeordnete Rolle spielen. Sie ist ein integraler Bestandteil der Identitätsresilienz.

Fähigkeit zur Wiederherstellung ohne Internetzugang: Im Falle eines katastrophalen Ausfalls oder Cyberangriffs können Sie nicht davon ausgehen, dass Ihnen ein stabiler oder sicherer Internetzugang zur Verfügung steht. Ihre Lösung für Identitätsresilienz muss in der Lage sein, Ihre kritischen Identitätssysteme auch ohne Internet erfolgreich wiederherzustellen, sodass Sie in jeder Situation sauber wiederherstellen und Systeme wieder online bringen können.

Rund um die Uhr verfügbare Unterstützung bei Zwischenfällen: Identität ist eine einzigartige und komplexe Workload, insbesondere, wenn es um ihre Wiederherstellung geht. Im Hinblick auf die Cyber-Wiederherstellung kritischer Identitätsinfrastruktur ist es entscheidend, sicherzustellen, dass der Hersteller der Lösung über nachgewiesene Expertise beim Schutz, der Absicherung und der Wiederherstellung von Identitäten verfügt und dem Kunden die notwendige Anleitung bereitstellen kann. Jede Wiederherstellungssituation ist einzigartig, und die richtige Reaktionsunterstützung und Forensik durch erfahrene Experten ist der Schlüssel, um sicherzustellen, dass Ihre Organisation sich auch von den katastrophalsten Identitätsangriffen oder Ausfällen sicher und schnell erholen kann.

Kritische Fragen, die Sie Herstellern stellen sollten

1. Wie verhindern Sie, dass Angreifer AD-, Entra ID- oder Okta-Backups manipulieren oder löschen?
2. Können Sie die vollständige Wiederherstellung Ihrer gesamten Identitätsinfrastruktur in weniger als einem Tag demonstrieren?
3. Wie überprüfen Sie, dass wiederhergestelltes AD, Entra ID oder Okta frei von Malware und Hintertüren ist oder keine kompromittierten Zugangsdaten wiederhergestellt wurden?
4. Können Sie Identitäten mit derselben Erfahrung und Bedienoberfläche ohne Internetzugang wiederherstellen?
5. Unterstützen Sie hybride Identitätsumgebungen (lokales AD + Entra ID + Okta)?
6. Kann Ihre Lösung vollständige Forest-Wiederherstellungen für AD automatisiert durchführen und das Microsoft Recovery Runbook einhalten?
7. Erkennt Ihre Lösung identitätsspezifische Bedrohungen, um Angreifer zu identifizieren und zu entfernen, bevor es zu einer Kompromittierung kommt?

Warnzeichen, auf die Sie achten sollten

- Keine Fähigkeiten im Bereich Identitätssicherheit. Resilienz umfasst die Risikoreduzierung vor dem Eintreten eines Vorfalls sowie die Abwehr von Bedrohungen, um eine Kompromittierung zu verhindern.
- Lösungen, die sich ausschließlich auf native Microsoft-Tools stützen. Diese sind manuell, langsam und unzuverlässig, wenn man sie am dringendsten braucht.
- Backups, die in der Produktionsumgebung gespeichert werden. Angreifer können sie löschen, woraufhin Sie nichts mehr haben, das wiederhergestellt werden könnte.No identity security capabilities.
- Keine Orchestrierung oder Automatisierung für parallele Wiederherstellungen mehrerer Domänencontroller (DCs). Ohne diese sind Administratoren gezwungen, in einer Zeit hoher Belastung und in einer chaotischen Umgebung langwierige, manuelle Schritte zu befolgen.
- Die Lösung ist darauf angewiesen, dass ein sicherer und stabiler Internetzugang vorhanden ist. Sie können nicht davon ausgehen oder sich darauf verlassen, dass während eines Cyberangriffs oder einer Wiederherstellung eine Internetverbindung verfügbar ist.
- Keine Möglichkeit, die Wiederherstellung zu testen. Wenn Sie etwas nicht testen können, können Sie ihm auch nicht vertrauen.
- Keine Möglichkeit, das Betriebssystem während der Wiederherstellung zu entkoppeln. Die Wiederherstellung des Betriebssystems zusammen mit Ihren Identitätsdaten kann Malware und Hintertüren zurückbringen.
- Keine Möglichkeit, eine physische/virtuelle Quelle für die Wiederherstellung auszuwählen. Die Anforderung eines exakten Patch-Standes kann zu längeren Ausfallzeiten führen.
- Keine Expertise in Identitätsforensik und Vorfallreaktion (IFIR) für 24/7-Unterstützung bei der Vorfallreaktion.

Checkliste zur Bewertung von Herstellern

Verwenden Sie diesen Bewertungsbogen bei Gesprächen mit Herstellern:

Requirement	Hersteller 1	Hersteller 2	Hersteller 3	Notizen
Unveränderliche, isolierte AD-Backups				
Granularität der Wiederherstellung von Objektebene bis Forest-Ebene				
Automatisierte Workflows zur Forest-Wiederherstellung				
Proaktive Härtung zur Identifizierung und Schließung von Angriffspfaden				
Erkennung von Malware/Schäden in Backups				
Manipulationssichere Änderungsverfolgung und Rollbacks mit mehreren Quellen				
Inventarisierung und Überwachung stark angegriffener Dienstkonten				
Unterstützung für Hybrid-AD (lokal + Entra ID)				
Post-Breach-Forensik				
Skalierbarkeit (Multi-Forest/global)				
24/7-Unterstützung durch Experten für Identity Incident Response				
Parallele Wiederherstellung mehrerer DCs (für AD)				
Auswahl einer physischen/virtuellen Quelle für die Wiederherstellung				
Stellt mehrere Domänencontroller (DCs) parallel wieder her (für AD)				

Das Endergebnis

Identitätsbasierte Kompromittierung steht im Mittelpunkt nahezu jeder größeren Sicherheitsverletzung. Deshalb ist die Beschleunigung der Cyber-Resilienz in Bezug auf Ihre kritischen Identitätssysteme nicht mehr länger optional – sie ist grundlegend für die Unternehmenssicherheit.

Eine bewährte Lösung für Identitätsresilienz geht über Backups hinaus. Sie härtet Identitäten gegen Kompromittierung, schützt vor Identitätsangriffen und -bedrohungen, ermöglicht eine blitzschnelle, vertrauenswürdige Wiederherstellung und hilft Ihnen dabei, Hintertüren zu schließen, um vertrauenswürdige, Malware-freie Wiederherstellungen zu ermöglichen. Um mehr über Identitätsresilienz zu erfahren und darüber, wie sie dazu beitragen könnte, Ihre kritischsten Identitätsdienste abzusichern, sprechen Sie noch heute mit Ihrem Cohesity Account-Team.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500064-001-DE 8-2026