Commvault

eBOOK

DIE NICHT-MENSCHLICHE IDENTITÄTEN KRISE:

ÜBERBRÜCKUNG DES BLINDEN FLECKS IN MODERNEM DATENSCHUTZ & CYBERRESILIENZ

ZUSAMMENFASSUNG FÜR FÜHRUNGSKRÄFTE

Im Zeitalter KI-gesteuerter Automatisierung hat sich der traditionelle Sicherheitsperimeter aufgelöst, und die Identität ist zur letzten Verteidigungslinie geworden. Während die Unternehmenssicherheit jahrzehntelang die menschliche Authentifizierung verstärkt hat, hat eine stille Explosion nicht-menschlicher Identitäten (NHI) – Dienstkonten, API-Schlüssel, OAuth-Token und KI-Agenten – eine massive, unkontrollierte Angriffsfläche geschaffen.

Diese Identitäten übertreffen die Zahl der Menschen mittlerweile um das Verhältnis 144:11, werden aber selten mit der gleichen Strenge verwaltet. Dieses E-Book untersucht, wie moderne Angreifer diese „technische Identitätsschulden" ausnutzen, um dauerhaften Zugriff aufrechtzuerhalten, und warum Unternehmen auf eine Tier-0-Architektur mit Fokus auf Wiederherstellung umstellen müssen, um Identitätsresilienz zu gewährleisten.

1 Der NHI & Secrets Risikobericht H1 2025, Entro

ABSCHNITT 1: DEFINIEREN DER MASCHINENANGRIFFSFLÄCHE

Der Anwendungsbereich von NHIs reicht weit über Cloud-native Software hinaus; sie stellen das entscheidende Bindeglied für physische und medizinische Infrastrukturen, die die moderne Gesellschaft tragen. In diesen sensiblen Bereichen ist ein NHI jedes Gerät oder „Ding“, das über Zugangsdaten verfügt, Aktionen ausführt und Daten autonom überträgt.

Es ist unerlässlich zu erkennen, dass der „blinde Fleck“ des NHI nun auch Hardware-Assets umfasst, die direkt mit der physischen Welt interagieren. Wenn diese Identitäten übermäßig privilegiert oder unzureichend kontrolliert werden, besteht das Risiko nicht nur im Datenverlust, sondern umfasst auch physische Schäden.

Das Risiko umfasst nicht nur Datenverlust, sondern kann auch Menschenleben gefährden.

FINANZIELLE INFRASTRUKTUR

Moderne Geldautomaten fungieren als hochentwickelte NHIs (nicht-menschliche Identitäten), die sich über Servicekonten und API-Schlüssel bei Kernbankensystemen authentifizieren, um die Bargeldauszahlung zu autorisieren und sensible personenbezogene Daten zu verarbeiten.

HERSTELLUNG & INDUSTRIE-IOT

In intelligenten Fabriken fungieren speicherprogrammierbare Steuerungen und Roboterarme als Workload-Identitäten.. Sie fungieren als Workload-Identitäten innerhalb von DevOps-Automatisierungspipelines. Eine Schwachstelle ermöglicht es einem Angreifer, die Integrität zu manipulieren – also physische Produktionsparameter zu verändern, ohne menschliche Warnmeldungen auszulösen.

AGENTISCHE KI IN PHYSISCHEN SYSTEMEN

Beim Einsatz von agentischer KI zur Steuerung von Gebäudesteuerungssystemen oder Stromnetzen müssen sich diese Agenten authentifizieren, um agieren zu können. Durch böswillige Manipulation mittels Prompt-Injection könnte ein Agent dazu verleitet werden, sensible Standortpläne zu exfiltrieren oder Versorgungsleistungen zu stören.

BIOTECH & MEDIZINISCHES IOT:

Krankenhausgeräte

Bildgebende Geräte und Infusionspumpen fungieren als nicht-menschliche Identitäten (NHIs), die Zugriff auf elektronische Patientenakten erhalten, oft unter Verwendung langlebiger Token, die selten ausgetauscht werden.

Implantierbare Geräte

Vernetzte Herzschrittmacher und Insulinpumpen stellen den sensibelsten Bereich der Identitätsebene dar. Diese Geräte authentifizieren sich gegenüber den Netzwerken der Gesundheitsdienstleister, um Telemetriedaten zu übertragen. Wird die Identitätsebene kompromittiert, handelt es sich bei der manipulierten „automatisierten Entscheidung “ um eine lebenswichtige medizinische Anpassung.

Die Identitätsresilienz dieser Geräte erfordert eine Architektur, bei der die Wiederherstellung an erster Stelle steht. Die Organisation muss in der Lage sein, unautorisierte Rechteausweitungen in Echtzeit zu auditieren und rückgängig zu machen, um sicherzustellen, dass ihre physischen und medizinischen „Identitäten“ in einem vertrauenswürdigen und sicheren Zustand bleiben

DIE RISIKOZAHLEN

Das Ausmaß der NHI-Landschaft ist überwältigend und wächst 4- bis 10-mal schneller als die Anzahl

GOVERNANCE-LÜCKE

Weniger als

25%

der Organisationen verfügen über formale Richtlinien für die Schaffung oder Abschaffung dieser Identitäten.3

ÜBERMÄSSIGE PRIVILEGIEN

97%

NHIs verfügen über Berechtigungen, die weit über das für ihre eigentliche Funktion Notwendige hinausgehen.4

VERLETZUNG

Only

12%

of organizations express high confidence in their ability to prevent an attack targeting these machine identities.[5]

2. CyberRisk-Allianz
3. Der Stand der nicht-menschlichen Identitäts- und KI-SicherheitCloud Security Alliance
4. Stand der nicht-menschlichen Identitäten und Geheimnisse in der Cybersicherheit im Jahr 2025, Entro
5. Der Stand der nicht-menschlichen Identitäts- und KI-SicherheitCloud Security Alliance

ABSCHNITT 2: FALLSTUDIE ZUR MODERNEN KRIEGSFÜHRUNG – DIE SLH UND SHINYHUNTERS MODELLE

Gegner wie die Cyberkriminellen-Supergruppe die Cybercrime-Gruppe LAPSUS$ – darunter berüchtigte Akteure wie ShinyHunters und Scattered Spider – haben einen grundlegenden Wandel in der Angriffsmethodik ausgelöst. Ihre Taktiken verdeutlichen, warum NHIs strategisch wertvoller sind als menschliche Zugangsdaten.

DIE INDUSTRIELLE VISHING-PIPELINE

SLH hat Voice-Phishing industrialisiert **(Vishing),** ein Vektor, der einen Anstieg von 449 % verzeichnete im Jahr[2026.6]

01 REKRUTIERUNG UND ANREIZ

The group has been observed offering financial incentives of $500 to $1,000 per call to recruit specialized talent, specifically seeking women to conduct vishing attacks.7 This tactic is designed to increase the success rate of help desk impersonation by bypassing traditional “attacker” profiles that staff may be trained to identify.

02 DER EINTRAG

Using pre-written scripts, these recruits impersonate employees to convince IT help desks to perform password or multi-factor authentication (MFA) resets.

03 DER ÜBERGANG ZU NHIS

Sobald Angreifer Zugriff erlangt haben, bewegen sie sich lateral in virtualisierte und Cloud-Umgebungen. Sie sichern ihre Persistenz häufig, indem sie von Benutzerkonten auf Nicht-menschliche Identitäten wechseln, beispielsweise durch den Diebstahl von OAuth-Tokens oder die Erstellung neuer administrativer Dienstkonten.

04 DIE PERSISTENZ

Im Gegensatz zu menschlichen Passwörtern werden diese Nicht-menschliche Identitäten selten geändert und sind für herkömmliche Überwachungsmethoden oft unsichtbar. Dadurch kann der Angreifer den Zugriff lange aufrechterhalten, nachdem der kompromittierte menschliche Benutzer bereits zurückgesetzt wurde.

6 2025 Phishing Threat Trends Report, Vol. 6, KnowBe4
7 The Hacker News

ABSCHNITT 3: DIE KRITISCHEN SCHWACHSTELLEN VON NHIS

NHIs umgehen die drei traditionellen Säulen der Sicherheit: Benutzer-MFA, Endpunkterkennung und E-Mail-Filterung.

OAUTH-MISSBRAUCH

Angreifer verleiten Nutzer über eine Zustimmungsmaske zur Genehmigung von Anwendungen und gewähren ihnen so delegierten Zugriff auf Postfächer und Daten. Diese Aktivitäten erscheinen legitim und bleiben selbst nach Passwortzurücksetzungen aktiv, was es erschwert, sie als Bedrohung zu erkennen und entsprechende Maßnahmen zu ergreifen.

GHOSTING VON DIENSTKONTEN

In großen Unternehmen operieren Tausende undokumentierter Servicekonten mit administrativen Rechten und bleiben oft lange aktiv, nachdem ihr ursprüngliches Projekt beendet ist. Diese mangelnde Systemhygiene ist ein zentrales Problem.

Dieses Problem muss konsequent und effizient behoben werden.

TOKEN- UND SCHLÜSSELDIEBSTAHL

Langlebige API-Schlüssel, die in statischen Konfigurationsdateien oder DevOps-Pipelines eingebettet sind, verfügen über keinen Geräte- oder Geolokalisierungskontext und ermöglichen so einen umfassenden, automatisiertenn Zugriff, ohne eine interaktive Anmeldebenachrichtigung auszulösen.

ABSCHNITT 4: EIN RAHMEN FÜR IDENTITÄTSRESILIENZ

Organisationen müssen ihre Arbeitsabläufe weiterentwickeln, um NHIs als Vermögenswerte der Stufe 0 zu behandeln, die hinsichtlich des Risikos gleichwertig sind.

An Domänenadministratoren oder Cloud-Steuerungsebenen.

PRIVILEGIERTE ERSTELLUNGS PROTOKOLLE

Die Erstellung eines OAuth-App- oder Dienstkontos sollte eine administrative Genehmigung erfordern und hochrelevante Sicherheitstelemetriedaten generieren.

KORRELATION ZWISCHEN MENSCH UND NHI

Die meisten Sicherheitslücken könnten frühzeitig verhindert werden, indem domänenübergreifende Sicherheitsereignisse korreliert werden, wie beispielsweise eine Interaktion mit dem Helpdesk, auf die unmittelbar eine MFA- Zurücksetzung oder die Erstellung eines neuen Tokens folgt.

ELIMINIERUNG STATISCHER GEHEIMNISSE

Statische Geheimnisse stellen ein inakzeptables Risiko dar. Sie müssen durch kurzlebige Token und automatische Rotation ersetzt werden.

RESILIENZORIENTIERTE ARCHITEKTUR

Da eine hundertprozentige Prävention unmöglich ist, müssen Organisationen in der Lage sein, die Identitätsumgebung schnell zu erkennen, einzudämmen und in einen vertrauenswürdigen und sicheren Zustand zurückzuversetzen.

ABSCHNITT 5:
COMMVAULT IDENTITÄTSRESILIENZ

Commvault-Identitätsresilienz

hilft dabei, die Transparenz und Wiederherstellungsfunktionen bereitzustellen, die zum Schutz komplexer Identitätsumgebungen im Unternehmensmaßstab erforderlich sind.

SCHNELLE IDENTITÄTSWIEDERHERSTELLUNG

Bietet automatisierten Wiederherstellungsfunktionen, die von einzelnen AD-Attributen und -Objekten bis hin zur vollständigen Wiederherstellung der Gesamtstruktur reichen. Da die Wiederherstellung der AD-Gesamtstruktur einer der komplexesten und fehleranfälligsten Wiederherstellungsprozesse in der IT ist und DNS, SYSVOL, FSMO-Rollen und globale Kataloge umfasst,

Die Lösung ist darauf ausgelegt, Vertrauensstellungen, Replikation und Wiederherstellungssequenzen über mehrere Domänen hinweg zu automatisieren und zu orchestrieren. Dies geschieht durch geführte Arbeitsabläufe und Runbooks.

Dies hilft Organisationen dabei, die Identitätsumgebung schnell wiederherzustellen und in einen bekannten, zuverlässigen Zustand zu versetzen, Ausfallzeiten zu minimieren, das Risiko menschlicher Fehler zu reduzieren sowie die Grundlage für Authentifizierung und Autorisierung wiederherzustellen, auf der der Rest der Organisation beruht.

SCHWACHSTELLENANALYSE

Bewertet die Active Directory (AD)-Umgebung hinsichtlich ihrer Sicherheit. Die Bewertung deckt Schwächen auf, die die Wahrscheinlichkeit oder die Auswirkungen einer Kompromittierung erhöhen. Dazu gehören übermäßige Berechtigungen und Konten mit zu vielen Zugriffsrechten, die Verwendung veralteter und unsicherer Protokolle wie NTLMv1, SMBv1 und unsigniertes LDAP, schwache Authentifizierungseinstellungen, fehlende Sicherheitsvorkehrungen sowie riskante Konfigurationsabweichungen.

Es beleuchtet außerdem Probleme wie unkontrollierte Delegierung, veraltete privilegierte Konten, schwache Passwort- und Kerberos-Richtlinien, unsichere Vertrauensbeziehungen und mangelnden Schutz für Tier-0-Assets. Das Ergebnis ist eine priorisierte Risikokarte für Identitätsrisiken, die Unternehmen hilft, den potenziellen Schaden zu begrenzen und die Resilienz ihrer Identitäten zu stärken.

Ein Angreifer kann AD in eine dauerhafte Plattform für Kompromittierung und laterale Bewegung verwandeln.

ECHTZEITPRÜFUNG UND ROLLBACK

Der Dienst überwacht Active Directory kontinuierlich mithilfe von Verzeichnissynchronisierungsdaten und Windows-Ereignisprotokollen, um verdächtige oder unautorisierte Änderungen sofort zu erkennen. Er verfolgt Aktivitäten wie Rechteausweitung, das Hinzufügen von Benutzern zu privilegierten Gruppen, Änderungen an Gruppenrichtlinienobjekten (GPOs), Änderungen an Tier-0-Konten, Änderungen an Authentifizierungsrichtlinien, die Erstellung von unbefugten Benutzern und Versuche, die Sicherheitseinstellungen zu schwächen.

Jedes Ereignis wird in einer Zeitleiste erfasst, sodass Administratoren reguläre Verwaltungsvorgänge schnell von den ersten Schritten eines Identitätsangriffs unterscheiden können. Werden böswillige oder versehentliche Änderungen festgestellt, unterstützt die Plattform ein schnelles Rollback mit nur einem Klick, um den vorherigen, vertrauenswürdigen und sicheren Zustand wiederherzustellen.

Erfahren Sie mehr über Identitätsresilienz.

commvault.com | 888.746.3849 | get-info@commvault.com