CYBERARK

SOLUTION BRIEF

CYBERARK FÜR SAP-UMGEBUNGEN

Highlights

Zusammen stellen CyberArk und SAP Unternehmen folgende Möglichkeiten bereit:

- Ergänzung der SAP-Sicherheitskontrollen und Minderung des Sicherheitsrisikos von privilegiertem Zugriff durch das Verwalten, Schützen und Kontrollieren privilegierter SAP-Accounts
- Isolierung privilegierter Benutzer vom direkten Zugriff auf geschäftskritische SAP-Systeme und Überwachung der Aktivitäten privilegierter SAP-Benutzer, um verdächtige Aktivitäten zu erkennen und zu unterbinden
- Compliance abbilden, indem vollständig offengelegt wird, wer auf privilegierte SAP-Accounts zugreift, wann Einzelpersonen privilegierten Zugriff benötigen und welche Aktionen durchgeführt werden
- Bereitstellung einer ganzheitlichen Sicherheitsstrategie für privilegierten Zugriff im Unternehmen, die für den gesamten SAP-Bestand sowie andere Infrastrukturen und Anwendungen gilt

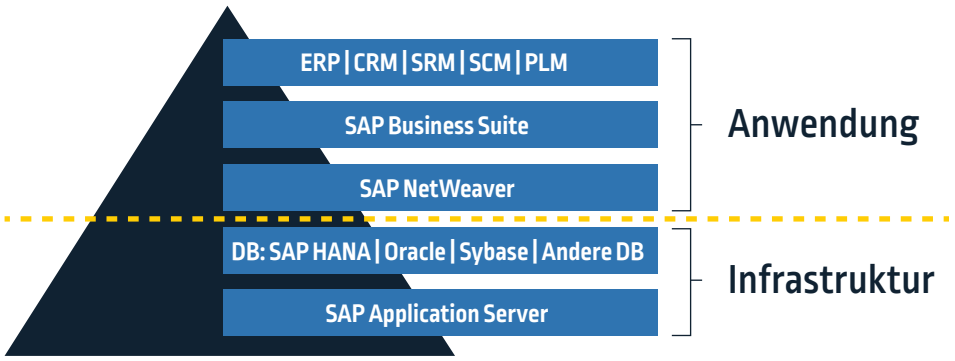
Überblick

Die Unternehmen von heute vertrauen immer noch auf eine komplexe Struktur aus Systemen, Anwendungen und Daten, um ihre Geschäfte am Laufen zu halten und für einen offenen Informationsfluss zu sorgen. SAP, weltgrößter Anbieter von Unternehmenssoftware, stellt die Tools bereit, die moderne Firmen brauchen, um ihre Geschäfte abzuwickeln, ihre Daten zu verwalten und den zukünftigen Bedarf ihrer Kunden zu prognostizieren. Mehr als 91% der Forbes-2000-Firmen sowie die wichtigsten globalen Marken und Regierungsbehörden vertrauen auf SAP-Anwendungen, um genau das zu erreichen.[1]

Da immer mehr Unternehmen zahlreiche SAP-Systeme, -Anwendungen und -Datenbanken für ihre Geschäfte verwenden, besteht für sie ein verstärkter Bedarf an einer Reduzierung des Angriffsvektors und der Verwaltung des privilegierten Zugriffs.

Die Herausforderung

Geschäftskritische Daten und hochwertige Geschäftsressourcen befinden sich auf allen Ebenen der SAP-Unternehmensanwendungen und -Systeme, daher braucht jede Schicht privilegierten Zugriff. Das macht SAP zu einem attraktiven Ziel für schädliche Cyber-Angriffe. Die Omnipräsenz von SAP bedeutet, dass das Potenzial für Störungen des Betriebs, die Kompromittierung von Daten und das Risiko von Compliance- und regulatorischen Folgen so hoch ist wie nie. Tatsächlich gehen Sicherheitsexperten davon aus, dass die Anzahl von Angriffen auf SAP-Systeme weiterhin steigen wird, und mit einem durchschnittlichen Schaden von 5 Millionen USD pro SAP-Sicherheitsverletzung können die Kosten ins Unermessliche wachsen.[2]



In vielen Fällen werden umfassende Berechtigungen von mehreren Mitarbeitern geteilt (z. B. Administratorgruppen) und die zugehörigen Passwörter sind im ganzen Unternehmen bekannt. Benutzer mit Zugriff auf NetWeaver können beispielsweise umfassenden Zugriff auf leistungsstarke Datenbanken, Anwendungen und Analysen gewähren und bekommen. Außerdem ist es schwierig zu kontrollieren, wo diese Passwörter verwendet werden und unter welchen Umständen.

[1] SAP
[2] Crowd Research Partners Cybersecurity Research Report

Auch wenn die SAP-Sicherheitsmaßnahmen dazu entwickelt wurden, solche Schwachstellen anzugehen, sorgt das Sichern von privilegiertem Zugriff mithilfe von nativen Tools für zusätzliche Komplexität und greift hinsichtlich Sicherheits- und Compliance-Anforderungen oftmals zu kurz. Das zugrundeliegende Betriebssystem sowie die Anwendungen und Systeme, die Teil eines SAP-Ökosystems sind, stellen ebenfalls potenzielle Sicherheitsrisiken dar.

Während SAP Administratoren die Möglichkeit für das Erstellen von Rollen und Profilen für die Verwaltung, Trennung und Einschränkung von Aktivitäten gibt, brauchen Unternehmen angesichts der sich ständig verändernden Bedrohungslandschaft von heute und des Potenzials geschäftlicher und finanzieller Schäden einen besseren Weg, um die in einer SAP-Umgebung so wichtigen privilegierten Accounts zu verwalten, schützen und kontrollieren.

CyberArk Privileged Access Security Lösungen für SAP

Als Mitglied des SAP Partner Edge Program, verfügt CyberArk über eine zertifizierte Integration in SAP unterstützt von NetWeaver. Die CyberArk Privileged Access Security (PAS) Lösung ermöglicht den Schutz und die Rotation von Anmeldedaten, die Session-Isolation und -Überwachung sowie die Bedrohungserkennung und -prävention, die erforderlich sind, um den Angreifern immer einen Schritt voraus zu sein und die kritischsten SAP-Ressourcen des Unternehmens zu schützen.

Das automatische Onboarding von SAP-Accounts und -Anwendungen kann mit dem CyberArk Enterprise Password Vault und der CyberArk REST API konfiguriert werden. CyberArk hilft Unternehmen ebenfalls dabei, Audit- und Compliance-Anforderungen zu vereinfachen und zu erfüllen, indem sie einen zentralen Datensatz mit dem gesamten Zugriff auf privilegierte Accounts und Systeme im Zusammenhang mit SAP pflegen. Dadurch werden Risiken gemindert, da die Auditfunktionen von SAP in vielen Fällen möglicherweise deaktiviert oder nicht vollständig betriebsfertig konfiguriert wurden.

Durch die Verwaltung, den Schutz und die Kontrolle privilegierter SAP-Accounts, die von SAP- und IT-Administratoren verwendet werden, reduziert CyberArk das Sicherheitsrisiko von hochwertigen SAP-Ressourcen und verringert gleichzeitig die administrative Belastung und gewährleistet Compliance. CyberArk lässt sich in das SAP-System aus Benutzern, Rollen, Profilen und Berechtigungen integrierten, um unerwünschten Zugriff zu verhindern, und verstärkt native SAP-Sicherheitsfunktionen und Best Practices für eine einheitliche Schnittstelle für den gesamten privilegierten Zugriff in einem Unternehmen. Dies ermöglicht einen ganzheitlichen Ansatz für Unternehmenssicherheit, bei dem auch die erhöhten Risiken in einer SAP-Umgebung berücksichtigt werden.

Zusätzliche Sicherheit

CyberArk ergänzt die Sicherheitsfunktionen von SAP, einschließlich Bedrohungserkennung und GRC-Zugriffskontrolle, und verbessert so die Sicherheitsposition des Unternehmens. CyberArk unterstützt klassische SAP-ERP-Systeme sowie eine Vielzahl von SAP-Produkten und -Technologien, einschließlich: SAP CRM, SRM, SCM, SAP NetWeaver Java, SAP HANA und Sybase ASE.

- Sichern von Anmeldeinformationen, die in allen Schichten des SAP-Bestands genutzt werden, vom Betriebssystem und den virtuellen Maschinen und Datenbanken bis zur Anwendung selbst. CyberArk schützt die SAP-Datenschicht durch die Integration in übliche Datenbanken in SAP-Umgebungen von Oracle, SAP HANA, Sybase, SQL Server und DB2.
- Verwalten der SAP-Anmeldeinformationen an einem einzigen Ort und Verhindern von unbefugtem Zugriff auf geschäftskritische Systeme.
- Rotation und Aktualisierung der Anmeldeinformationen in regelmäßigen Intervallen oder bei Bedarf (je nach Richtlinie), einschließlich der Verwaltung sensibler DDIC-Anmeldeinformationen, die im SAP-Upgradeprozess zum Einsatz kommen.
- Isolation von Sessions privilegierter Benutzer und Durchsetzung starker Zugriffskontrollen, um geschäftskritische SAP-Systeme vor Gefahren durch Mensch und Maschine zu schützen.
- Erfassung und Überwachung der Benutzeraktivitäten in privilegierten Sessions für Mitarbeiter und Dienstleister, was Sicherheitsteams sowohl beim Erkennen als auch beim Verhindern von nicht autorisiertem Zugriff auf privilegierte SAP-Accounts unterstützt.

Effizienz

CyberArk verwaltet SAP-Anmeldeinformationen, indem ein manueller Eingriff überflüssig gemacht und ein sicherer Zugriff ermöglicht wird. Mit einer einzigen Lösung für die Verwaltung von privilegiertem Zugriff in SAP- und anderen Umgebungen vereinfacht CyberArk die Administration privilegierter Accounts und reduziert gleichzeitig den Arbeitsaufwand.

- Erkennung von privilegierten SAP-Accounts und automatisches Onboarding zur Verbesserung der Betriebseffizienz und Minderung von Risiken
- Automatisierte Verwaltung und Rotation von SAP-Administratorpasswörtern, um die für die manuelle Sicherung erforderlichen IT-Ressourcen zu reduzieren
- Priorisierung bei der Durchsicht von Aufzeichnungen privilegierter Sessions anhand von Risikostufen, um die Effizienz zu verbessern und IT-Auditzyklen von SAP-Sessions zu verkürzen und somit die Kosten zu reduzieren

SAP Accounts, die von CyberArk geschützt werden:

- SAP*
- DDIC
- EARLYWATCH
- SAPCPIC
- TMSADM

Compliance

Unabhängig von der Branche brauchen Unternehmen die Möglichkeit, ihre SAP-Umgebung hinsichtlich Richtlinien, Branchenstandards und gesetzlichen Vorschriften bewerten und prüfen zu können. Von allgemeinen IT-Audits und -Berichten über die Durchsetzung interner Kontrollen und die Berichterstattung zur Erfüllung von SOX-Compliance-Anforderungen bis zur Konzentration auf grundlegende DSGVO-Datenschutzanforderungen – CyberArk bietet Unternehmen einen vollständigen Einblick darin, wer auf privilegierte SAP-Accounts zugreift, wann einzelne Mitarbeiter privilegierten Zugriff brauchen und welche Aktionen mit diesen kritischen Accounts durchgeführt werden. Die Verwendung der SAP-Auditfunktionen kann sich als schwierig erweisen, da viele Kunden Dutzende oder sogar Hunderte verschiedene SAP-Systeme und Infrastrukturen verwenden und die Auditfunktionen in einigen Fällen nicht richtig konfiguriert sind.

- Ergänzt SAP-Zugriffs- und Autorisierungskontrollen, um die SAP-Umgebung an den Anforderungen hinsichtlich Governance, Risiko und Compliance (GRC) auszurichten
- Zentrale Verwaltung, Erfassung und Berichterstattung hinsichtlich privilegierter SAP-Anmeldedaten und Kontoaktivität
- Einfache, kosteneffiziente Erstellung von Audit-Berichten über ein zentrales Repository sämtlicher Audit-Daten

Wichtigste Erkenntnisse

Durch diese Partnerschaft von CyberArk und SAP werden die Sicherheits-Best-Practices von SAP-spezifischen Anwendungen auf das gesamte Unternehmen ausgeweitet. Durch das Sichern des privilegierten Zugriffs über ein zentralisiertes, verschlüsseltes Repository wird gewährleistet, dass die richtigen Leute auf die benötigten Systeme zugreifen. Gleichzeitig wird unnötiger Zugriff vermieden. Dank der Möglichkeit, privilegierte Anmeldedaten gemäß Richtlinien rotieren zu lassen, wird sichergestellt, dass kritische SAP-Systeme vor schädlichen Aktivitäten geschützt sind, während Session-Isolation und -Überwachung IT-Administratoren einen umfassenden und automatisierten Audit-Trail liefern, der bei der Erfüllung interner Audits hilft. Darüber hinaus wird die Compliance mit verschiedenen externen Vorschriften gewahrt. Interne Administratoren können Sessions außerdem auf Grundlage von vorab konfigurierten Regeln beenden oder stoppen, wodurch die Sicherheit und erhöhte Effizienz von IT-Teams sichergestellt wird. Gleichzeitig werden Daten erfasst, um eine richtige Verwendung und einen korrekten Zugriff zu gewährleisten.

Über CyberArk

CyberArk ist der globale Marktführer für die Sicherheit von privilegiertem Zugriff und bietet eine kritische Schicht für IT-Sicherheit zum Schutz von Daten, Infrastruktur und Ressourcen im Unternehmen, in der Cloud und in der DevOps-Pipeline. CyberArk liefert die branchenweit kompletteste Lösung zur Minderung von Risiken im Zusammenhang mit privilegierten Anmeldeinformationen und vertraulichen Zugangsdaten. Weltweit führende Unternehmen, darunter mehr als 50 Prozent Fortune-100-Firmen, vertrauen auf CyberArk zum Schutz vor externen Angreifern und böswilligen Insidern. Als globales Unternehmen verfügt CyberArk über Firmensitze in Petach Tikva, Israel, sowie in Newton, Massachusetts, USA. Das Unternehmen besitzt außerdem Standorte in Amerika, EMEA, Asien-Pazifik und Japan.

Mehr über die CyberArk SAP-Lösungen erfahren Sie unter www.cyberark.de.