KuppingerCole Report

EXECUTIVE VIEW

von Martin Kuppinger | Januar 2018

BeyondTrust PowerBroker for Unix & Linux

PowerBroker for Unix & Linux von BeyondTrust bietet Server Privilege Management und Session Management speziell für Unix- und Linux-Server. Solche Server sind häufig Angriffen sowohl von böswilligen Insidern als auch externen Hackern ausgesetzt. PowerBroker for Unix & Linux bietet umfassenden Schutz für privilegierte Accounts auf Unix- und Linux-Plattformen.

von **Martin Kuppinger**
mk@kuppingercole.com
Januar 2018

Inhalt

Verwandte Dokumente

Leadership Compass: Privilege Management - 72330

Executive View: BeyondTrust PowerBroker PAM - 70725

Leadership Brief: Privileged Account Management Considerations - 72016

1 Übersicht

Im Zeitalter der digitalen Transformation verändern sich die Anforderungen an IT - aber auch die Art und Weise, in der IT gehandhabt wird. Unternehmen müssen sich neu erfinden und agiler sowie innovativer werden. Smart Manufacturing und das Internet der Dinge vergrößern ihre Angriffsfläche und sie müssen immer strengere gesetzliche Anforderungen erfüllen. Um mit der gewaltigen Anzahl von Angriffen und den steigenden gesetzlichen Anforderungen Schritt zu halten, müssen Unternehmen auf neue Weise auf diese Herausforderungen reagieren, ohne dabei ihre Kunden zu vernachlässigen. Dies bedeutet, dass sie ihre Sicherheit stetig verbessern und die richtigen Gegenmaßnahmen ergreifen müssen, um Angriffe abzuwehren.

Privilege Management kann heute als Teilbereich der Cyber-Sicherheit betrachtet werden, da Angreifer sich üblicherweise auf hochprivilegierte Accounts konzentrieren. Die Nutzer solcher privilegierter Accounts haben besonders umfangreichen Zugriff auf sensible Unternehmensdaten, wie beispielsweise Personal- und Gehaltsdaten, Finanzdaten oder die IP eines Unternehmens. Aus diesem Grund müssen diese Accounts besonders geschützt werden, um das Risiko von Datenlecks zu verringern. In solchen Szenarien kann Privilege Management den Schutz digitaler Assets erhöhen, indem es besonders empfindliche Accounts sowie ihren Systemzugriff vor Angriffen bewahrt.

Privilege Management ist außerdem ein Teilbereich von IAM (Identity and Access Management), da es nicht nur Accounts und Kennwörter, sondern auch deren Prozesse während der Laufzeit verwaltet, beispielsweise mittels Session Monitoring.

Moderne Privilege Management-Tools müssen eine Vielzahl von Anforderungen erfüllen - vom Schutz für Kennwörter und gemeinsam genutzte Accounts über die regelmäßige Rotation von Kennwörtern für Wartungs- und System-Accounts bis hin zur Überwachung von Sessions und Verhaltensanalysen.

Hochentwickelte Privilege Management-Lösungen gehen weit über das einfache Generieren von Kennwörtern sowie die Zugriffsüberwachung für einzelne Systeme hinaus. Sie bieten vielmehr eine einheitliche, robuste und insbesondere transparente Privilege Management-Plattform, die in die allgemeine IAM-Strategie (Identity and Access Management) eines Unternehmen eingebettet werden kann. Während früher „Kennwort-Vaults" im Mittelpunkt des Interesses standen, spielen heute andere, in umfangreiche Suites integrierte Funktionen, wie z. B. fortgeschrittene Verhaltensanalysen bezüglich privilegierter Nutzer sowie hochentwickelte Session-Überwachungs- und -analysefähigkeiten eine größere Rolle. Allerdings gibt es auch immer mehr Anbieter, die andere Herangehensweisen verfolgen, um das zugrundeliegende Problem der Einschränkung, Überwachung und Analyse von privilegierten Zugriffsrechten sowie die gemeinsame Nutzung von Accounts zu lösen.

Zu den Sicherheitsrisiken in Bezug auf privilegierte Nutzer zählen:

- Anmeldedaten für gemeinsam verwendete Accounts werden publik
- Missbrauch erweiterter Privilegien durch betrügerische Nutzer
- Kaperung privilegierter Accounts durch Cyber-Kriminelle

- Risiken durch den Missbrauch erweiterter Privilegien auf Client-Systemen
- Risiken durch Fehler bei der Nutzung erweiterter Privilegien durch Nutzer

Darüber hinaus gibt es verschiedene Bereiche in Bezug auf Sicherheit sowie Benutzerfreundlichkeit, die mit privilegierten Accounts im Zusammenhang stehen:

- Verwaltung des Besitzes und der Kenntnis aller privilegierter Accounts, sowohl individueller als auch gemeinsam genutzter Accounts
- Single Sign-On für gemeinsam genutzte Accounts für Administratoren und Operator
- Einschränkung der erweiterten Privilegien von Administratoren sowie insbesondere von Operatoren zur Verringerung der damit verbundenen Risiken
- Steuerungsmöglichkeiten zur Verwaltung, Einschränkung und Überwachung des Zugriffs von MSPs (Managed Service-Providern) auf interne Systeme
- Steuerungsmöglichkeiten zur Verwaltung, Einschränkung und Überwachung des Zugriffs von internen Nutzern auf Cloud-Services

In den vergangenen Jahren wurden verschiedene Technologien und Lösungen entwickelt, um all diese Risiken zu verringern und eine verbesserte Aktivitätsüberwachung und Bedrohungserkennung zu erzielen. Ein spezieller Bereich ist der umfassende Schutz von Server-Plattformen mit Unix, Linux oder Windows. Lösungen aus diesem Bereich konzentrieren sich auf den Schutz von „root"-, „admin"- oder ähnlichen Accounts in solchen Systemen, sowie auf den tiefgreifenden Schutz vor ungewollten Erweiterungen von Privilegien und Funktionen, z. B. zur Einschränkung der Nutzung bestimmter Shell-Befehle. Auch wenn diese Tools nicht alle Bereiche abdecken, stellen sie dennoch eine essentielle Komponente in einer umfassenden Privilege Management-Architektur dar, die tiefgreifenden Schutz für bestimmte Zielplattformen bietet.

Eine detaillierte Übersicht über die führenden Privilege Management-Anbieter finden Sie im KuppingerCole Leadership Compass zu **Privilege Management**[1].

2 Produktbeschreibung

BeyondTrust ist ein us-amerikanischer Anbieter für Privilege Access Management- und Vulnerability Management-Lösungen mit Sitz in Phoenix (Arizona). Der im Jahre 1985 ursprünglich unter dem Namen Symark gegründete Anbieter für Identity & Access Management-Lösungen übernahm 2009 zusammen mit einem Software-Unternehmen, das sich auf IAM-Lösungen für Windows spezialisiert hatte, auch den Namen dieses Unternehmens. Heute ist BeyondTrust ein in Privatbesitz stehendes Unternehmen mit über 400 Mitarbeitern und über 4.000 Kunden weltweit.

Seit 2009 hat das Unternehmen verschiedene strategisch wichtige Übernahmen getätigt, wie z. B. eEye Digital Security, Likewise und die Blackbird Group. Auf diese Weise konnte BeyondTrust sein eigenes

[1] Leadership Compass: Privilege Management (#72330)

Portfolio erweitern und seine Produkte in eine umfassende Risk Intelligence-Suite, die BeyondInsight IT Risk Management Platform, überführen. Durch die Kombination zweier Hauptkomponenten - PowerBroker, einer Privileged Access Management-Suite, und Retina, einer Reihe von Schwachstellenmanagementprodukten - ist BeyondTrust in der Lage, Privileged Access Intelligence durch Informationen zu Schwachstellen bezüglich Endgeräten und Webanwendungen zu ergänzen. Auf diese Weise bietet das Unternehmen eine konsolidierte Risikoübersicht sowohl für Corporate-Nutzer als auch für Assets, einschließlich On-Premise-, Cloud- sowie mobiler Ressourcen.

Das Hauptprodukt des Unternehmens ist die BeyondTrust PowerBroker PAM Platform, eine integrierte Produktfamilie für die Verwaltung von Privileged Access, Berechtigungen, Kennwörtern und Anmeldedaten für Unix/Linux-, Windows- und Mac-Systeme, mit denen Anwender die Privilegien von Systemadministratoren auf Server-Systemen (Unix/Linux, Mac, Windows) sowie auf Endgeräten (Mac, Windows) verwalten und anzeigen können.

Im Rahmen dieser Plattform ist PowerBroker for Unix & Linux ein spezialisiertes Produkt zum Schutz bestimmter Zielumgebungen, in diesem Fall Unix- und Linux-Systemen, insbesondere Server. Solche Server spielen nicht nur in vielen Unternehmen, sondern auch in Cloud-Rechenzentren eine große Rolle für die IT-Architektur.

PowerBroker for Unix & Linux kann über 100 verschiedene Unix- und Linux-Distributionen verwalten. Es steuert zentral den Zugriff über Server-Protokolle und bietet eine Funktion zur Aufzeichnung von Tastaturanschlägen während privilegierter Sessions an den Konsolen. Darüber hinaus ist es in der Lage, die Protokolle solcher Sessions zu indexieren, um Audit-Analysen zu beschleunigen.

Für Umgebungen, in denen sudo nicht ersetzt werden kann, bietet BeyondTrust das Produkt PowerBroker for Sudo, das ein zentrales Repository mit Change Management zur Speicherung verschiedener sudo-Konfigurationen für alle unterschiedlichen Hosts sowie eine Funktion zur Definition von Nutzer-/Host-Rollen für das gesamte Unternehmen mit erweiterten Richtliniengruppen umfasst. Ähnliche Funktionen für Windows-Umgebungen bietet PowerBroker for Windows. Ein weiteres enthaltenes Produkt für Server Privilege Management ist PowerBroker Identity Services, das Identity Bridging-Funktionen zwischen Linux-/Unix- und Mac-Systemen sowie Active Directory umfasst.

PowerBroker for Unix & Linux umfasst sechs Kernfunktionen:

- Auditing und Governance für Protokolle und Session-Aufzeichnungen
- Privileged Behavior Analytics zur Identifizierung von Anomalien im Nutzerverhalten
- Feinkörniges Least Privilege- Enforcement auf Unix- und Linux-Systemen
- Dynamische Zugriffsrichtlinie, die Faktoren für fundierte Entscheidungen bezüglich der Erweiterung von Privilegien nutzt
- Auditing und Reporting zu Änderungen in Bezug auf Richtlinien-, System-, Anwendungs- und Datendateien und
- Funktionen zur Steuerung von Remote-Systemen und -Anwendungen

Das Ziel der Lösung besteht darin, Unternehmen die Möglichkeit zur Steuerung des Zugriffs auf wichtige Ressourcen sowie Überwachungsfunktionen zu bieten. PowerBroker for Unix & Linux sammelt verschiedenste Daten über die Aktivitäten von Nutzern in verwalteten Systemen, einschließlich

Tastatureingabeprotokollen und Aufzeichnungen vollständiger Sessions sowie zugehöriger Ereignisse. Diese Ereignisse werden sicher gespeichert und können anschließend für forensischen Untersuchungen, für die Echtzeit-Session-Steuerung sowie für die Privileged Behavior Analytics-Lösung genutzt werden. Dies ermöglicht die Korrelation der gesammelten Informationen mit Schwachstellendaten und Sicherheits-Intelligence aus externen Quellen. Auf diese Weise kann kritisches Verhalten, das beispielsweise im Zusammenhang mit bestimmten bekannten Angriffsvektoren auftritt, identifiziert werden.

Allerdings reicht es nicht aus, im Nachhinein zu verstehen, welche Fehler aufgetreten sind. PowerBroker for Unix & Linux bietet feinkörnige, richtlinienbasierte Steuerungsfunktionen und dynamische Zugriffsrichtlinien, mit denen Unternehmen den Zugriff auf der Grundlage verschiedener Faktoren steuern können, wie z. B. des Standorts oder des Schwachstellenstatus einer Anwendung oder eines Assets. Basierend auf den Richtlinien und zusätzlichen Funktionen kann der Zugriff auf Systeme auf bestimmte Accounts und/oder Funktionen beschränkt werden.

Des Weiteren gibt es Remote-Steuerungsfunktionen, die nicht nur den standardmäßigen, offenen Remote-Zugriff (der ohnehin eine Standardfunktion in Unix- und Linux-Umgebungen ist), sondern auch einen auf bestimmte Befehle und Session beschränkten Remote-Zugriff bieten. Diese Zugriffsfunktion basiert auf Richtlinien und gibt Administratoren die Möglichkeit, eine eingeschränkte Menge von privilegierten Aktivitäten durchzuführen, ohne dass sie sich mit einem Root-Account oder einem anderen hochprivilegierten Account anmelden müssen.

Anders als sudo arbeitet PowerBroker for Unix & Linux nicht auf der Befehls-, sondern auf der Systemebene. Dies bietet eine wesentlich höhere Sichtbarkeit und Kontrolle über alle Systemprozesse, einschließlich der Script-Ausführung. Darüber hinaus können Sessions auf „Root"-Ebene nach wie vor gesteuert werden, indem die Ausführung spezifischer binärer Dateien blockiert und der Zugriff auf sensible Bereiche des Dateisystems eingeschränkt wird.

Zusammengefasst können die Berechtigungen von Nutzern, die Zugriff auf Unix- und Linux-Systeme benötigen, individuell auf dem Least-Privilege-Prinzip entsprechende Zugriffsfunktionen beschränkt werden, während zusätzlich alle Aktivitäten - ob bei eingeschränktem Zugriff oder vollem Root-Zugriff - überwacht, protokolliert und analysiert werden können.

Die aktuelle Version verfügt über eine Reihe von neuen Funktionen. Dazu zählt das File Integrity Monitoring, bei der die Integrität festgelegter Dateien überwacht und Modifizierungen verhindert werden. Dies trägt zur Abwehr von Angriffen bei, bei denen wichtige Dateien durch manipulierte Versionen ersetzt werden.

Eine weitere neue Funktion ist die PowerBroker Servers Management Console, eine zentralisierte, webbasierte Lösung zur Vereinfachung der Implementierung und Verwaltung mehrerer PowerBroker-Lösungen. Das vielleicht wichtigste neue Werkzeug ist der GUI Policy Manager. Damit können IT-Administratoren alle Richtlinien - von rollenbasierten bis hin zu script-basierten Richtlinien sowie Richtlinien zur Überwachung der Dateiintegrität - zentralisiert und ohne eine direkte Befehlszeilenschnittstelle verwalten. Diese Funktion gibt Unix-/Linux-Administratoren mit geringer Erfahrung die Möglichkeit, PowerBroker-Lösungen einzusetzen.

Andere neue Funktionen umfassen detailliertere Session-Aufzeichnungen für schnellere und umfassendere forensische Analysen.

3 Stärken und Herausforderungen

Die PowerBroker-Produktfamilie bietet eine einfach zu handhabende Implementierung zentraler Komponenten. PowerBroker for Unix & Linux ist eine der zentralen Komponenten der angebotenen Lösung und stellt tiefgreifende Privilege Management-Funktionen für Unix- und Linux-Server bereit. Das Produkt bietet alles, was Unternehmen zur Durchsetzung des Least-Privilege-Prinzips, aber auch zur Protokollierung und Analyse von Ereignissen auf solchen Plattformen benötigen.

Zu den besonderen Vorteilen der Produkt-Suite zählt neben der Stabilität des Anbieters, einem langjährigen Akteur im Bereich Privilege Management, auch die Ausgereiftheit der PowerBroker PAM Platform im Allgemeinen, einschließlich der verbesserten Produktintegration, sowie die Ausgereiftheit und Funktionsvielfalt von PowerBroker for Unix & Linux im Speziellen.

Der host-zentrierte Ansatz bezüglich der Verwaltung von privilegierten Systemen ist eine Stärke und eine Schwäche zugleich. Einerseits ermöglicht dieser Ansatz eine tiefe Integration und Steuerung der Zielplattformen, andererseits geht dies zu Lasten geringfügig verlängerter Implementierungs-Timelines. Allerdings ist dies keine funktionale Schwäche des Produkts, sondern eine Folge des Konzepts - der Preis für die tiefe Integration und Steuerung. Insgesamt ist BeyondTrust PowerBroker for Unix & Linux zweifellos ein ausgereiftes, funktionsreiches, stetig weiterentwickeltes Produkt und zählt deshalb zu den führenden Produkten in diesem Bereich.

Stärken	Herausforderungen
• Stabiles Unternehmen mit langjähriger Geschichte • Starke Funktionen zur Verwaltung des privilegierten Zugriffs auf Unix- und Linux-Systeme • Exzellente Unterstützung für eine Vielzahl von Linux- und Unix-Distributionen • Leistungsfähige Protokoll-, Auditing- und Analysefunktionen • Gute Integration des gesamten Produktportfolios • Tiefe Integration in Zielplattformen aufgrund des host-orientierten Ansatzes	• Host-basierter Ansatz für Least Privilege erfordert die Bereitstellung und Verwaltung von Komponenten in verwalteten Systemen • Noch relativ kleines, aber stetig wachsendes Partnernetzwerk auf globaler Ebene, mit starker Präsenz in Nordamerika

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com