DEFENDEER
Data Centric Security Solutions

Risiken von Privilegierten Benutzerkonten reduzieren

STEALTHBITS PRIVILEGED ACTIVITY MANAGER® – sbPAM

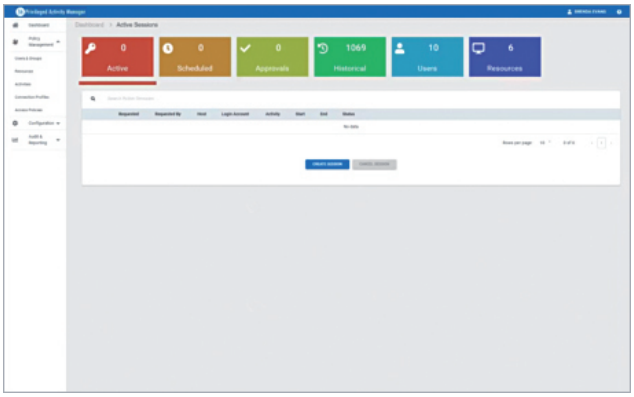
Sichere, prozessgesteuerte Verwaltung von privilegierten Berechtigungen für System- & Datenbankadministratoren in Unternehmen.

Durch die starke Digitalisierung der Geschäftswelt sind auch Datenlecks oder Verletzung der Datenintegrität an der Tagesordnung und verbreiten sich oft durch die Menge an privilegierten Zugriffsberechtigungen durch Benutzerkonten auf Systeme. Diese Konten stehen oft im Zentrum von Angreifern, können aber auch durch Unachtsamkeit zu kompromittierenden Situationen führen.

Viele der heute verfügbaren «Privileged-Access-Management» Produkte fokussieren auf das Verwalten der Zugriffe bzw. administrierten Übernahme von solchen Privilegien durch einen Benutzer. Dieser Ansatz stellt zwar den bedarfsorientierten Zugriff im Moment einem Benutzer zur Verfügung, belässt aber die Berechtigungen des Kontos auch dann, wenn das Konto nicht in Verwendung ist und ermöglich so einem Angreifer sich lateral nach der Übernahme eines Kontos zu bewegen. Dieses Problem verschärft sich umso mehr, wenn Unternehmen einem Administrator (oder -gruppe) mehrere verwaltete Konten zuweisen.

Just-in-Time Privilegierte Berechtigungen bei gleichzeitiger Reduktion der Risiken mit sbPAM

Stealthbits Privileged Activity Manager (sbPAM) stellt den sicheren Verwaltungszugriff auf Systeme mithilfe moderner Technologien zur Verfügung, welche eine einfache und effiziente Implementierung in Ihrer Organisation ermöglichen.



sbPAM erstellt automatisiert temporäre Zugriffskonten für jeden Administrator und stellt dynamisch die benötigen Berechtigungen bedarfsorientiert für die benötigte Aufgabe bereit und entzieht diese anschliessend wieder. Dieser Prozess eliminiert die mögliche Angriffsfläche durch sogenannte stehende Berechtigungen (auch Standing Privileges) wenn Konten nicht verwendet werden. Im Weiteren wird dadurch der Verwaltungsaufwand von komplexer Berechtigungsgruppen stark reduziert.

Ihre Vorteile auf einen Blick

Garantieren Sie berechtigte Zugriffe	Mit der adaptiven «Zero-Trust» Sicherheitsarchitektur kann sichergestellt werden, dass alle privilegierten Zugriffe nach einer mehrstufigen Genehmigung autorisiert sind.
Keine stehenden Berechtigungen	Die erforderlichen Zugriffsrechte werden zum benötigten Zeitpunkt dynamisch bereitgestellt und anschliessen wieder vollständig entzogen.
Erfüllen Sie «Best Practices»	Durchsetzen der Trennung von Berechtigungen für den privilegierten Zugriff von den Standardberechtigungen, mittels automatisierter Verfahren sind die die Prinzipien «Least Privileges» und Need to know» sichergestellt.
Nachvollziehbarkeit und Beweislage sichern	sbPAM zeichnet alle Administrationsaktivitäten während der Session als Video auf, welches bei möglichem Fehlverhalten oder Angriffen im Nachgang zur Kontrolle und Beweissicherung abgespielt werden kann.
Just-in-Time Zugriffe ermöglichen	Privilegierte Zugriffsberechtigungen können dynamisch für einzelne Benutzer, im Dual Modus (temporär oder als Namensvertreter) und für Shared-Accounts bereitgestellt werden.
Reduzieren Sie die Angriffsfläche	Mit sbPAM können Kerberos-Tickets nach der Session automatisch gelöscht werden, um so mögliche Angriffe via Pass-the-Hash oder Golden-Ticket zu verhindern.

DEFENDEER Data Centric Security Solutions, a bluecoons group GmbH Division
Pilatusstrasse 3 | 6300 Zug/Switzerland | www.defendeer.com | +4141 552 02 95

Hauptmerkmale von sbPAM

Keine ruhenden Berechtigungen (Standing Privileges) Die benötigten Berechtigungen zum Ausführen einer geplanten Aktivität werden zum erforderlichen Zeitpunkt erteilt und nach Abschluss der Session wieder vollständig entzogen.	**Unterstützung für kurzlebige Konten** Mit sbPAM können mittels «Activity Tokens» temporäre Berechtigungen und Zugriffsrechte im Moment des Bedarfs automatisch breitgestellt anschliessend wieder gelöscht werden.
Unterstützt BYOV (Bring your own Vault®) sbPAM verfügt über einen eigenen VAULT für die Verwaltung von Anmeldeinformationen, kann aber auch mit bestehenden Vault anderer Hersteller integriert werden umso eine Wiederverwendung bestehender Mittel zu garantieren (Investitionsschutz).	**Sicherstellen Governance für Zugriffsvergaben** Mit sbPAM können die Compiance-Vorgaben bei der Vergabe von privilegieren Berechtigungen eingehalten werden, da die Freigaben mit dem integrierten Workflow-Prozess jederzeit ersichtlich sind und exportiert werden können. Die verlangte Transparenz ist damit garantiert.
Session Recording & Wiedergabe sbPAM verfügt über eine integrierte Aufzeichnungs- & Wiedergabe Funktion der verwalteten Sessions. Damit können im Falle von internen oder externen Nachforschungen oder dem Sicherstellen der Beweiskette die nötigten Nachweise erbracht werden.	**Schnelle & einfache Integration garantiert** Die Architektur von sbPAM ermöglicht eine rasche und einfache Integration in die bestehende Unternehmensinfrastruktur. Im Gegensatz zum Sicherheitsgewinn sind die Betriebsleistungen marginal und durch bestehende Organisationen erfüllbar.

Einfache Konfiguration

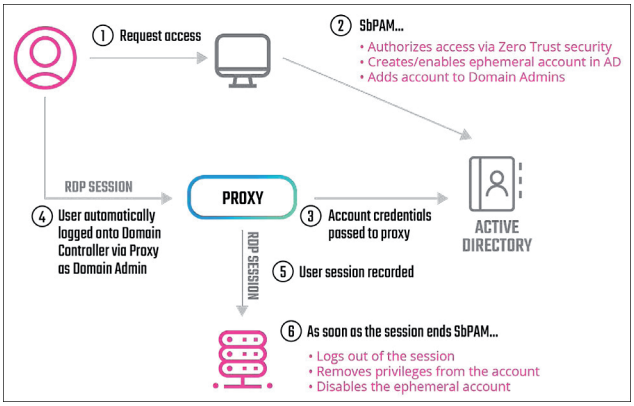
Im Vergleich zu anderen vergleichbaren Verwaltungsinstrumente bietet sbPAM ein einfaches und unkompliziertes Policy-Management, welches aus drei Grundelementen besteht:

- Benutzer: Administratoren, welche einen privilegierten Zugriff benötigen
- Ressourcen: Systeme oder Anwendungen
- Aktivitäten: Schritte zum Einrichten, Überwachen und Löschen von Berechtigungen

Eine Reduktion der Komplexität bei der Verwaltung und Erteilung von Privilegierten Berechtigungen ist der Schlüssel zur Erhöhung der Sicherheit und Einhaltung der Governance Vorgaben. Zugriffe auf kritische Infrastrukturen benötigen klare und verständliche Richtlinien, welche aber auf die Bedürfnisse und Anforderungen jeder Umgebung adaptiert werden können. Die Konfigurationsmöglichkeiten von sbPAM unterstützen diesen Anforderungen im hohen Masse.

Proxy-Element – der kritische Erfolgsfaktor

Werden Systeme direkt von einem Desktop aus verwaltet, werden nicht nur systemische Artefakte auf dem Gerät gespeichert, sondern es müssen zwangsläufig auch Zugänge in sichere Netzwerkzonen eingerichtet werden. Somit bildet der Proxy bei jeder PAM-Lösung das kritische Element, dass die Verbindung zwischen den sicheren Netzwerkzonen und dem Zugriffspunkt zentralisiert, sowie die Funktionen für das Aufzeichnen der Aktivitäten der eingeloggten Administratoren bereitstellt.
Die Proxy-Architektur von sbPAM basiert auf Redundanz und Skalierbarkeit und unterstütze sowohl Windows wie Linux Plattformen. Ein Zugriff kann direkt mittels SSH oder RDM Clients gestartet werden und sbPAM unterstützt eine 2-Faktor Authentisierung aller Verbindungstypen.



Ein wirksames Mittel: Aktivitäten

Angriffsfläche reduzieren

Heute stellen die stetig wachsende Anzahl an privilegierten Benutzerkonten und damit die Erhöhung der Risiken in Bezug auf Verletzbarkeit für Unternehmen eine grosse Last dar. Traditionelle Methoden fokussieren primär auf die Verwaltung dieser Konten, aber nicht auf die damit verbunden Risiken der Möglichkeiten mit den vorhandenen Berechtigungen.
sbPAM steuert dynamisch die Erteilung und den Entzug von Berechtigungen auf Konten. Damit werden die nötigten Berechtigungen im Moment, wo sie benötigt werden bereitgestellt und so garantiert sbPAM das nicht verwendete Konten keine Zugriffsberechtigungen verfügen und so bei einer möglichen Kompromittierung nutzlos sind.

Was sind Aktivitäten?

Unter einer Aktivität versteht sbPAM ein strukturierter Ablauf von Schritten in unterschiedlichen Phasen:

- Phase I: Vor-der-Session (Erteilen von Berechtigungen an einen Benutzer)
- Phase II: Session: (Verbinden des Benutzers mit dem Zielsystem und Starten der Aufzeichnung)
- Phase III: Nach-der-Session (Entfernen der zugeteilten Berechtigungen an den Benutzer

Im Rahmen der Phase I können je nach Konfiguration Konten erstellt, aktiviert und Rollen zugewiesen werden. Die Session bestimmt die eigentliche Art der Aktivitäten wie z.B. Login auf einem Server, Start von Applikationen, Prozessen etc. Die Phase III stellt sicher, dass die bereitgestellten Konten deaktiviert oder gelöscht und die damit verbunden Berechtigungen entzogen werden.