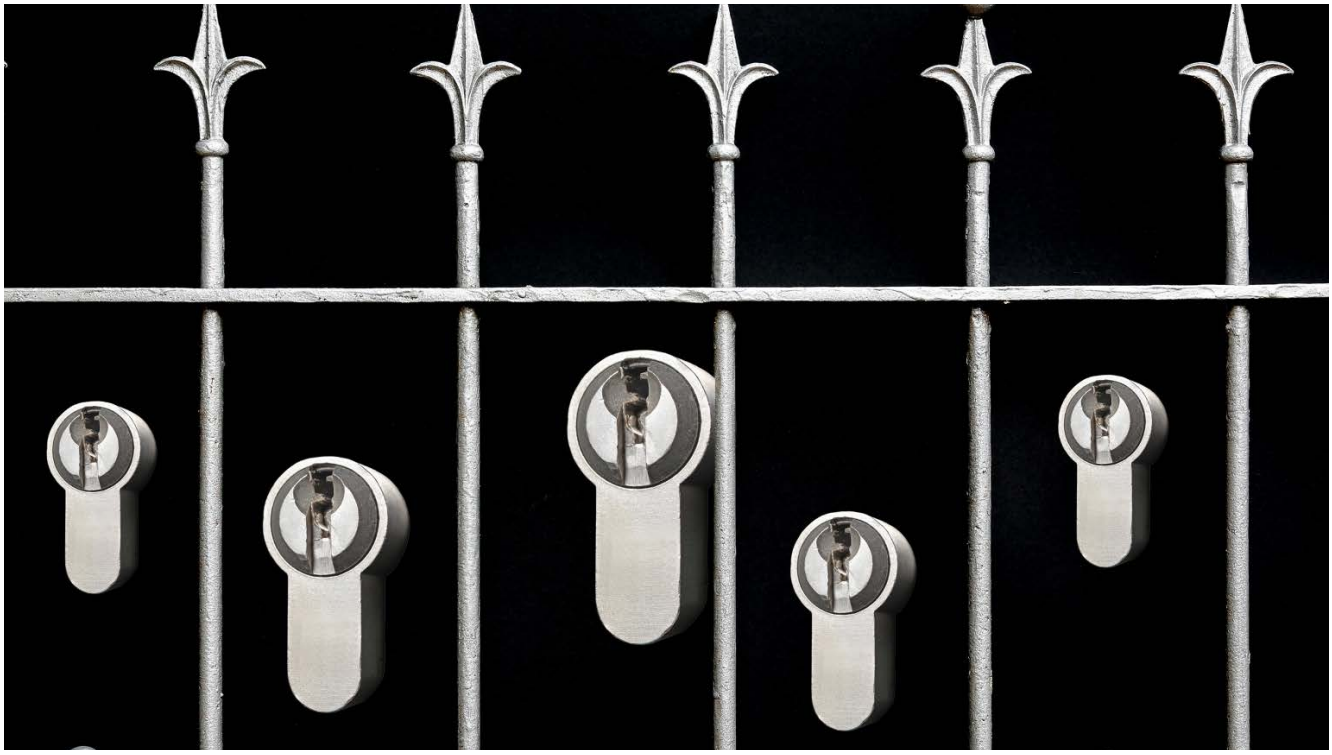


Marktübersicht Privileged-Identity-Management-Software

Nicht für jeden

Marco Lorenz

Privilegierte Konten in Unternehmen sind für Angreifer attraktiv und erfordern besonderen Schutz. Diese Marktübersicht skizziert die Anforderungen und Lösungsansätze und stellt neun Tools vor.

Nicht erst seit Advanced Persistent Threats, Lateral Movement und Datenpannen aufgrund unzureichend gesicherter AWS-Schlüssel wissen Unternehmen um die Herausforderungen bei der Verwaltung privilegierter Zugangsinformationen.

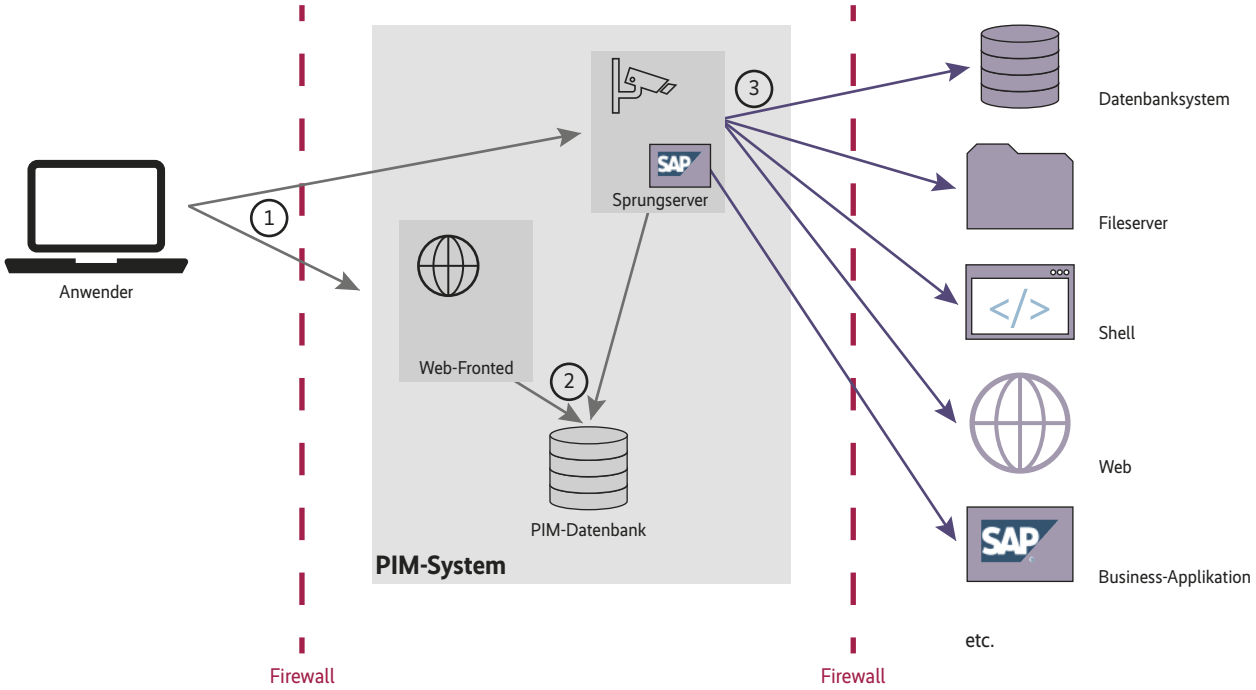
Gemeinhin assoziiert man mit einem privilegierten Konto zunächst den Administrator unter Windows oder den root-Account unter Linux. Allerdings gehören streng genommen alle Konten dazu, die es ermöglichen, privilegierte Aktionen durchzuführen. Demnach ließen sich auch die Benutzerkonten, die beispielsweise im ERP-System die Berechtigung haben, besonders heikle Transaktionen auszulösen, hinzuzählen. Wenngleich die in diesem Artikel vorgestellten Lösungen prinzipiell keinen Unterschied zwischen Betriebssystem und Applikation machen, liegt der Schwerpunkt derzeit klar auf Betriebssystemen.

Wer kennt sie nicht, die mannigfaltigen Excel-Dokumente oder KeePass-Dateien, die auf so manchem Netzwerklaufwerk mit Kolleginnen und Kollegen geteilt werden, um die von der IT-Abteilung geforderten komplexen Passwörter einsetzen zu können. Sie sind schnell eingerichtet und mehr oder weniger komfortabel im Zugriff. Problematisch wird es erst dann, wenn einer der Zugriffsberechtigten keinen Zugriff mehr haben soll. Was tun? Reicht es, das KeePass-Passwort zu ändern? Eher nicht: Der Ehemalige könnte die Datei kopiert haben und immer noch mit dem alten Passwort zugreifen. Konsequenterweise müsste man also auch gleich alle in der Datei gespeicherten Passwörter in den betroffenen Systemen ändern. Wer aber soll das bei mehr als ein paar Dutzend Passwörtern machen? Und: Weiß man, welche Abhängigkeiten zu anderen Prozessen, Systemen und Abteilungen bestehen?

Unter anderem dieses Problem wollen Produkte im Bereich Privileged Identity Management (PIM) lösen. Die hier vorgestellten Werkzeuge können sowohl bei

iX-TRACT

- Privilegierte Nutzer- und System-Accounts stellen ein beliebtes Angriffsziel dar.
- Privileged-Identity-Management-Tools (PIM) helfen Unternehmen, solche Accounts zu verwalten und abzusichern.
- Die vorgestellten Werkzeuge eignen sich sowohl für kleine und mittelständische Unternehmen als auch für den Einsatz in internationalen Großkonzernen.



Ein Sprungserver agiert als Vermittler zwischen dem Client und dem Zielsystem (Abb. 1).

kleinen und mittelständischen Unternehmen als auch bei internationalen Großkonzernen eingesetzt werden.

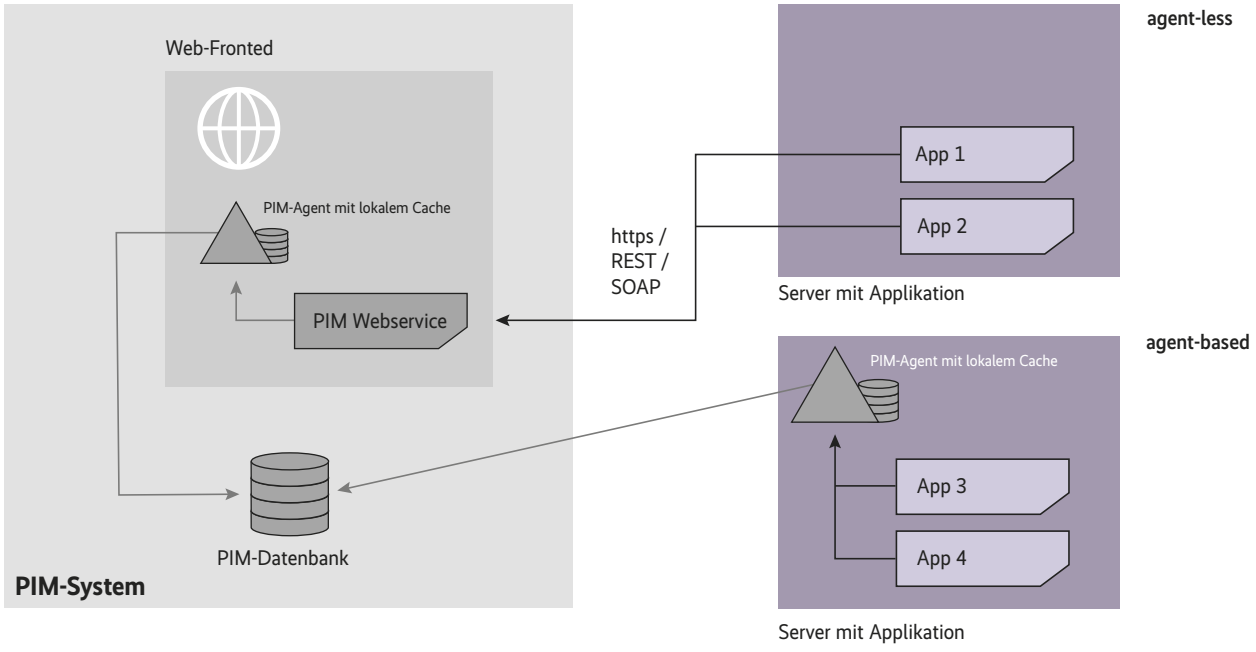
Kennwörter sicher verwalten

Ursprung und Kernkompetenz aller vorgestellten Produkte ist die Verwaltung von Passwörtern. Die angebotenen Funktionen variieren im Detail, was jedoch in der Praxis unwesentlich ist. Hinter dem Begriff der *Verwaltung* eines Passwortes stecken die verschlüsselte Ablage, die Kontrolle des Zugriffs sowie die automatisierte Änderung des Passwortes. Das Erstellen, Ändern und Löschen von Konten hingegen ist die Aufgabe spezialisierter IAM-Tools (Identity and Access Management).

Die meisten Anbieter reichern die Passwortverwaltung noch mit allerlei zusätzlichen Funktionen an. So gibt es oft die Möglichkeit, das Kennwort innerhalb eines definierbaren Zeitraums nach Zugriff zu ändern (one-time password). Dabei ist es unerheblich, ob das Passwort tatsächlich für den Zugriff auf ein System genutzt oder ob es nur angezeigt wurde.

Bei Verwendung von geteilten Konten (shared accounts) bleibt bei paralleler Nutzung durch mehrere Anwender unklar, welche Person zu welchem Zeitpunkt welche Aktion durchgeführt hat. In den Logdateien findet sich allenfalls die Information, dass das Konto „Administrator“ eine bestimmte Änderung durchgeführt hat. Die Lösung dieses Problems besteht bei vielen Herstellern darin, einen exklusiven Zugriff (exclusive access) zu erzwingen. Dabei sperrt der erste Anwender beim Zugriff auf das Passwort automatisch weitere Zugriffe. Nach expliziter Freigabe durch den ersten Anwender wird das Passwort zunächst automatisch geändert, bevor weitere Personen es nutzen können. So will man sicherstellen, dass zu einem Zeitpunkt stets nur ein Anwender Kenntnis vom Passwort hat.

Manche Organisationen fordern zur Durchführung bestimmter Tätigkeiten die Zwei-Personen-Regel (dual control). Auch



Mithilfe einer REST-API lassen sich Anwendungen automatisch mit Zugangsdaten versorgen (Abb. 2).

PIM-PAM-Tools im Vergleich

Hersteller	BeyondTrust	CA Technologies	CyberArk	ManageEngine	Mateso
Produkt	BeyondTrust Password Safe	Layer 7 Privileged Access Manager	Privileged Access Security	ManageEngine Password Manager Pro	Password Safe
Version	6.9	3.2	10.8	10.0	8.7
Angeboten als	Appliance (phys, virt.), Windows Installer	Appliance (phys., virt.), Cloud-Image (AWS, Azure)	Appliance (virt.), Windows Installer	Appliance (virt., AWS, Azure), Windows / Linux Installer	Windows Installer
PIM als Kernprodukt?	ja	nein	ja	nein	ja
Firmensitz	Atlanta, Georgia, USA	San Jose, Kalifornien, USA	Petah Tikva, Israel	Chennai, Indien	Augsburg, Deutschland
Mitarbeiter (Entwickler)	750 (k. A.)	1000 (k. A.)	1146 (287)	7000 (60)	35 (10)
Webseite	www.beyondtrust.com	www.ca.com/de/products/privileged-access-management.html	www.cyberark.com	www.manageengine.com/products/passwordmanagerpro/	www.passwordsafe.de
Passwortverwaltung	ja	ja	ja	ja	ja (Enterprise Plus Edition)
Benutzerschnittstelle	Web	Client, Web	Web	Browser Plugin, mobile App, Web	Browser Plugin, Client, Web
UI Automatisierung	ja	ja	ja	ja	ja (Enterprise Plus Edition)
Voraussetzungen für Passworverwaltung (Produkt / Zielsystem / Netzwerk)	– / – / native Protokolle der Zielsysteme	– / – / native Protokolle der Zielsysteme	ggfs. Datenbanktreiber, Bibliotheken (SAP) / – / native Protokolle der Zielsysteme	– / keine (optional: Agent) / native Protokolle der Zielsysteme	– / – / native Protokolle der Zielsysteme
Passwortarten	Passwörter, SSH-Schlüssel	Passwörter, SSH-Schlüssel	Cloud Keys, Passwörter, SSH-Schlüssel	API / Cloud-Schlüssel, Dateien, Passwörter, SSH-Schlüssel, Zertifikate	Passwörter
typ. Zielsysteme	AWS, Azure, Datenbanken, Firewalls, Linux / Unix, Router, SAP, Switches, VMWare, Windows	AWS, Datenbanken, Firewalls, Linux / Unix, Router, Switches, VMWare, Windows	AWS, Azure, Datenbanken, Firewalls, Linux / Unix, Router, SAP, Switches, VMWare, Windows	AWS, Azure, Datenbanken, Firewalls, Linux / Unix, Router, SAP, Switches, VMWare, Windows	Datenbanken, Linux / Unix, Windows
benutzerdefinierte Metadaten (vorhanden / durchsuchbar / reporting)	ja / nein / nein	ja / ja / ja	ja / ja / ja	ja / ja / ja	ja / ja / teilw.
Onboarding-Möglichkeiten	manuell, REST-API, scan / einmalig, geplant / inklusive	CSV, manuell, REST-API, scan / einmalig, geplant / inklusive	CSV, manuell, REST-API, scan / einmalig, geplant / inklusive	CSV, KeePass, manuell, REST-API, scan / einmalig, geplant / inklusive	CSV, manuell, REST-API, scan / einmalig, geplant / inklusive, API+Scan: Enterprise Plus Edition
Erkennung von Abhängigkeiten	ja	ja	ja	ja	ja (Enterprise Plus Edition)
Offboarding-Möglichkeiten	manuell: API, Web UI	manuell: API, WebUI	manuell: API, WebUI	autom.: markieren gelöschter Konten, manuell: API, WebUI	autom.: AD sync, manuell: Client, WebUI, API (API: Enterprise Plus)
Komplexitätsregeln					
Länge / Zeichensatz	4-128 / Zeichenliste definierbar (blacklist / whitelist)	4-255 / Zeichenliste definierbar (blacklist / whitelist)	keine Einschränkung / Zeichenliste definierbar (blacklist / whitelist)	1-255 / Zeichenliste definierbar (blacklist / whitelist)	3-100 / Zeichenliste definierbar (blacklist / whitelist)

diese Anforderung lässt sich durch eingebaute Freigabeworkflows abbilden. Dabei ermittelt das System statisch (durch feste Rollenzuordnung) oder dynamisch (durch im Verzeichnisdienst zugeordnete Attribute) den Kreis der freigabeberechtigten Personen. Die Benachrichtigungen kommen dabei üblicherweise per E-Mail und die Freigabe einer Anforderung geschieht im jeweiligen Produkt.

Eine Abwandlung der Zwei-Personen-Regel besteht in der gelegentlichen Anforderung, ein split Passwort darstellen zu können. In diesem Fall gibt es üblicherweise zwei Benutzergruppen, die jeweils die erste oder die zweite Hälfte des Passwortes einsehen können. Mit diesem Wissen ist dann eine gemeinsame Passworteingabe möglich. Unternehmen setzen dieses Verfahren jedoch selten ein, da es die Verwendung derselben Systemkonsole erfordert.

Alternativ zur Verwendung der Zwei-Personen-Regel fordern viele Unternehmen die Bindung des Passwortzugriffs an bestehende Abläufe in ihrem ITSM- oder Ticketing-System. Bei dieser ticketing integration gewährt das Tool den Zugriff auf das Passwort nur dann, wenn der anfordernde Nutzer auch im ITSM der aktive Bearbeiter ist und das im ITSM betroffene Zielsystem mit dem Zielsystem in der Passwortverwaltung übereinstimmt. Natürlich sind dabei auch Notfallprozesse möglich, die keine Online-Prüfung im ITSM vornehmen, sondern den Zugriff – mit entsprechender Protokollierung oder Alarmierung – unmittelbar freigeben.

Die Passwortverwaltung wird in der Praxis nicht nur für Konten eingesetzt, die Mitarbeiter interaktiv nutzen, sondern häufig auch für technische Konten, die bestimmte Dienste oder Batch-Jobs benötigen. Bei dieser Art von Konten reicht es nicht, das Kennwort im jeweiligen System (wie Active Directory) zu ändern. Es müssen auch die spezifischen Abhängigkeiten (account dependencies) berücksichtigt werden: Die Passwortänderung eines Windows-Kontos erfordert auch die Anpassung der Konfiguration von Diensten, die dieses Konto nutzen, da der Dienst sich andernfalls nicht mehr neu starten lässt. Die Berücksichtigung derartiger Abhängigkeiten ist je nach Anbieter unterschiedlich stark ausgeprägt. Windows-Dienste und geplante Aufgaben gehören zum Standard-Repertoire, COM-Objekte, IIS-Application Pools oder die Anpassung von Registry oder Konfigurationsdateien sind weniger häufig zu finden.

Alle Anbieter führen die Änderung von Passwörtern im Zielsystem ohne Agenten und unter Nutzung der für die jeweilige Plattform üblichen Protokolle durch: SMB/CIFS oder WMI für Windows, SSH

	Micro Focus	One Identity	Thycotic	Wallix
	NetIQ Privileged Account Manager	One Identity Safeguard	Thycotic Secret Server	WALLIX Bastion
	3.6	2.6, 5.11 (Bundle)	10.6	7.0
	Installer	Appliance (phys., virt., AWS, Azure)	Windows Installer	Appliance (phys., virt.)
	nein	nein	ja	nein
	Newbury, Berkshire, Großbrittanien	Aliso Viejo, Kalifornien, USA	Washington DC, USA	Paris, Frankreich
	14000 (19)	800 (122)	400 (50)	140 (50)
	www.microfocus.com/de-de/products/netiq-privileged-account-manager	www.oneidentity.com/one-identity-safeguard/	www.thycotic.com	www.wallix.com
	ja	ja	ja	ja
	Web	Client, Web	Client, mobile App, Web	Client, Web
	ja	ja	ja	ja
	„PAM Taskmanager" / – / native Protokolle der Zielsysteme	– / Stellvertreter-Konto / native Protokolle der Zielsysteme	– / – / native Protokolle der Zielsysteme	– / – / native Protokolle der Zielsysteme
	Cloud / API-Schlüssel, Passwörter, SSH-Schlüssel	Passwörter, SSH-Schlüssel	Passwörter, SSH-Schlüssel, Zertifikate	Passwörter, SSH-Schlüssel, Zertifikate
	AWS, Azure, Datenbanken, Firewalls, Linux / Unix, Router, SAP, Switches, VMWare, Windows	AWS, Datenbanken, Firewalls, Linux / Unix, Router, SAP, Switches, VMWare, Windows	AWS, Azure, Datenbanken, Firewalls, Linux / Unix, Router, SAP, Switches, VMWare, Windows	Datenbanken, Firewalls, Linux / Unix, Router, Switches, VMWare, Windows
	nein / – / –	ja / ja / ja	ja / ja / ja	nein / – / –
	manuell, scan / einmalig, geplant / inklusive	manuell, REST-API, scan / einmalig, geplant / inklusive	CSV, manuell, REST-API, scan / einmalig, geplant / inklusive	CSV, manuell, REST-API, scan / einmalig, geplant / inklusive
	ja	ja	ja	ja
	manuell: WebUI	autom.: LDAP sync, manuell: API, Web UI	autom.: AD sync (separate Lizenz: Account Lifecycle Manager)	manuell: API, WebUI
	keine Angaben / Zeichenliste definierbar (blacklist / whitelist)	3-255 / Zeichenliste definierbar (blacklist / whitelist)	1-999 / Zeichenliste definierbar (blacklist / whitelist)	unbegrenzt / Zeichenliste voreingestellt

für Linux/Unix und Netzwerkgeräte, SQL für Datenbanken. Dabei erbt die Passwortänderung naturgemäß die Stärken und Schwächen des jeweiligen Protokolls. Auf den Einsatz von Klartextprotokollen sollte man daher nicht nur bei diesem Verwendungszweck verzichten.

Alles noch ganz dicht?

Ergänzend zur Passwortänderung ist eine regelmäßige Überprüfung (password verify) vor allem dann sinnvoll, wenn Anwender die Möglichkeit haben, das Passwort auf dem betroffenen System zu ändern. Das ist zum Beispiel der Fall, wenn die im Produkt gespeicherten Passwörter angezeigt oder in die Zwischenablage übernommen werden können: Der Anwender wäre in der Lage, das Passwort auf einfache Art und Weise zu ändern.

Ein anderes Szenario ist die Wiederherstellung eines Systembackups, das vor dem letzten Passwortwechsel durchgeführt wurde. Da wäre die Verwaltungssoftware nicht mehr in der Lage, das Passwort zu ändern, da das aktuelle nicht mit dem im Backup gespeicherten Passwort übereinstimmt. Die Überprüfung stellt hier sicher, dass solche Abweichungen frühzeitig erkannt werden. Einige Produkte bieten für solche Fälle die Möglichkeit, automatisiert einen Rücksetzprozess (reconciliation, password sync) anzustoßen. Dabei kommen stets zusätzliche Konten ins Spiel, die auf dem jeweiligen System das Recht besitzen, Passwörter anderer Konten zurückzusetzen.

Beim Generieren von Passwörtern unterstützen die vorgestellten Tools die üblichen Anforderungen an die Komplexität und die Länge (complexity rules). Die in Unternehmen oft anzutreffenden Richtlinien zu Komplexitätsvoraussetzungen, Kennwortchroniken sowie minimalem und maximalem Kennwortalter sind bei Einsatz eines Automaten zum Passwortwechsel meist überflüssig (Passwörter werden zufällig erzeugt und zuverlässig im gewünschten Zeitrahmen geändert) und teilweise sogar hinderlich (Mindestalter kollidiert mit Passwortänderung nach Nutzung).

Alle Anbieter speichern die Passwortinformationen in einem strukturierten Format. Es enthält neben dem Kennwort selbst Metadaten, die für die Verwaltung relevant sind. Dazu gehören die offensichtlichen Informationen wie Benutzername, Adresse des Zielsystems und Zielsystemtyp. Je nach Anbieter kommen noch andere Metadaten hinzu.

Firmen nutzen diese Möglichkeit oft, um Kommentare oder Verweise auf andere Systeme zu hinterlegen. Beim auto-

PIM-PAM-Tools im Vergleich

Hersteller	BeyondTrust	CA Technologies	CyberArk	ManageEngine	Mateso
Historie / Zeichenwiederholung / aussprechbar	nein / nein / nein	ja / ja / nein	ja / ja / nein	ja / nein / nein	nein / nein / ja
weitere Funktionen					
Überprüfung (password verify) auf Anforderung / geplant	ja / ja	ja / ja	ja / ja	ja / ja	ja / ja
Zurücksetzen (reconcile) vorhanden / automatisch / manuell	ja / ja / k. A.	ja / ja / k. A.	ja / ja / ja	ja / ja / ja	ja / ja / k. A.
Zwischenablage Copy & Paste / auto-clear	ja / nein	ja / nein	ja / ja	ja / ja	ja / ja
Workflows exclusive access / one-time password / dual-control / split password	ja / ja / ja / nein	ja / ja / ja / nein	ja / ja / ja / ja	ja / ja / ja / nein	ja / ja / ja / teilw.
Ticketing Integration	ja (BMC Remedy, CA ServiceDesk, JIRA, ServiceNow)	ja (BMC Remedy, CA Service Desk Manager, HP Service manager)	ja (BMC Remedy, ServiceNow, custom)	ja (JIRA, ServiceDesk Plus, ServiceNow)	nein
Sitzungsverwaltung (session management)	ja	ja	ja	ja	ja (Enterprise Plus Edition)
Funktionen Sitzungsverwaltung Architektur / Protokollsupport / Aufzeichnung ohne verwaltetes Passwort	agent-less / RDP, SSH / ja	agent-based, jump host, SSH / telnet Proxy / HTTPS, RDP, SSH, Telnet, VNC / nein	jump host / abhängig vom verwendeten Client / ja	jump host / RDP, SQL, SSH, VNC / ja	agent-less / Browser Plugin, RDP, SSH / nein
Sitzungsaufzeichnung (session recording)	ja	ja	ja	ja	ja
Einschränkung nach Benutzer und Gruppen / Zielsystem	ja / ja	ja / ja	ja / ja	ja / ja	nein / ja
Live Session Monitoring unterstützt / Auditor je Zielsystem	ja / ja	nein / –	ja / ja	ja / nein	nein / –
live session termination unterstützt / durch Auditor / durch Ereignis	ja / ja / teilweise	ja / ja / ja	ja / ja / ja	ja / ja / nein	– / – / –
Aufzeichnungen Format / Indizierung / OCR	proprietär / ja / nein	k. A. / ja / nein	AVI, Text / ja / nein	proprietär/ja (SSH, SQL) / nein	JPG / nein / nein
Aufzeichnungszugriff verfügbar / Zugriffsbeschränkung nach Nutzer / Zugriffsbeschränkung nach Zielsystem / dual-control	Sitzungsende / ja / ja / nein	Sitzungsende/ja / ja / nein	Text: unmittelbar, Video: Sitzungsende / ja / ja / ja	Sitzungsende / ja / ja / nein	währenddessen / ja / ja / nein
Integration mit Applikationen (AAPM)	ja	ja	ja (Zusatzlizenz)	ja	teilw.
AAPM Architektur / Zugriffsprotokoll	AAPM API / REST	AAPM agent / HTTP, REST	AAPM agent, AAPM API, credential push / REST	AAPM API / REST, XML-RPC	AAPM agent / REST

matisierten Zugriff wäre es daher denkbar, hier weitere Statusinformationen, die für den Automatisierungsprozess relevant sind, abzulegen.

Sitzungsverwaltung

Die reine Passwortverwaltung wie oben beschrieben ist heutzutage kaum noch anzutreffen. Nahezu alle Anbieter ermöglichen per Knopfdruck eine Remote-Sitzung zum gewünschten Zielsystem unter Verwendung der verwalteten Passwortinformationen herzustellen. Eine solche interaktive Sitzung lässt sich in der Regel auch aufzeichnen, sodass nachvollziehbar bleibt, wer, wann, wo und wie lange welche Aktionen durchgeführt hat – oder eben auch nicht. Bei dieser Sitzungsverwaltung kommen unterschiedliche Architekturen zum Einsatz: Es gibt Sprungserver, Proxys und client-basierte Verfahren; letztere sowohl agentenbasiert als auch ohne vorinstallierten Agenten (agent-less).

Eine Motivation zur Sitzungsverwaltung ist, das verwaltete Passwort möglichst nicht gegenüber dem Anwender zu exponieren. Einerseits aus Gründen der Bequemlichkeit (wer will schon gerne 20-stellige, komplexe Passwörter eintippen?) und andererseits aus Sicherheitsgründen (Schadsoftware könnte die Passwörter auf Endgeräten abfangen und nutzen).

Die Verwendung eines Sprungservers (jump host) bietet derzeit die größte Isolation privilegierter Passwörter gegenüber einer möglichen Kompromittierung. Das Prinzip ist immer gleich: Ein vom Anbieter der Lösung zur Verfügung gestellter Server agiert als eine Art Proxy für den Verbindungsaufbau zum gewünschten Zielsystem. Will der Anwender beispielsweise eine RDP-Verbindung zum Dateiserver herstellen, erfolgt der Verbindungsaufbau

	Micro Focus	One Identity	Thycotic	Wallix
	ja / ja / nein	nein / ja / nein	nein / nein / nein	ja / ja / nein
	ja / ja	ja / ja	nein / ja	nein / nein
	ja / nein / ja	ja / ja / ja	ja / nein / k. A.	ja / nein / k. A.
	nein/-	ja / nein	ja / nein	ja / nein
	ja / ja / ja/ nein	ja / ja / ja / nein	ja / ja / ja / teilw.	ja / ja / ja / nein
	ja (ServiceNow)	ja (BMC Remedy, ServiceNow)	ja (BMC Remedy, ServiceNow, custom)	ja (k. A.)
	ja	ja	ja	ja
	agent-based, jump host / RDP, SQL, SSH, abhängig vom verwendeten Client / ja	proxy-based / HTTPS, ICA, RDP, SSH, Telnet, TN3270, TN5250, VNC / ja	agent-less, jump host (optional) / abhängig vom verwendeten Client / ja	jump host / RDP, RLOGIN, SSH, VNC / ja
	ja	ja	ja	ja
	ja / ja	ja / ja	ja / ja	ja / ja
	ja / ja	ja / ja	ja / nein	ja / ja
	ja / ja / ja	ja / ja / ja	ja / ja / nein	ja / ja / ja
	WebM / ja / nein	proprietär / ja / ja	MPEG / ja / nein	MP4 / ja / ja
	währenddessen / ja / ja / ja	währenddessen / ja / ja / ja	Sitzungsende / ja / nein / ja	Sitzungsende / ja / ja / nein
	ja	ja	ja	ja
	k. A. / REST	AAPM API / REST	AAPM agent, AAPM API, credential push / REST	AAPM API / REST

vom Anwender-Desktop zum Sprungserver und von dort zum Zielsystem. Der Sprungserver startet dabei seinerseits einen lokalen RDP-Client und befüllt diesen mit den notwendigen Zugangsdaten und Adressen (siehe Abbildung 1). So verbleiben die Zugangsdaten stets im Speicher des Sprungservers und gelangen nicht zum Anwender-Desktop.

Je nach Anbieter basieren die Sprungserver auf unterschiedlichen Plattformen und Technologien. Einige Produkte nutzen Windows Server oder Remote Desktop Server (in Version 2012 oder 2016), andere bieten dafür selbst entwickelte (Linux-)Appliances. Beim regulären Remote Desktop Server ist die Flexibilität hinsichtlich unternehmensspezifischer Applikationen am größten. RDP und SSH sind vergleichsweise einfache Standardprotokolle, für die es Client-Applikationen auf allen relevanten Plattformen gibt. Beim Einfüllen der Zugangsinformationen können die Tools daher auf verbreitete Schnittstellen zurückgreifen.

Anders sieht es bei weniger häufig genutzten Applikationen wie beispielsweise einem SAP GUI oder einem Datenbankwerkzeug wie Toad aus. Hier gibt es keine einheitlichen Schnittstellen. Noch schwieriger sind die weit verbreiteten Browser-basierten Schnittstellen, wie sie unter anderem in Netzwerkdruckern, VoIP-Telefonen, Management-Boards (iLO, DRAC, et cetera) und Security-Appliances zu finden sind: Ein automatisches Befüllen von Anmeldeformularen scheitert häufig daran, dass die entsprechenden Formulare erst mittels JavaScript auf Client-Seite generiert oder gerne auch als Flash-Objekte eingebunden werden. Tastaturkürzel oder eindeutige Merkmale im HTML-DOM sind dann selten zu finden. Viele Werkzeuge zur Administration im Windows-Umfeld sind MMC-basiert und

PIM-PAM-Tools im Vergleich

Hersteller	BeyondTrust	CA Technologies	CyberArk	ManageEngine	Mateso
Authentifikation	Benutzer / Passwort, API Key, Source IP, Client Zertifikat	Benutzerkonto, Hash, Pfad	Adresse, Applikationsname, Benutzerkonto, Hash, Hostname, Zertifikat	SSH-CLI: public key, XML-RPC: Zertifikat, REST: API-Key + Hostname	k. A.
Offline-Fähigkeit	ja (Agent)	ja (Agent)	ja (Agent)	nein	ja
Anomalieerkennung (threat analytics)	ja	ja (separate Lizenz)	ja	nein	nein
Erkennung autom. Baseline / Umgehungserkennung / Sitzungsanalyse / Pass-the-Hash / Kerberos Golden Ticket	ja / nein / ja / nein / nein	ja / nein / ja / nein / nein	ja / ja / ja / ja / ja	nein / nein / nein / nein / nein	nein / nein / nein / nein / nein
Reaktion Sitzungstrennung / Passwortänderung	ja / ja	ja / ja	ja / ja	nein / nein	nein / nein
Benutzerverwaltung					
Verzeichnisdienste	Active Directory	Active Directory, CA Directory, Red Hat, LDAPv3	Active Directory, eDirectory, OpenLDAP, Oracle Internet Directory	Active Directory, Azure Active Directory, LDAPv3	Active Directory
Authentifizierungsverfahren	Kerberos, LDAP, RADIUS, SAML, SSO	LDAP, lokal, NTLM / Kerberos, PKI, RADIUS, SAML, TACACS+	LDAP, NTLM / Kerberos, PKI, RADIUS, SAML, SSO	Azure Active Directory, LDAP, lokal, NTLM / Kerberos, PKI, RADIUS, SAML: ADFS, Okta, OneLogin	LDAP, NTLM / Kerberos, PKI, RADIUS
mehrere Verfahren parallel?	ja	nein: globale Einstellung	ja	ja	ja
Fallback (z. B. SmartCard -> RADIUS)	nein	ja: SmartCard -> RADIUS	nein	ja: extern -> intern	nein
2-FA Unterstützung	via RADIUS	via RADIUS, RSA, SmartCard, SAML	via OAUTH, RADIUS, SAML	via DUO, Google Authenticator, Microsoft Authenticator, Okta Verify, PhoneFactor, RADIUS, RSA SecurID, YubiKey	Google Authenticator, PKI, RADIUS, RSA, SafeNet, Yubico
Betrieb & Sicherheit					
Verschlüsselung					
Ort der Verschlüsselung / data-at-rest / data-in-motion	Produkt / AES-256 / AES-256	Produkt / AES-256 / TLS 1.2	Produkt / AES-256, RSA-2048 / AES-256, RSA-2048	Produkt + Datenbank / AES-256 / AES-256	Produkt + Datenbank / AES-256, RSA-4096, PBKDF2 / TLS1.2
Schlüsselkonzept / Schlüsselwiederherstellung / HSM-Support	gemeinsamer Schlüssel für alle Passwörter / Schlüssel Backup möglich / ja (über PKCS#11-Treiber)	gemeinsamer Schlüssel für alle Passwörter / nein („Schlüssel geht nicht verloren") / ja	eigener Schlüssel je Passwort und Version / Wiederherstellungsschlüssel / ja	gemeinsamer Schlüssel für alle Passwörter / k. A. / ja	eigener Schlüssel je Container / Recovery-Mechanismus / ja (über PKCS#11-Treiber)
Protokollierung					
Integritätssicherung / Abdeckungsgrad / (SIEM) Anbindung	Berechtigungskonzept, Appliance-Kapselung / alle Aktivitäten / ja, syslog	Berechtigungskonzept, Appliance-Kapselung / alle wesentlichen Applikationsvorgänge / ja, syslog	RBAC, Verschlüsselung / alle wesentlichen Applikationsvorgänge / ja, syslog	RBAC und Verschlüsselung / alle wesentlichen Applikationsvorgänge / ja, syslog, SNMP traps	Verschlüsselung / alle Aktivitäten / ja, syslog, API
Reporting					
Reporting / Zugriff auf Rohdaten	vodefinierte Templates / ja	vordefinierte Templates / teilweise (Datenexport möglich)	vordefinierte Templates / ja	vordefinierte Templates / ja (SQL)	vordefinierte Templates / ja

bieten keinen expliziten Authentifizierungsdialog an. Stattdessen nutzen sie beispielsweise die vorhandenen Kerberos-Tickets der aktuellen Benutzersitzung. Solche Applikationen lassen sich mittels Run-As auf den Sprungservern nutzen.

Entscheidet man sich für den Sprungserver-Ansatz, müssen alle relevanten Applikationen und Zugangsprogramme auf dem Sprungserver installiert sein, um sie nutzen zu können. Das ist in der Praxis nicht trivial: Manche Administrationsprogramme setzen noch Java 8 voraus, während andere erst ab Java Version 10 funktionieren. Wieder andere Programme installieren zusätzlich einen MS SQL Server Express, um Einstellungen zu speichern. Die gegenseitigen Abhängigkeiten und Inkompatibilitäten erfordern daher fast immer die Nutzung mehrerer, dedizierter Sprungserver.

Im Hinblick auf die Integration im Netzwerk sind Architekturen ähnlich, die einen Application Layer Proxy (auf Schicht 7 des OSI-Modells) zur Verfügung stellen. Dabei kann dieser Proxy explizit angesprochen oder vom Netzwerkrouter als next hop auf dem Weg zum Zielserver zum Einsatz kommen. Zur Aufzeichnung der Sitzungsinhalte muss die Software verschlüsselte Verbindungen aufbrechen. Eine solche Implementierung stellt den Hersteller vor besondere Herausforderungen, da sein Produkt bei Protokoll-Änderungen (wie neue RDP-Funktionen) nachziehen muss. Darüber hinaus lassen sich in der Praxis nur ausreichend dokumentierte Protokolle sinnvoll im Proxy untersuchen.

Die Nutzung einer Client-basierten Sitzungsverwaltung umgeht einige dieser Probleme. Die beim Sprungserver beschriebenen Inkompatibilitäten treten hier seltener auf, da die rivalisierenden Programme oft nicht parallel installiert sind: Selten ist der Datenbankadministrator

	Micro Focus	One Identity	Thycotic	Wallix
	API Key	API key + Zertifikat	Adresse, Benutzerkonto, Hostname	k. A.
	nein	nein	ja (Agent)	ja
	nein	ja	ja (separate Lizenz)	ja
	nein / nein / ja / nein / nein	ja / nein / ja / nein / nein	ja / nein / nein / nein / nein	nein / nein / ja / nein / nein
	ja / nein	ja / nein	nein / nein	ja / nein
	Active Directory, eDirectory, OpenLDAP	Active Directory, OpenLDAP	Active Directory	Active Directory, LDAPv3
	LDAP, NTLM / Kerberos, SSO	lokal, LDAP, PKI, RADIUS, SAML, SSO	NTLM / Kerberos, PKI, SAML, SSO	LDAP, NTLM / Kerberos, PKI, RADIUS, SAML, SSO, TACACS+
	ja	ja	nein: globale Einstellung	ja
	ja	nein	nein	ja
	eigene: Microfocus Advance Authentication	via RADIUS, SafeGuard 2-FA	via DUO, Email, Google Authenticator, RADIUS, SAML	via RADIUS
	Produkt / AES-256 / TLS 1.2	Produkt / AES-256 / TLS 1.2	Produkt / AES-256 / TLS	Produkt / AES-256, CHACHA20 / TLS
	eigener Schlüssel je Objekt / k. A. / nein	gemeinsamer Schlüssel für alle Passwörter, optional: unterschiedliche Schlüssel für Aufzeichnungen / Wiederherstellungsschlüssel / ja	eigener Schlüssel je Passwort / Schlüsselbackup möglich / ja	k. A. / ja / k. A.
	Verschlüsselung / alle Aktivitäten / ja	RBAC / alle Aktivitäten / syslog	k. A. / alle Aktivitäten / ja, syslog	digitale Signatur / alle Aktivitäten / ja
	vordefinierte Templates / ja	vordefinierte Templates / ja	vordefinierte Templates / ja	vordefinierte Templates / ja

auch gleichzeitig für die Firewall zuständig. Das Befüllen der jeweiligen Applikationen geschieht teilweise über lokal installierte Agenten, die – ähnlich wie das Desktop-Tool KeePass – die Möglichkeit bieten, Benutzername und Passwort über die Zwischenablage oder Formularfeld-Erkennung einzuspeisen.

Bei den Browser-basierten Schnittstellen werden in der Regel auch Browser-Plug-ins angeboten, die dasselbe leisten, bei Formularfeldern auch das automatische Befüllen. Dabei existieren grundsätzlich die gleichen Herausforderungen wie auch beim Sprungserver: Wie kann die Software Eingabefelder zuverlässig erkennen und befüllen? Bei der agentenlosen Variante findet diese Konfiguration für die bekannten Applikationen typischerweise an zentraler Stelle statt. Fordert ein Anwender eine Verbindung an, generiert die Sitzungsverwaltung eine ausführbare Datei (Wrapper), die auf dem Endgerät des Anwenders zur Ausführung kommt. Sie startet die gewünschte Applikation und befüllt diese mit Zugangsdaten. Bei Beendigung der Sitzung wird auch die Wrapper-Anwendung wieder entfernt.

Alle beschriebenen Architekturen bieten die Möglichkeit, Sitzungen auch aufzuzeichnen (session recording). Dabei stehen zur Steuerung diverse Filtermöglichkeiten zur Verfügung, darunter Anwender und Anwendergruppen sowie Zielsystem und Zielsystemgruppen.

Einige Lösungen bieten zusätzlich die Möglichkeit, Sitzungen mittels Session Monitoring live zu beobachten. Bei Sprungservern ist hierfür die bei Microsoft integrierte Spiegeltechnik (session shadowing) zuständig. Je nach Konfiguration kann man beobachtete Sitzungen auch auf Knopfdruck terminieren.

Kommt es zu einem Vorfall, bei dem die Auswertung der Aufzeichnungen eine

Rolle spielt, möchte kaum jemand stundenlang Videomaterial sichten müssen. Daher bieten fast alle Anbieter die Möglichkeit, Aufzeichnungen zu verschlagworten. Bei textbasierten Sitzungen wie SSH ist zusätzlich eine Volltextsuche möglich.

Beide Ansätze (Jumpserver/Proxy und Client-basiert) haben ihre spezifischen Vor- und Nachteile. Sprungserver bieten den Vorteil, dass der Konfigurationsaufwand auf Client-Seite fast komplett entfällt (der Client benötigt lediglich einen Zugangsclient zum Sprungserver). Weiterhin isolieren sie die sensiblen Passwortinformationen nahezu vollständig vom möglicherweise kompromittierten Client-System. Auf der Netzwerkebene lassen sich zudem Zugriffe auf die Administrations-Ports von Serversystemen mithilfe von Firewalls auf die Sprungserver beschränken.

Eher von Nachteil ist bei den Sprungservern der notwendige Betriebsaufwand: Je nachdem, wie viele nicht-kompatible Applikationen vorhanden sind, kann es erforderlich sein, viele Sprungserver bereitzustellen. Auch die Systemlast spielt eine entscheidende Rolle: Beispielsweise empfehlen einige der Tool-Anbieter, nicht mehr als 100 parallele Sitzungen je RDS-Server durchzuführen. In großen Unternehmen mit mehreren tausend Anwendern landet man so schnell bei vier bis fünf nicht redundanten Serversystemen mit 32-Kern Prozessoren ab 32 GByte RAM.

Architekturen, die ohne Sprungserver auskommen, haben in der Regel keine der zuvor beschriebenen Ressourcenprobleme. Im Vergleich zu den Sprungservern erfordern sie jedoch fast immer direkte Netzwerkverbindungen zum Zielsystem. Das verwendete Passwort wird zumindest kurzfristig im Hauptspeicher gehalten, wo es anfällig gegenüber gezielten Angriffen durch Schadsoftware ist.

Automatisierung und Applikationen

Kaum ein mittleres oder großes Unternehmen administriert seine Systemlandschaft ausschließlich manuell. Stattdessen kommen Automatisierungswerkzeuge zum Einsatz, die über Agenten oder Netzwerkverbindungen vordefinierte administrative Aufgaben durchführen. Die Zugangsdaten für die Systeme sind in vielen Fällen die gleichen. Das freut im Zweifelsfall auch etwaige Angreifer: Gelingt der Einbruch in ein einzelnes System, verfügen sie unmittelbar über administrativen Zugriff auf viele weitere Systeme.

Auch Web-Applikationen und Batch-Jobs benötigen regelmäßig Zugangsdaten zu weiteren Systemen. Nicht selten fordern Penetrationstests Zugangsdaten zu Datenbank-Backends und anderen Drittsystemen zutage. Deren Speicherung geschieht immer noch häufig im Klartext in den zugehörigen Konfigurationsdateien. Ein Spezialfall sind Schwachstellenscanner (siehe ix.de/z3mx), die privilegierte Zugangsdaten verwenden, um Detailinformationen vom gescannten System zu ermitteln. Auch bei diesen Systemen liegen die benötigten Zugangsdaten im Klartext oder zumindest reversibel vor.

Fragt man Unternehmen nach ihrer Passwortrichtlinie für Benutzeraccounts, geben viele die einschlägigen Antworten hinsichtlich Komplexität, Länge und Wechselintervall. Stellt man dieselbe Frage in Bezug auf Systemkonten, erhält man stattdessen die Antwort, dass solche Passwörter zwar komplex sein, aber nicht geändert werden müssen. Das liegt fast immer an den vielen Abhängigkeiten: Ändert man das Passwort im Verzeichnisdienst, muss die gleiche Änderung auch an vielen anderen Stellen passieren. Leider wissen viele Unternehmen oft gar nicht, welche diese „anderen Stellen“ sind, und ändern daher aus Angst vor etwaigen Ausfällen diese Passwörter lieber gar nicht.

Zwar lösen die betrachteten Produkte das Problem der „anderen Stellen“ nicht, aber sie bieten zumindest die Möglichkeit, bekannte Abhängigkeiten bei der Passwortänderung zu berücksichtigen oder die betroffenen Systeme anzubinden und so administrative Aufwände zu reduzieren.

Hierzu bieten sie Schnittstellen an, über die sie Applikationen mit den benötigten Zugangsdaten versorgen können. Dies ermöglicht nicht nur, die Speicherung der Informationen aus der Applikation auszulagern, sondern auch die regelmäßige Änderung der jeweiligen Passwörter. Zudem ist der Aufwand bei der Verwendung unterschiedlicher Zugangsdaten je Zielsystem vergleichsweise gering. Im eingangs geschilderten Angreifer-Szenario wären die erbeuteten Zugangsdaten für den Angreifer daher relativ wertlos, da sie nur für das aktuelle System gelten.

Für die Möglichkeit, Applikationen mit Zugangsinformationen zu versorgen, hat sich der Begriff Application-to-Application Password Management (AAPM)

Glossar

AAPM: Application to Application Password Management

CASB: Cloud Access Security Broker

EPM: Endpoint Privilege Management

IAM: Identity and Access Management

PADLM: Privileged Account Discovery and Lifecyle Management

PAG: Privileged Access Governance

PAM: Privileged Access Management (teilweise auch: Privileged Account Management)

PASM: Privileged Account and Session Management

PEDM: Privilege Elevation and Delegation Management (teilweise auch: Controlled PEDM)

PIM: Privileged Identity Management

PSM: Privileged Session Management

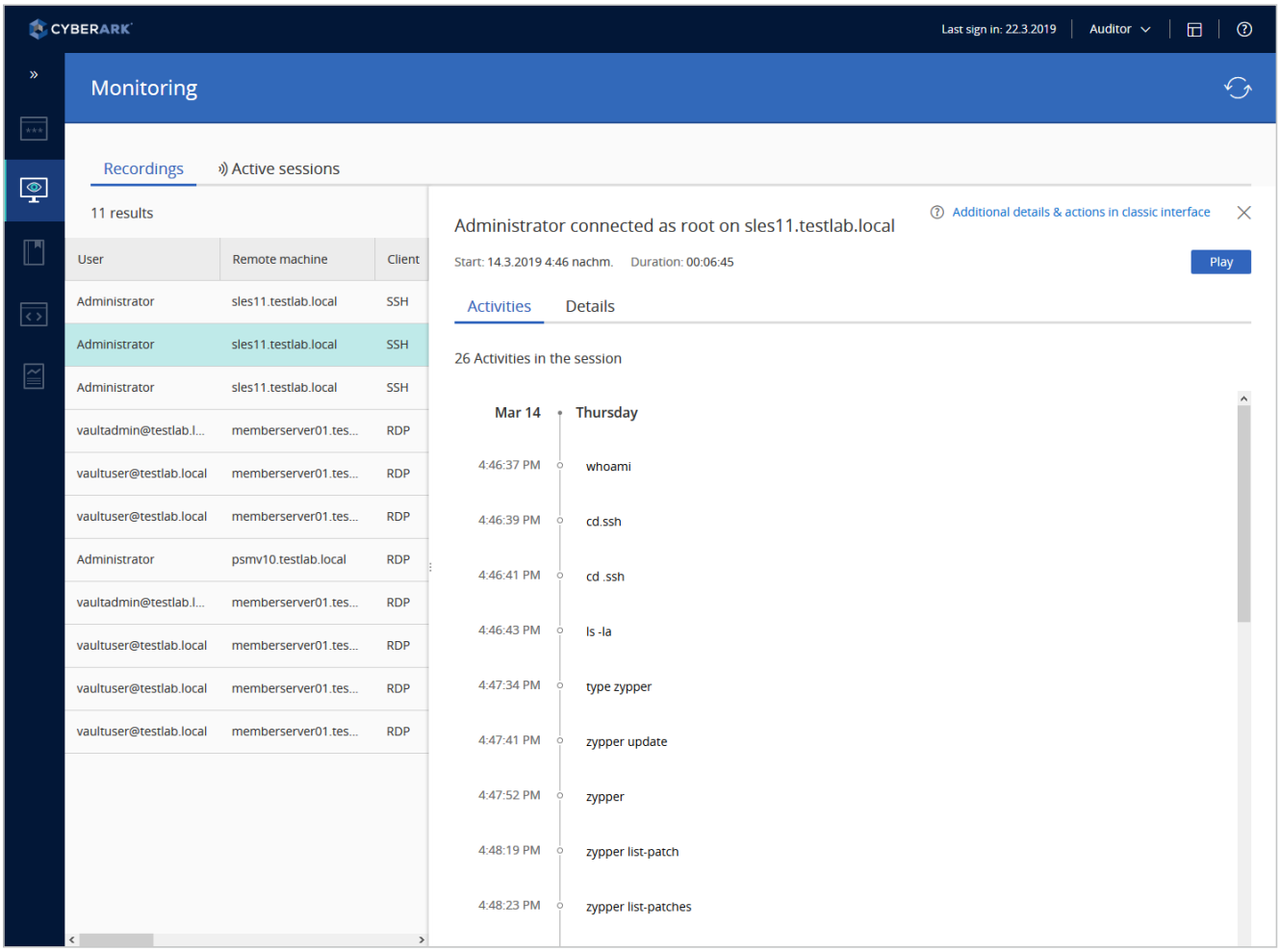
PUBA: Privileged User Behavior Analytics

PUM: Privileged User Management

PxM: Privileged {Account, Access, Identity, Session, User, ...} Management

SAPM: Shared Account Password Management

SRM: Session Recording and Monitoring



Aufgezeichnete Sitzungen lassen sich im Dashboard von CyberArk verfolgen (Abb. 3).

etabliert (siehe Abbildung 2). Die meisten der betrachteten Produkte bieten zu diesem Zweck APIs, SDKs oder mit Applikationsherstellern abgestimmte Integrationen an. Der Zugriff erfolgt bei allen Anbietern über eine REST-API.

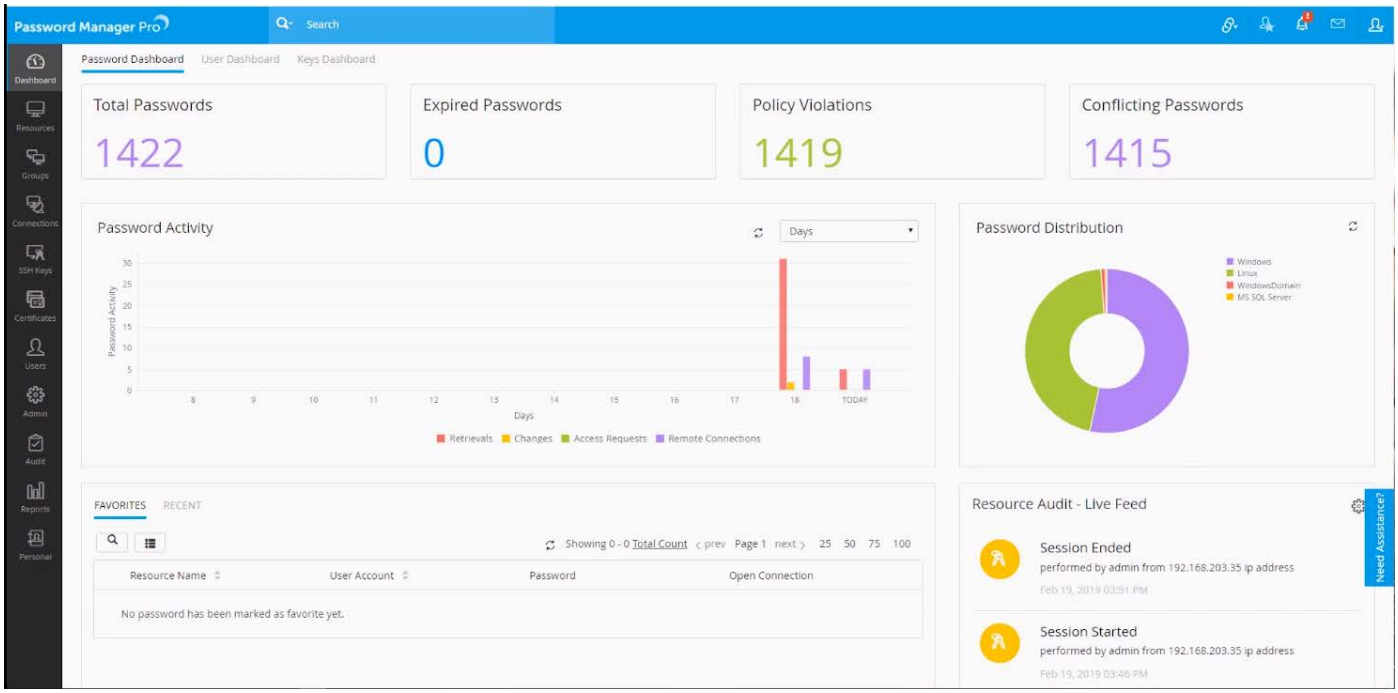
Sag mir, wer du bist

Während sich die Autorisierung für den Zugriff in den jeweiligen Produkten analog zu den regulären Benutzerberechtigungen steuern lässt, ist der Knackpunkt meist die Authentifizierung, also die Sicherstellung der Identität des Anfragenden. Hier kommen Verfahren wie ein vordefinierter API-Schlüssel, Benutzername/Passwort, Client-Zertifikate oder eine Kombination dieser Methoden zum Einsatz. Schlussendlich garantiert jedoch auch eine Kombination der Verfahren nicht, dass die Zugangsdaten der Applikation nicht kompromittiert und von Dritten verwendet wurden. Zur Abmilderung solcher Szenarien prüfen einige Hersteller auch den zuvor im System hinterlegten Hostnamen des anfragenden Systems. Trotz all dieser Maßnahmen lässt sich der Zugriff auf Zugangsdaten über den beschriebenen Weg nicht optimal absichern.

Einige Anbieter haben daher noch zusätzliche Möglichkeiten im Portfolio. Das Problem der genauen Identifikation der anfragenden Applikationen versuchen sie mit Agenten (AAPM agents) in den Griff zu bekommen, die auf dem gleichen System wie auch die Applikation installiert sind. Die Applikation fragt nun nicht mehr per REST einen Web-Service an, sondern nutzt das SDK des jeweiligen Herstellers, um den lokalen Agenten abzufragen. Der Agent kann nun seinerseits den aufrufenden Prozess identifizieren und zusätzliche Prüfungen, beispielsweise des Betriebssystemkontos des Aufrufers, des lokalen Pfades oder eines Hashwerts durchführen. Welche Prüfungen das sind, konfiguriert der Admin jeweils zentral. Bei erfolgreicher Prüfung bekommt die Applikation das Passwort, während es das PIM-Tool gleichzeitig im verschlüsselten Cache des Agenten ablegt. Bei erneuter Anfrage führt das Werkzeug die gleichen Prüfungen durch, es liest jedoch das Kennwort nicht erneut aus dem zentralen Speicher aus. Dieses Vorgehen beschleunigt einerseits die Passwortabfrage und entlastet andererseits den zentralen Speicher. Es kann die Verfügbarkeit der Passwörter auch dann gewährleisten, wenn der zentrale Speicher nicht erreichbar ist (Offline-Funktion).

Unabhängig davon, ob eine API oder ein Agent zum Einsatz kommt: Stets muss die Applikation entsprechend angepasst werden, um benötigte Zugangsdaten abzufragen. Lediglich bei einigen Applikationsservern wie Tomcat oder WebSphere kann der Administrator AAPM über eine Bibliothek direkt im Applikationsserver konfigurieren.

Die genannten Verfahren implementieren allesamt einen sogenannten credential pull, bei dem die jeweilige Applikation bei Bedarf die Daten abfragt. Nicht alle Applikationen funktionieren allerdings in dieser Form. Manche Anwendungen speichern ihre Zugangsdaten verschlüsselt oder unverschlüsselt in



Password-bezogene Aktivitäten zeigt der Password Manager Pro als Bestandteil von ManageEngine übersichtlich an (Abb. 4).

Konfigurationsdateien, der Registry oder erhalten diese über Kommandozeilenparameter. In diesen Fällen steht als Alternative ein credential push zur Verfügung: Der Passwortspeicher oder ein Agent aktualisiert bei Passwortänderung auch die entsprechende Konfigurationsdatei.

Anomalie-Erkennung

Die konsequente Verwendung von Passwort- und Sitzungsverwaltung kann helfen, Angriffe auf administrative Passwörter wie beispielsweise Pass-the-Hash zu verhindern oder zumindest zu erschweren, indem die entsprechenden Informationen erst gar nicht auf möglicherweise exponierten Endgeräten gespeichert werden. Nicht immer funktioniert aber die Prävention und manchmal sind es nicht externe Angreifer, die mit Exploits oder Schadsoftware versuchen, ins Unternehmensnetz vorzudringen. Manchmal sind es berechtigte Anwender, die unerwünschte Aktionen durchführen, ob nun absichtlich oder nicht. In diesem Fall benötigt man Methoden, die normale von unerwünschten Aktivitäten unterscheiden und alarmieren oder bereits bestehende Verbindungen abbrechen können.

Für die Analyse und Erkennung ungewöhnlicher Aktivitäten sind meist Security Information and Event Management Systeme (SIEM) zuständig. Das Unterbrechen bestehender und das Verhindern weiterer Verbindungen obliegt jedoch auch beim Einsatz von SIEM-Systemen anderen Komponenten.

Einige der hier betrachteten Lösungen bieten auch Module zur Anomalie-Erkennung (threat analytics) an. Neben der Analyse der vom eigenen System generierten Protokolle klappt dabei auch die automatisierte Reaktion (das Unterbrechen von Verbindungen) erwartungsgemäß gut. Die Erkennung von ungewöhnlichem Verhalten eines Anwenders berücksichtigt bei den betrachteten Produkten stets die Uhrzeiten und Wochentage, zu denen in der Regel Aktivitäten stattfinden. Darüber hinaus bezieht das System teilweise auch die üblicherweise abgesetzten Kommandos, die angesteuerten Zielsysteme und die Quelladressen in die Analyse ein. Um eine echte Anomalie-Erkennung zu ermöglichen, gibt es statt starrer Regelwerke Verfahren, die je Anwender dynamische Regeln erzeugen (profiling). Obwohl die Tools dabei das normale Arbeitsverhalten der Anwender aufzeichnen und bei ungewöhnlichen Abweichungen alarmieren, lässt sich damit keine Leistungskontrolle realisieren, da die gespeicherten Daten weder einsehbar noch exportierbar sind.

Interessant sind weiterführende Funktionen wie die Erkennung von möglichen Umgehungsversuchen der Passwortverwaltung: Im Normalfall muss ein Anwender zunächst das aktuell gültige Passwort abfragen, um sich dann zum Zielsystem zu verbinden. Sollte der Anwender das Passwort im Klartext einsehen können, wäre es denkbar, dass zukünftige Verbindungen unter Umgehung der Passwortverwaltung stattfinden. Die Erkennung derartiger Versuche basiert auf der Idee, alle Systemprotokolle und insbesondere die Login-Protokolle der infrage kommenden Zielsysteme an die Anomalie-Erkennung weiterzuleiten. Geht einem erfolgreichen Login-Ereignis keine Passwortabfrage voraus, so stellt dies offensichtlich eine Anomalie dar. Insbesondere in Umgebungen mit SIEM lässt sich ein solches Feature als eine Art ausgelagerten SIEM-Filter nutzen. Dabei schicken die Zielsysteme Ihre Protokolle wie üblich ans SIEM, das die relevanten Login-Ereignisse an die Anomalie-Erkennung weitergibt. Erkannte Anomalien fließen als sicherheitsrelevante Ereignisse an das SIEM zurück.

In Verbindung mit der Sitzungsaufzeichnung findet meist auch eine automatische Analyse der durchgeführten Aktionen statt. Kommandos oder Programme, die ein Unternehmen als risikoreich betrachtet, kann der Admin vorab auf eine Art Blacklist setzen. Dies kann dazu führen, dass die Sitzung bei Erkennung der unerwünschten Kommandos angehalten oder abgebrochen wird.

Systemabsicherung

Geht es nach den Vorstellungen der Hersteller, werden stets alle privilegierten Konten und Passwörter durch ihre jewei-

lige Lösung abgesichert und verwaltet. Prinzipbedingt befinden sich dann die Kronjuwelen der IT-Systeme an einer Stelle. Besondere Schutzmaßnahmen sind daher zwingend notwendig.

Hochverfügbarkeit, Disaster Recovery, Datenverschlüsselung, rollenbasierte Zugriffskonzepte, die auch Administratoren der jeweiligen Tools vom Vollzugriff ausschließen, sowie revisionssichere Protokollierung aller Aktionen gehören daher bei allen betrachteten Produkten zum Standard.

Die Systemhärtung findet häufig intransparent für den Betreiber durch den Hersteller statt. Insbesondere bei den fertigen Appliances bestehen wenig Einflussmöglichkeiten. Bei den als zu installierende Software angebotenen Produkten gibt es einerseits automatische Härtungsmaßnahmen und andererseits separat dokumentierte Härtungsempfehlungen. Es empfiehlt sich daher, ein Konzept zum sicheren Betrieb zu entwickeln. Einigen Unternehmen reichen die Zusicherungen der Hersteller nicht aus: sie wollen mit regelmäßigen Penetrationstests auch die Passwortverwaltung geprüft wissen.

Viele Implementierungsprojekte legen großen Wert auf Virenschutz und Backups. Die Sicherung eines Produkts, dessen Daten (hier: die Passwörter) sich permanent verändern, erscheint wenig sinnvoll: Im Restore-Fall klappt ein Zugriff auf den Großteil der Infrastruktur aufgrund veralteter Passwörter nicht mehr. Die Verfügbarkeit der gespeicherten Daten stellen bereits die Produkte mithilfe ihrer Redundanzmechanismen sicher.

Klassische AV-Produkte bringen keinen Sicherheitsgewinn beim Einsatz auf den zentralen Datenspeichern, da sie dort ausschließlich verschlüsselte Dateien und Daten vorfinden, die sie nicht scannen können. Nicht selten ist es in der Vergangenheit auch zu Komplikationen gekommen, bei denen legitime Dateien des Betriebssystems fälschlicherweise als Schadsoftware erkannt wurden. Ist in so einem Fall der Datenspeicher für Passwörter nicht mehr ansprechbar, könnte das zum Super-GAU werden.

Drum prüfe, wer sich bindet

Die Kernfunktionen einer auch für große Unternehmen geeigneten Passwortverwaltung mit gesicherter Informationsablage, starker Zugriffskontrolle und automatischer Passwortänderung erfüllen alle Anbieter. Unterschiede gibt es naturgemäß in Details wie den standardmäßig unterstützten Zielsystemen oder Automatisierungsmöglichkeiten beispielsweise bei der Übernahme von Konten und Passwörtern aus anderen Systemen.

Stärkere Abweichungen bestehen im Bereich der Sitzungsverwaltung und hier insbesondere bei der Systemarchitektur sowie den konkreten Aufzeichnungs- und Eingriffsmöglichkeiten der jeweiligen Anbieter.

Auch die Funktionen zur (UI-)Automatisierung sind bei den Anbietern unterschiedlich ausgeprägt. Die meisten von ihnen stellen dazu REST-APIs bereit. Damit lassen sich ihre Tools leicht mit bestehenden Orchestrierungslösungen oder Provisionierungsworkflows verbinden.

Nur bei einzelnen Anbietern vorhanden sind Funktionen zur Anomalie-Erkennung sowie zur Reaktion auf erkannte Abweichungen. Die meisten Hersteller verweisen hier auf ihre jeweiligen Log-Export-Schnittstellen zu einem SIEM-System.

Wer vorhat, ein entsprechendes Produkt einzusetzen, sollte sich zunächst über seine

aktuellen und zukünftig absehbaren Anforderungen klar werden: Welche Betriebssysteme, Netzwerkkomponenten und Anwendungen möchte man einbinden? Welche Compliance-Anforderungen gibt es?

Eine Gegenüberstellung weniger Anbieter mit Gewichtung und Bewertung der angebotenen Funktionen ist ebenso wichtig wie ein anschließender Proof of Concept mit einer nochmals reduzierten Auswahl. Im PoC sollte man im Anschluss ausgewählte Nutzungsszenarien testen.

BeyondTrust

BeyondTrust ist mit seinen PowerBroker-Produkten (PEDM – siehe Glossar) bereits seit vielen Jahren vor allem im Finanzsektor bekannt und wird seit längerem von Analysten hoch bewertet. So konnte PowerBroker bereits sehr früh Unternehmen helfen, einen Least-Privilege-Ansatz auch praktisch umzusetzen. Neben dem bereits vorhandenen Password-Management hat BeyondTrust seit 2012 eEye (Retina, Schwachstellenscanner) im Portfolio.

2018 hat der bis dato in Europa im PIM-Bereich wenig bekannte Hersteller Bomgar (sicherer Fernzugriff) zunächst Lieberman (Enterprise Random Password Manager), danach Avecto (Privilege Guard/Defendpoint, PEDM) und zum Schluss BeyondTrust gekauft. Seit dem Jahreswechsel tritt die gemeinsame Firma unter der Marke BeyondTrust auf und konsolidiert inzwischen Schritt für Schritt die unterschiedlichen Produkte.

Im PEDM-Bereich setzt das Unternehmen unter Linux/Unix weiterhin auf die bekannten PowerBroker-Tools, während unter Windows die ehemals marktführende Avecto-Software zum Einsatz kommt.

CA Technologies

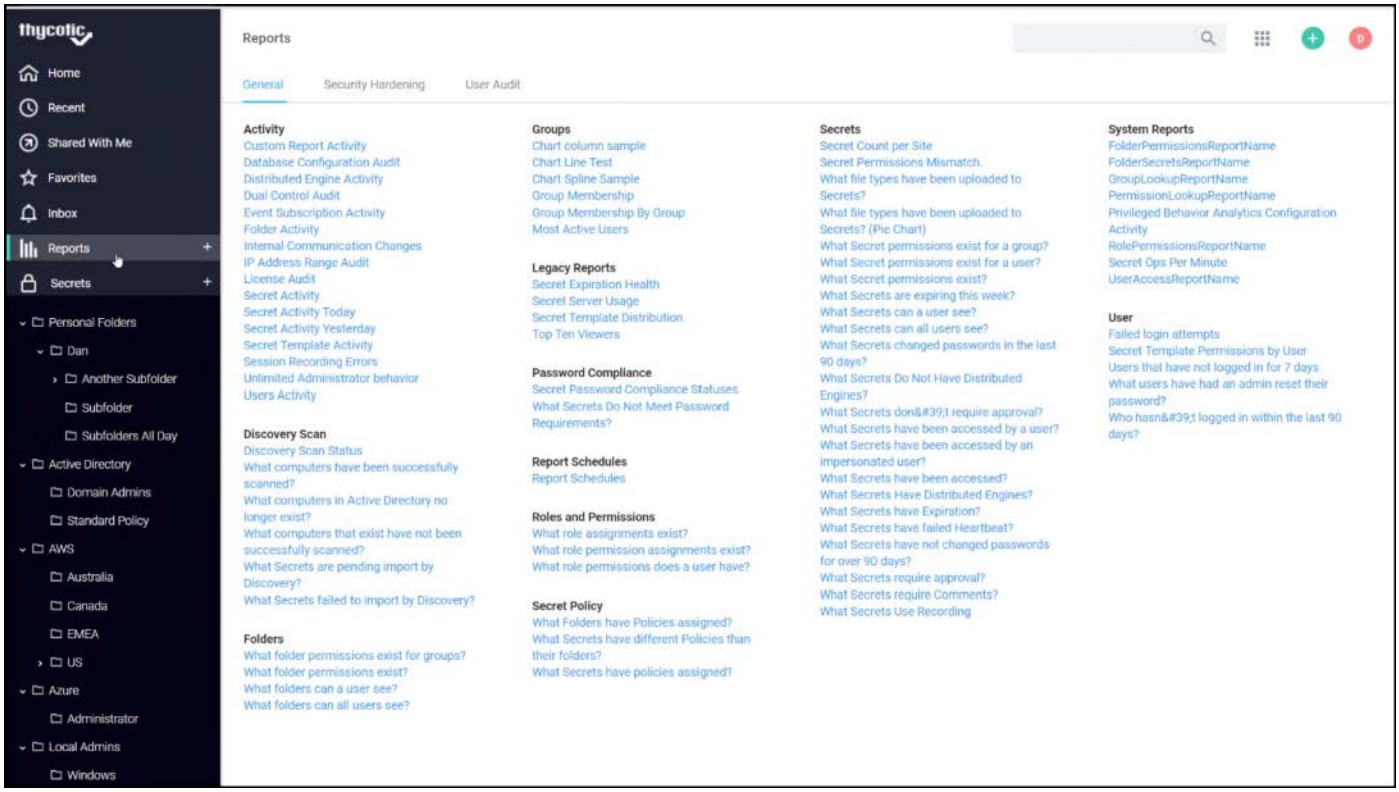
CA Technologies ist eines der weltweit größten Softwareunternehmen und für eine Vielzahl an Produkten bekannt. Mit seinen Kenntnissen aus Produkten im Bereich der Netzwerk- und Computersicherheitssoftware auf unterschiedlichsten Plattformen hat es gute Voraussetzungen für ein Privileged Identity Management-System: Plattformen und technologische Herausforderungen sind wohlbekannt. So überrascht es kaum, dass auch CA Technologies regelmäßig auf den vorderen Rängen bei den Vergleichen der Analysten landet.

CA's Privileged Access Manager bietet eine herausragende Skalierbarkeit, sowohl im Hinblick auf die Menge der gleichzeitig durchführbaren Passwortänderungen als auch in Bezug auf eine Verteilung des Gesamtsystems auf mehrere, geografisch stark verteilte Standorte.

CyberArk

CyberArk sehen viele Analysten als Marktführer an (Abbildung 3). Tatsächlich dringt die Firma sehr früh in neue Segmente des PxM-Marktes vor. Dies geschieht teils durch kontinuierliche Weiterentwicklung des bestehenden Produktes, in jüngerer Vergangenheit jedoch auch durch Zukäufe spezialisierter Anbieter wie Viewfinity (PEDM), Conjur (DevOps-Integration) und Vaultive (CASB).

Innerhalb seiner „Privileged Threat Analytics (PTA)"-Komponente stellt CyberArk als einziger Anbieter auch Möglichkeiten zur Verfügung, Pass-The-Hash- oder Kerberos-Golden-Ticket-Angriffe zu erkennen. Dabei setzt die Software – ähnlich dem Ansatz von Microsofts Advanced Threat Analytics (ATA) – Sensoren im Netzwerk vor oder auf den Domänen-Controllern ein. Durch Integration mit der Passwortverwaltung kann CyberArks PTA somit automatisch auf derartige Attacken reagieren, indem das Tool beispielsweise die Passwörter der betroffenen Konten mehrfach rotiert. Weiterhin lässt sich PTA als eine Art SIEM-Filter nutzen, bei dem ausgewählte Login-Ereignisse vom



Über die Web-Oberfläche bietet Thycotic Zugriff auf eine große Auswahl an Berichten (Abb. 5).

SIEM-System mit Passwort- oder Sitzungsverwaltungsereignissen des eigenen Produkts korreliert werden.

ManageEngine

Ähnlich wie CA Technologies bietet auch ManageEngine diverse Produkte im Bereich IT-Management, IT-Servicemanagement sowie Netzwerk-, Firewall-, Schwachstellen-, Desktop-, Mobilgeräte- und Applikationsmanagement an. Der hier betrachtete Password Manager Pro integriert sich nahtlos in die Suite der vorgenannten Produkte und kann somit auch auf deren Funktionalitäten und Informationen zurückgreifen (siehe Abbildung 4).

Im Hinblick auf die Implementierungstiefe der angebotenen Funktionen steht ManageEngine leicht hinter den Mitbewerbern. Insbesondere bei den Fähigkeiten der Sitzungsverwaltung sind Administratoren auf die angebotene Web-Oberfläche angewiesen und können bestehende eigene Werkzeuge nicht einsetzen.

Die im Vergleich mit den anderen Anbietern bei ManageEngine noch fehlende Anomalie-Erkennung ist nach eigenen Angaben geplant. Zu einem Veröffentlichungstermin wollte sich der Hersteller jedoch noch nicht äußern.

Mateso

Die Mateso GmbH aus Augsburg ist mit seinem Password Safe der einzige deutsche Vertreter in dieser Marktübersicht. Das Produkt ist seit über 18 Jahren verfügbar und wird kontinuierlich weiterentwickelt. Mittlerweile nutzen 19 der Top-30-Dax-Unternehmen und laut Firmenangaben weltweit mehr als 10.000 Unternehmen den Password Safe.

Während der Fokus in früheren Versionen auf der sehr sicheren Passwortablage ohne Passwortänderung und Sitzungsverwaltung sowie auf einem ausgereiften Zugriffskonzept mit diversen Workflows lag, hat der Hersteller in den letzten Jahren immer mehr Funktionen hinzugefügt, die das Produkt vergleichbar mit denen der anderen Anbieter machen.

Im Vergleich zu diesen erscheinen die Bereiche Sitzungsverwaltung, AAPM und die Anomalie-Erkennung von Password Safe noch ausbaufähig.

Micro Focus

Der Privileged Account Manager von Micro Focus basiert auf dem ehemaligen NetIQ Privileged User Manager. Sowohl bei der Passwort- als auch bei der Sitzungsverwaltung leistet er sich keine Schwächen. Die Anomalie-Erkennung analysiert auch Sitzungsaufzeichnungen und kann risikoreiche Aktivitäten erkennen.

Wie auch andere Anbieter bietet Micro Focus PEDM-Funktionen. Diese sind direkt im Privileged Account Manager integriert. Durch die optionale Integration mit dem IAM-Produkt Identity Manager ist die Liste der unterstützten Zielsysteme sehr lang.

One Identity

One Identity Safeguard for Privileged Passwords, Safeguard for Privileged Sessions und Safeguard for Privileged Analytics bilden zusammen die Safeguard Suite. Die Module sind auch einzeln erhältlich. Die Architektur der Sitzungsverwaltung ist im Vergleich mit den Mitbewerbern ungewöhnlich und basiert auf dem Zukauf von Balabit im Jahr 2018. Neben der Sitzungsverwaltung „shell control box“ hat dabei auch syslog-ng den Eigentümer gewechselt. One Identity nutzt das Tool für das zentrale Logmanagement der einzelnen Komponenten.

Neben den Produkten für privilegierte Konten verfügt One Identity über ein komplettes IAM-Portfolio, zu dem auch ein Identity Governance Modul gehört, das auch privilegierte Konten erfasst.

Thycotic

Thycotic bietet mit dem Secret Server ein ausgereiftes Produkt an, das auch als Software-as-a-Service erhältlich ist. Die Oberfläche ist auch für Gelegenheitsanwender einfach und intuitiv zu bedienen (Abbildung 5). Mit dem Zukauf von Arellia im Jahr 2016 hat der Hersteller das Angebot um PEDM-Funktionen erweitert (Privilege Manager).

Die Passwort- und Sitzungsverwaltung verwendet ein sehr granulares Berechtigungskonzept, das flexibel an unterschiedlichste Anforderungen anpassbar ist. Im Bereich der Anomalie-Erkennung fehlen im Vergleich zu den Mitbewerbern Funktionen zur Analyse der in den Sitzungen durchgeführten Tätigkeiten.

Das SaaS-Angebot vonThycotic ist vor allem für Kunden interessant, die sich den Betrieb eigener Infrastruktur sparen wollen. Im Unterschied zu anderen Anbietern, die dafür einzelne AWS- oder Azure-Instanzen starten, betreibt Thycotic das seinen Saas-Dienst selbst als mandantenfähige Lösung.

Wallix

Ausgehend von einer reinen Sitzungsverwaltung mit überdurchschnittlich guter Zielsystem-Unterstützung hat sich Wallix (einer der wenigen europäischen Anbieter in der Übersicht) in den letzten Jahren stark weiterentwickelt und sich in einem bereits gut etablierten Markt für Passwortverwaltungswerkzeuge positioniert.

Wallix hebt die Integration mit den Mitbewerbern CyberArk und Thycotic besonders hervor. Diese stammt noch aus der Zeit, in der die Sitzungsverwaltung bei den Mitbewerbern noch nicht in den Standardlizenzen enthalten war. Einige Kunden entschieden sich daher für die ausschließliche Nutzung deren Passwortverwaltung und konnten bei Bedarf Wallix als Sitzungsverwaltung anschließen.

Die Wallix-Software punktet vor allem mit einer einfachen Installation und geringem Betriebsaufwand. Auch lässt sie sich gut skalieren.

Nicht dabei: IBM, HashiCorp, Centrify

Zum Redaktionsschluss standen die Antworten von Centrify und HashiCorp aus, sodass deren PIM-Produkte nicht berücksichtigt werden konnten. IBM bietet im PxM-Umfeld den „IBM Security Privileged Identity Manager (ISPIM)“ sowie den „IBM Security Secret Server“ an und hat für die vorliegende Marktübersicht Informationen zum letztgenannten Produkt zur Verfügung gestellt. Es betrifft jedoch eine OEM-Version des Thycotic Secret Servers, die keine vom Thycotic-Produkt abweichenden Funktionen anbietet. Daher wurde auf eine gesonderte Darstellung des IBM-Angebotes verzichtet. (akl@ix.de)

Quellen

[1] Research-Berichte und Analysen zu den erwähnten PIM-Tools (meist kostenpflichtig oder gegen Preisgabe einer E-Mail-Adresse): ix.de/z3mx

Marco Lorenz

Marco Lorenz ist Partner und Mitgründer der cirosec GmbH. Seine Schwerpunkte liegen in den Bereichen Malwareschutz und Privileged Identity Management.