Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Bereich Digitale Transformation und IKT-Lenkung DTI

AR012 – Architekturrichtlinie für den Identitätenschutz - Beilage 2

Beilage zur IKT-Vorgabe

Sachtitel (der Beilage):	**Architekturprinzipien PAM**
Ausgabedatum dieser Beilage:[1]	17. August 2023
Gehört zu:	AR012, Version 1.0
Status der Weisung:	Genehmigt

[1] Das *Ausgabedatum* stimmt bei der Erstpublikation einer Beilage mit dem *Beschlussdatum* der genehmigten Version einer Weisung zur Bundesinformatik überein. Bei einer geringfügigen Änderung in der Beilage wird auf eine Anpassung der Version der Weisung verzichtet. Es ist lediglich das *Ausgabedatum* der Beilage anzupassen sowie die Änderung in *Anhang A der Beilage* festzuhalten.

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Gegenstand

Diese Beilage zur Architekturrichtlinie Identitätenschutz regelt die Grundsätze und Gestaltungsprinzipien für Privileged Access Management (PAM) in der IAM-Plattform (siehe IAM-Sollarchitektur) Büroautomation.

1.2 Geltungsbereich

[1] Der Geltungsbereich dieser IKT-Vorgabe ist identisch mit dem Geltungsbereich des Hauptdokuments.

[2] Der Verbindlichkeitsgrad der einzelnen Bestimmungen in dieser IKT-Vorgabe ist gemäss den Schlüsselwörtern in Anhang B des Hauptdokuments festgelegt.

1.3 Begriffe

Nebst den Begriffen im Hauptdokument bedeuten in dieser Beilage:

a. **Break Glass**: Notfallzugriffskonten sind auf Notfall- oder "Glasbruch"-Szenarien beschränkt, in denen normale administrative Konten nicht verwendet werden können.
b. **Credentials Vault**: Der Vault (Tresor) speichert die Credentials (Anmeldeinformationen) und deren Informationen in einem gesicherten Verfahren.
c. **Jump Host**: Ein Jump-Server oder ein Jump Host ist ein System in einem Netzwerk, über welches auf Zielsysteme in verschiedenen Netzzonen zugegriffen werden kann.
d. **JiT-Administration (Just in Time)**: Credentials für privilegierte Konten, die nach dem JIT Prinzip behandelt werden, werden nur für den Zeitraum des Bedarfes erstellt. Danach werden diese Credentials wieder restlos von den Systemen entfernt. So wird eine «Just-In-Time» Bereitstellung gewährleistet.
e. **Lateral Movement**: Von Lateral Movement spricht man, wenn ein Angreifer ein Gerät innerhalb eines Netzwerks und Tiers kompromittiert oder die Kontrolle darüber erlangt und dann von diesem Gerät zu anderen innerhalb desselben Netzwerks und Tiers gelangt. Dies muss verhindert werden.
f. **Service Account**: Ein Service Account (Dienstkonto) ist ein Benutzerkonto, das erstellt wird, um eine bestimmte Software oder einen bestimmten Dienst auszuführen.
g. **Session Recording and Monitoring (SRM)** (Sitzungsaufzeichnung und -überwachung): SRM ist eine Erweiterung der PSM-Tools, um erweiterte Auditing-, Überwachungs- und Überprüfungsmöglichkeiten für privilegierte Aktivitäten während einer privilegierten Sitzung zu bieten. Dies kann z.B. Tastenanschlagsprotokollierung, Videositzungsaufzeichnung, Screen Scraping, OCR-Übersetzung und andere Sitzungsüberwachungstechniken beinhalten.
h. **Privilege Escalation**: Diese Methode beinhaltet die Entwendung von Credentials auf einem System und die Erlangung von Zugriff auf höhergestellten Systemen oder System-Typen, dadurch, dass Credentials auf unterschiedlichen Stufen eingesetzt werden können oder bereits eingesetzt wurden.

2 PAM: Ausgangslage und Ziele

2.1 Ausgangslage

Die Leistungsbezüger (LB) der Bundesverwaltung verlassen sich darauf, dass die IT-Infrastrukturen gemäss den durch den IT-Grundschutz (Si001) vorgegebenen Rahmenbedingungen und den Best Practices der Hersteller betrieben werden.
Die heute eingesetzte Technik, sowie die bestehenden Betriebsverfahren in den IT-Infrastrukturen bei den Leistungserbringern (LE) der Bundesverwaltung müssen mit der aktuellen und zukünftigen Bedrohungslage von Cyber-Angriffen umgehen können.

Besonders die privilegierten Konten einer IT-Landschaft müssen gut vor gängigen Angriffsmethoden, welche sich auf den Credential-Diebstahl fokussieren, geschützt werden.

Die Administration von IT-Systemen und -Services erfolgt bei den fünf Leistungserbringern im Bund auf unterschiedliche Art und Weise. In der Vergangenheit wurden in vielen Bereichen Systeme mit persönlich bekannten privilegierten Credentials, häufig mit Username und Passwort, administriert. Die Einführung von MFA (Multi-Factor Authentication), welche in den meisten Bereichen Anwendung durch die Leistungserbringer findet, hat zu einer gewissen Erhöhung der Sicherheit geführt, jedoch noch nicht vollständig im Bereich der System-Administration resp. der Administration mit privilegierten Credentials. In Teilbereichen sind bei Leistungserbringern bereits PAM-Systeme (Privileged Access Management) im Einsatz, die Passwörter und Accounts sowie deren Verwendung zusätzlich schützen.

Oftmals haben die privilegierten Accounts einzelner Administratoren Berechtigungen auf sehr viele Systeme, was zu einem erhöhten Risiko führt und bei einem Angriff viele Systeme mittels «Lateral Movement» (Seitwärts Ausbreitung) in Mitleidenschaft ziehen kann. Die Systeme werden teilweise direkt von APS Systemen verwaltet. Teilweise sind Jump Hosts im Einsatz, auf denen die Credentials der privilegierten Accounts nicht isoliert und überwacht vom Administrator eingegeben werden. Solche Systeme stellen einen Angriffsvektor für Dritte dar.

Nicht in allen Bereichen der Bundesverwaltung wird das Principle of Least Privilege (PoLP) konsequent eingehalten, sodass die Menge an Berechtigungen von Administratoren höher als notwendig ausfällt und somit ein grundsätzliches Risiko darstellt.

Berechtigungen werden Administratoren in vielen Fällen permanent und persönlich zugewiesen. Somit ist ein Administrator zu Zeiten mit Berechtigungen ausgestattet, an denen diese gar nicht benötigt werden. Hierdurch entsteht ein unnötiges zusätzliches Risiko. Zudem besteht die Gefahr, dass bei einem internen Wechsel bestehende Berechtigungen nicht entfernt werden, und sie sich somit summieren.

Die Verwendung von oder der Zugriff auf privilegierte Credentials oder vergleichbare Secrets (Geheimnisse) kann heute in der Bundesverwaltung nicht lückenlos zurückverfolgt oder aktiv mitverfolgt werden. So besteht die latente Gefahr, dass der Missbrauch durch gestohlene Credentials unentdeckt bleibt. Kommt es zu Sicherheitsvorfällen, bei denen solche Credentials betroffen sind, ist es nicht immer möglich, Geschehnisse umfassend aufzuklären.

Privilegierte Credentials sind zum Teil nicht einer Rolle, sondern einer Person zugeteilt, was die Verwaltung und Kontrolle zusätzlich erschwert.
Service Accounts verfügen oftmals über statische Passwörter, werden oft nicht aktiv verwaltet oder unterliegen keiner Password-Policy. Das wiederum bedeutet, dass solche Accounts besonders gut geschützt werden müssen. Ein regelmässiger Passwortwechsel reduziert Risiken. Nicht in allen Bereichen der Bundesverwaltung ist dieser Prozess automatisiert.

Viele Bereiche der IT der Bundesverwaltung sind dem Risiko von Credential Theft ausgesetzt. Ein gestohlenes Credential kann zu extrem negativen Effekten in der Bundesverwaltung und damit auch zu hohen Kosten oder einem Image-Schaden führen.

2.2 Ziele

Der Einsatz von PAM-Systemen (Privileged Access Management) zur automatisierten Steuerung und Verwaltung der privilegierten Accounts und deren Zugriffe zielt darauf ab, die in der Ausgangslage beschriebenen Sicherheitsherausforderungen der IT in der Bundesverwaltung zu minimieren.

Die flächendeckende Verwendung einer PAM-Unterstützung ermöglicht ein verbessertes Handling und die Nachvollziehbarkeit der Nutzung privilegierter Accounts (z.B. Administratoren-Accounts, Service Accounts, etc.). Unerwünschte Aktionen, welche die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit gefährden können, werden dadurch behindert. Das Risiko einer Kompromittierung durch Credential-Diebstahl oder –Missbrauch wird insgesamt deutlich reduziert.

Im Falle eines Abflusses der Credentials eines Accounts ist bei der Verwendung von lokalen Accounts nur noch ein System betroffen. Sicherheitsvorfälle werden überwacht und ausgewertet. Zusätzlich wird durch die Automatisierung von Passwortwechseln bei privilegierten Accounts dank kurzer Wechselintervalle die Sicherheit erhöht und gerade bei Service Accounts der Aufwand reduziert.
Eine weitere Risikoreduktion kann durch die Verwendung von JiT-Administration (just in time) erzielt werden. Hierbei sind administrative Privilegien nur für einen benötigten Zeitraum verfügbar.

Ausserdem können durch den Einsatz von dedizierten, besonders geschützten Client-Systemen für die direkte Administration (sicherer Arbeitsplatz für Administratoren) Sicherheitsrisiken aufgrund von nicht ausreichend geschützten Administrationsumgebungen verhindert werden.

3 PAM: Architektur-Prinzipien

In diesem Kapitel werden Architektur-Prinzipien einer PAM-Lösung beschrieben.

Diese MÜSSEN bei der Implementierung einer PAM-Lösung und bei deren Nutzung berücksichtigt werden.

Nr.	**1**	Titel	**Verwaltung privilegierter Accounts über PAM Lösung**
Aussage (Prinzip)			Privilegierte Accounts müssen mit einer PAM-Lösung verwaltet werden.
Begründung			Um Credential-Diebstahl und -Missbrauch vorzubeugen, müssen privilegierte Accounts stets über die PAM-Lösung verwaltet werden und sollen dem nutzenden Administrator nicht bekannt gemacht werden.
Auswirkung			Verwendete Accounts müssen in der PAM-Lösung hinterlegt und verwaltet werden. Die separate, von einem Administrator manuell ausgeführte Verwaltung von Accounts ist nicht zulässig. Ausnahme bilden hier «Break Glass Accounts», welche aber nur im Notfall zum Einsatz kommen dürfen. Zur Wiederherstellung von Services müssen die notwendigen «Break Glass» Accounts sicher abgelegt werden. Bei Verwendung der Break Glass Accounts müssen die Credentials im Nachgang zeitnah geändert werden.

Nr.	**2**	Titel	**Nutzung privilegierter Accounts über die PAM-Lösung**
Aussage (Prinzip)			Privilegierte Accounts resp. deren Credentials müssen über die PAM-Lösung (PSM) automatisiert genutzt werden.
Begründung			Hierdurch wird der Abfluss von Credentials erschwert. Ein allfälliger Angriff/Missbrauch kann rasch detektiert und gestoppt werden.
Auswirkung			Die Nutzung von privilegierten Accounts erfolgt grundsätzlich automatisiert. Auf manuelle Prozesse soll verzichtet werden.

Nr.	**3**	Titel	**Privilegierte Credentials sind Administratoren nicht bekannt**
Aussage (Prinzip)			Die Credentials (mindestens das Secret) des über das PAM-Werkzeug genutzten Accounts sollen dem nutzenden Administrator (Mensch) prinzipiell nicht bekannt gegeben werden. Falls dies dennoch notwendig ist, so muss das PAM-Werkzeug nach der Nutzung der Credentials diese zeitnah ändern.
Begründung			Hierdurch wird der Abfluss von Credentials erschwert und ein allfälliger Angriff/Missbrauch kann rasch detektiert werden.
Auswirkung			Die Nutzung von privilegierten Accounts erfolgt grundsätzlich automatisiert. Auf manuelle Prozesse soll verzichtet werden.

Nr.	**4**	Titel	**PAM-Authentisierung nur mit MFA**
Aussage (Prinzip)			Am PAM-Werkzeug muss mittels zugelassener MFA authentisiert werden. Die Nutzung der privilegierten Accounts ist somit nur mittels MFA möglich.
Begründung			Hierdurch wird der Zugriff auf die Komponenten/Werkzeuge der PAM-Lösung gesichert und ein Missbrauch bestmöglich verhindert. Der IKT Grundschutz wird eingehalten.
Auswirkung			Ein zweiter Anmelde-Faktor muss gepflegt werden und stets einsatzbereit sein (Thema Verfügbarkeit). Ohne MFA ist eine geordnete Administration nicht möglich.

Nr.	**5**	Titel	**Einsatz von lokalen privilegierten Accounts**
Aussage (Prinzip)			Auf den Zielsystemen ist mit, durch das PAM-Tool verwalteten, lokalen privilegierten Accounts zu arbeiten.
Begründung			Durch den Verzicht auf Domänen-Accounts oder Verzeichnisdienst-Accounts für lokale privilegierte Rechte wird die Kompromittierung der IKT-Systeme und Komponenten mittels «lateral movement» und «privilege escalation» mitigiert.
Auswirkung			Ein Account gehört prinzipiell zu einem System und hat ein unikales Passwort (Secret). Betriebsprozesse müssen dahingehend angepasst werden, dass eine Verwaltung der Systeme mit lokalen Accounts nur über die PAM-Lösung erfolgen kann.

Nr.	**6**	Titel	**Einsatz unpersönlicher privilegierter Accounts**
Aussage (Prinzip)			Auf den Zielsystemen sind lokale, unpersönliche privilegierte Konten für privilegierte Aufgaben (z.B. System-Administration, OS-Administration, Konfiguration etc.) einzurichten, die durch die Rollenträger sicher und nachvollziehbar über die PAM-Lösung genutzt werden. Ausnahmen können bspw. Microsoft Active Directory Domain Administratoren sein.
Begründung			Gemäss Prinzip 5 sollen mit dem Einsatz von PAM auf den Zielsystemen lokale privilegierte Accounts verwendet werden. Würde man nun hierzu persönliche Accounts verwenden, so stiege die Anzahl der lokalen Accounts auf einem Zielsystem u.U. ins Unermessliche. Zudem wäre eine Administration dieser Accounts auf den Zielsystemen unabhängig von PAM notwendig.
Auswirkung			Administrative Prozesse und Zielsysteme sind dahingehend zu gestalten, dass unpersönliche Accounts verwendet werden können. Die Nachvollziehbarkeit der Nutzung von privilegierten Accounts verlagert sich vom Zielsystem auf die PAM-Lösung. Eine Mutation von Zugriffsberechtigten hat «nur» einen direkten Impact auf eine Rolle sowie das PAM-Werkzeug und nicht

Nr.	**6**	Titel	**Einsatz unpersönlicher privilegierter Accounts**
			aufs Zielsystem.
Bemerkungen			Unpersönliche Accounts lassen sich einfach einer Rolle zuteilen. Diese Rolle wird wiederum in PAM den Zugriffsberechtigten verfügbar gemacht. Eine Mutation von Accounts auf Zielsystemen wird nicht mehr notwendig.

Nr.	**7**	Titel	**100%-Nachvollziehbarkeit der Nutzung privilegierter Accounts**
Aussage (Prinzip)			Die Verwendung von privilegierten Accounts muss jederzeit nachvollziehbar lückenlos aufgezeichnet werden.
Begründung			Im Falle eines Sicherheitsvorfalls ist eine lückenlose Rückverfolgung von privilegierten Account-Verwendungen erforderlich.
Auswirkung			Entsprechende Logging-Mechanismen müssen eingerichtet werden. Das PAM-Werkzeug muss zu den von ihm verwalteten Accounts jederzeit Auskunft darüber geben können, wer welche privilegierten Accounts eingesehen, verändert oder wie genutzt hat.

Nr.	**8**	Titel	**Berechtigungen nach dem Prinzip Least Privilege**
Aussage (Prinzip)			Die Berechtigungen der privilegierten Accounts sollen nach dem Prinzip Least Privilege vergeben werden.
Begründung			Zum einen wird hierdurch verhindert, dass ein Administrator ungewollt Schäden an Systemen herbeiführen kann, die nicht in seinem Verantwortungsbereich liegen und zum anderen wird der Schaden minimiert, falls die Credentials eines Accounts abfliessen.
Auswirkung			Die Berechtigungsvergabe für privilegierte Accounts muss dahingehend gestaltet werden, dass diese dem Prinzip Least Privilege folgt.

Nr.	**9**	Titel	**Einsatz von Verzeichnisdienst-Accounts auf ein System oder wenige Systeme**
Aussage (Prinzip)			Werden privilegierte Accounts aus Verzeichnisdiensten genutzt, so sind diese auf so wenige Systemen/Services wie möglich anzuwenden Die Nutzung ist auf den Anwendungsfall zu begrenzen.
Begründung			Damit bei einem Angriff ein «Lateral Movement» nicht möglich ist, dürfen privilegierte Accounts, welche in einem Verzeichnisdienst gepflegt werden, nur auf ein oder eine eingeschränkte Menge Systeme/Services angewendet werden. Als solche Ausnahmen zählen bspw. Domain Administratoren oder Cluster-Accounts.
Auswirkung			Die Anzahl Accounts pro System und Service steigt.

Nr.	**9**	Titel	**Einsatz von Verzeichnisdienst-Accounts auf ein System oder wenige Systeme**
			Die Anzahl Accounts aus Verzeichnisdiensten, welche direkt auf Systemen berechtigt werden, wird fast gänzlich eliminiert. Eine Applikation hat nebst den Applikations-Rollen zumindest und prinzipiell auch pro System/Service unterschiedliche privilegierte Accounts. Ein Service muss unter Umständen mit mehreren Service Accounts bedient werden.

Nr.	**10**	Titel	**Geringstmögliche Anzahl privilegierter Accounts**
Aussage (Prinzip)			Die Anzahl der privilegierten Accounts ist so klein wie möglich zu halten (aber so viele wie notwendig für Zugriff auf PAM und Zugriff auf Zielsysteme).
Begründung			Hierdurch werden zum einen Betriebsprozesse schlank gehalten und zum anderen besteht eine gute Übersicht der vorhandenen Accounts und Zugriffe.
Auswirkung			Vergabeprozesse von Berechtigungen und Accounts müssen nach diesem Prinzip gestaltet werden. Eine regelmässige Prüfung ist erforderlich.
Bemerkungen			

Nr.	**11**	Titel	**Just-in-Time-Provisionierung von Accounts**
Aussage (Prinzip)			Die Nutzung der privilegierten Accounts soll nach Bedarf erfolgen (Just in Time, JiT). «Just in Time» Provisionierung von Accounts bedeutet, dass Credentials nicht persistent sind, sondern für die benötigte Zugriffsdauer bereitgestellt werden und danach entsorgt werden.
Begründung			Hierdurch wird verhindert, dass ein Account ausserhalb der vorgesehenen Nutzung durch Dritte missbraucht werden kann
Auswirkung			Ein PAM-Werkzeug muss JiT-Provisionierung von Accounts unterstützen.
Bemerkungen			

Nr.	**12**	Titel	**Detektion von Missbrauch oder Unregelmässigkeiten von privilegierten Accounts**
Aussage (Prinzip)			Unregelmässigkeiten oder die Umgehung bzw. der Missbrauch der privilegierten Accounts müssen detektiert werden können.
Begründung			Hierdurch können versuchte oder erfolgreiche Angriffe auf Bundessysteme oder Fehlkonfigurationen erkannt werden. Es besteht die Chance, Schäden abzuwenden und Einfallstore zu schliessen.
Auswirkung			Es müssen Werkzeuge eingesetzt werden, mit denen eine Detektierung möglich ist.

Nr.	**12**	Titel	**Detektion von Missbrauch oder Unregelmässigkeiten von privilegierten Accounts**
			Es müssen entsprechende Betriebsprozesse implementiert werden, damit diese Events nicht still auf den Systemen auf-poppen, sondern entsprechend beachtet und verarbeitet wer-den.

Nr.	**13**	Titel	**PAM berücksichtigt das Schichten-Modell (Tier Model)**
Aussage (Prinzip)			Die PAM-Lösung hält die Prinzipien bezüglich des Schichten-Modells ein (vgl. AR012 Beilage 2: Architektur Tier-Modell MCT [AR012-2])
Begründung			Durch die Einhaltung der Prinzipien können Schäden bei einem Abfluss von Credentials begrenzt und minimiert werden.
Auswirkung			Die Architektur der PAM-Lösung und seiner Komponenten muss das Schichten-Modell unterstützen.

Nr.	**14**	Titel	**Administration der PAM-Lösung über PAM**
Aussage (Prinzip)			Die tägliche Administration der PAM-Systemkomponenten erfolgt ebenfalls mit privilegierten Accounts aus der PAM-Lösung über einen sicheren Administrations-Arbeitsplatz.
Begründung			Hierdurch wird die Integrität der PAM-Umgebung gewährleistet und zusätzliche Einfallstore werden unterbunden.
Auswirkung			Es entsteht u.a. auch hierdurch ein Bedarf an einem sicheren Administrations-Arbeitsplatz. Das Aufsetzen der PAM-Systemkomponenten muss somit, bis die privilegierten Accounts in der PAM-Lösung installiert sind, über dedizierte Systeme oder direkt vor Ort physisch an den PAM-Systemkomponenten erfolgen.

Nr.	**15**	Titel	**Unabhängiges Bereitstellen der PAM-Systemkomponenten**
Aussage (Prinzip)			Zur Bereitstellung der PAM-Systemkomponenten werden keine Remote-Netzwerkverbindungen genutzt, bis die privilegierten Accounts der bereitzustellenden PAM-Systemkomponenten über die PAM-Lösung genutzt werden können. D.h. die PAM-Systemkomponenten werden in einem geschützten und abge-sicherten Rahmen aufgebaut.
Begründung			Hierdurch wird die Integrität der PAM-Umgebung gewährleistet.
Auswirkung			Der Prozess der Inbetriebnahme einer PAM-Lösung muss so gestaltet werden, dass das Prinzip eingehalten werden kann.

Nr.	**16**	Titel	**Angriffsfläche für privilegierte Accounts minimieren**
Aussage (Prinzip)			Die Angriffsfläche der privilegierten Accounts soll insbesondere durch Einsatz von aktuellen Authentisierungsmethoden, Verschlüsselungsparametern, und die Rotation von hinterlegten Credentials etc. minimiert werden.
Begründung			Hierdurch werden Angriffsflächen reduziert, die während einer Authentifizierung entstehen.
Auswirkung			Zielsysteme und Applikationen auf diesen müssen dahingehend konfiguriert werden, dass aktuelle Authentisierungsmethoden und Verschlüsselungen verwendet werden.

Nr.	**17**	Titel	**Bereitstellung der privilegierten Accounts**
Aussage (Prinzip)			Die privilegierten Accounts müssen im Regelfall über einen ordentlichen Prozess in das PAM System einfliessen.
Begründung			Die privilegierten manuellen Tätigkeiten im PAM-System sollen auf ein Minimum beschränkt werden. Der Entstehungsprozess der privilegierten Accounts und der entsprechenden Berechtigungen soll nachvollziehbar von aussen angestossen werden.
Auswirkung			Es sollte einen klaren organisatorischen Prozess mit stets aktuellen Prüfkriterien (z.B. Backgroundchecks) geben, um die Zuweisung eines privilegierten Accounts zu beantragen. In regelmässigen Abständen sollte die Verteilung der privilegierten Zugangsrechte überprüft werden. Die Account-Quellen müssen über eine Schnittstelle angeschlossen werden (z. B. CIS via HPP).

4 Optional: PAM-Architektur

In diesem Kapitel werden die Komponenten und Verbindungen beschrieben, welche bei einer PAM-Lösung zur Anwendung kommen.
Sie sind grafisch dargestellt und im Folgenden textuell beschrieben.

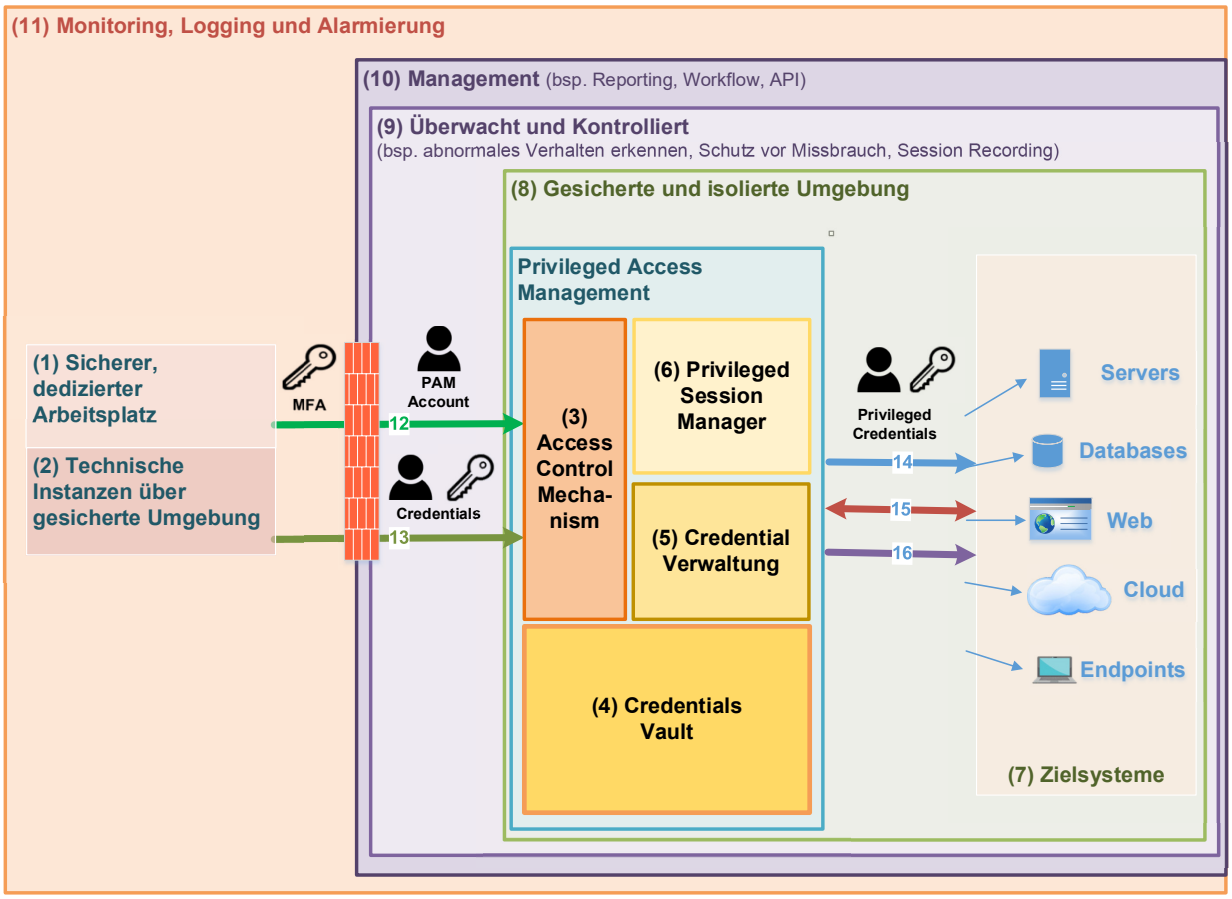

Abbildung 1: Grafische Darstellung eines möglichen Zielbilds (Quelle: eigene Grafik)

Beschreibung der Komponenten:

Nr. 1	**Komponente**	**Sicherer Arbeitsplatz für Administratoren**
Beschreibung		Der sichere Arbeitsplatz für Administratoren erlaubt die sichere Verwaltung der Zielsysteme über ein PAM-Werkzeug.
Funktion		- Vom Standard-Arbeitsplatz getrennter, dedizierter Arbeitsplatz für Administratoren - MFA-Authentisierung für den Zugang zum sicheren Arbeitsplatz
Anforderungen		Dem sicheren Arbeitsplatz liegt eine dedizierte, gehärtete Infrastruktur zugrunde (nicht etwa die gleiche Infrastruktur und deren Managementsysteme wie beim Standardarbeitsplatz). Der sichere Arbeitsplatz verfügt über keine Internetverbindung und über keine Mail-Postfachfunktion, da er ausschliesslich für die sichere Verwaltung der Zielsysteme verwendet werden soll. Der sichere Arbeitsplatz kann über gängige sichere Netzwerktechnologien (z.B. VDI, VPN) auch von ausserhalb des Bundesnetzwerkes erreicht werden. Jegliche administrativen Arbeiten mit privilegierten Rechten an den Zielsystemen dürfen nur über den Weg des sicheren Arbeitsplatzes für Administratoren und das PAM-Werkzeug erfolgen.

Nr. 2	**Komponente**	**«Technische Instanzen»** (5) **über gesicherte Umgebung**
Beschreibung		Technische Instanzen (5) sollen über eine sichere Umgebung analog menschlicher Administratoren Credentials für Zielsysteme aus dem PAM-Werkzeug «just in time» (JiT) nutzen können.
Funktion		- Das PAM-Werkzeug (5) bietet aus einer gesicherten Umgebung, einen gesicherten Zugang zu den Zielsystemen damit die «Technischen Instanzen» die Credentials für Zielsysteme bei der PAM-Lösung erfragen, nutzen und gegebenenfalls verwalten können.
Anforderungen		Damit die «Technischen Instanzen» (5) Credentials für Zielsysteme aus dem PAM-Werkzeug «just in time» (JiT) nutzen können, muss ein sicherer, isolierter Rahmen geschaffen und vom PAM-Werkzeug entsprechend unterstützt werden. Keine Speicherung der Credentials für das Zielsystem sowohl auf der sicheren Umgebung als auch auf der «Technischen Instanz». Die Credentials für das Zielsystem werden nur für eine «just in time»-Nutzung zur Verfügung gestellt.
Bemerkungen		Als Beispiele können die Produkte Tenable Nessus oder BMC Remedy genannt werden. Beide Suiten können sich auf Zielsysteme mit privilegierten Credentials verbinden.

Nr. 3-6	**Komponente**	**PAM-Lösung (Privileged Access Management)**
Beschreibung		Die PAM-Umgebung (hellblaues Kästchen) beinhaltet alle relevanten PAM-Komponenten und -Werkzeuge.

Nr. 3-6	Komponente	PAM-Lösung (Privileged Access Management)
Funktion		Funktionen aller bisher aufgeführten Beschreibungen und Komponenten wie auch (nicht abschliessend): - MFA-Unterstützung - HSM-Integration - Autorisierung für Zugang zu Zielsystemen
Anforderungen		Privilegierte Credentials werden ausschliesslich über die PAM-Lösung benutzt. Die PAM-Umgebung darf maximal über einen sicheren Arbeitsplatz administriert werden. Bestmöglich nur über PAM oder dann direkt physikalisch vor Ort. Die PAM-Umgebung muss an mehreren Standorten hochverfügbar aufgebaut sein Die Nutzung der Credentials muss aufgabenbezogen und zeitlich eingeschränkt werden können. Die PAM-Lösung soll auf physikalischen Systemen betrieben werden können. Die PAM-Lösung muss auditierbar und revisionssicher nachvollziehbar sein.

Nr. 3	Komponente	Access Control Mechanism
Beschreibung		Der ACM überprüft die Authentifizierung und die entsprechenden Rechte des zugreifenden Accounts. Es wird bei einer positiven Prüfung die Authorisierung zur Nutzung der PAM Lösung erteilt.
Funktion		Überprüfung der Credentials von Nutzern und Service-Accounts. Log-Erstellung von Nutzer Zugriffen.
Ausprägung		Der Policy Enforcement Point ist ein Tier 0-System und wird über eine dedizierte Administrationsrolle gesichert und isoliert betrieben.
Anforderungen		Der Policy Enforcement Point ist netzwerktechnisch im Cluster der PAM Lösung aufgehangen und ist von PAM-fremden Systemen getrennt. Die Kommunikation erfolgt auf spezifisch definierten Ports (kleinste mögliche Anzahl). Eine state-of-the-art Kommunikations-Verschlüsselung muss umgesetzt sein.

Nr. 4	Komponente	Credentials Vault
Beschreibung		Der Vault speichert die Credentials und deren Informationen in einem gesicherten Verfahren. Weiter werden Verbindungsinformationen und Nutzungsdaten zu den Credentials ebenfalls sicher gespeichert.
Funktion		- Sichere dedizierte Credentials-Speicherung - Sichere Speicherung der Verbindungsinformationen - Sichere und nachvollziehbare Speicherung der Nutzungsdaten

Nr. 4	Komponente	Credentials Vault
		- Rollen- und/oder benutzerbasiert getrennte Speicherung der Credentials
Ausprägung		Die Vault Systeme sind Tier 0-Systeme und werden über eine dedizierte Administrationsrolle gesichert und isoliert betrieben. Die Vault-Systeme sollen aus Sicherheits- und Verfügbarkeitsüberlegungen physikalische Systeme sein. Bei Einsatz einer Virtualisierung muss die Virtualisierung ebenfalls von den Administratoren des Vaults betrieben werden.
Anforderungen		Die Vault-Systeme sind netzwerktechnisch isoliert und bieten eine absolut minimale Angriffsfläche. Die Kommunikation erfolgt auf spezifisch definierten Ports (kleinste mögliche Anzahl). Eine state-of-the-art Kommunikations-Verschlüsselung muss umgesetzt sein. Die tägliche Administration der Vault-Systeme erfolgt ebenfalls über die PAM-Umgebung.

Nr. 5	Komponente	Credential Verwaltung der Zielsysteme
Beschreibung		Die PAM-Komponente Credential-Verwaltung verwaltet die Credentials der Zielsysteme selbständig und erlaubt auch die Verwaltung der Credentials der Zielsysteme durch einen Administrator. Die Credential-Verwaltung interagiert zwischen Administrator, technischer Instanz, Zielsystem und Credential Vault.
Funktion		- Automatische und manuelle Verwaltung der Credentials der Zielsysteme - Erfassung, Mutation und Löschung der Credentials - Einsehen und Nutzung der Credentials für manuelle Zwecke als Ausnahme - Einsehen/Auditieren der Aktivitäten/Verbindungsinformationen/Logs - Einsehen allfälliger Session Recordings
Anforderungen		MFA-Authentisierung für den Zugang zur Credential-Verwaltung Die Nachvollziehbarkeit jeglicher Veränderung muss auditsicher gewährleistet sein. Pro Tier und für die Cloud werden dedizierte Verwaltungs-Systeme verwendet.

Nr. 6	Komponente	PSM (Privileged Session Management)
Beschreibung		Die PAM Komponente PSM ermöglicht die interaktive Administration via privilegiertem Remote Session Management auf die unterschiedlichsten Zielsysteme. Die hierzu verwendeten Credentials für das Zielsystem werden automatisch vom PAM-Werkzeug gesichert und isoliert verwendet.
Funktion		- Privilegierte Zugriffe werden über isolierte und gesicherte Sessions abgehandelt. - Privilegierte Sessions sind überwacht, kontrolliert und können aufgezeichnet werden.

Nr. 6	Komponente	PSM (Privileged Session Management)
		- Die verwendeten Credentials für die Zielsysteme werden via PAM verwaltet und angewendet.
Anforderungen		Die Sessions müssen eine minimale Angriffsfläche gegen Missbrauch bieten. Nach Ablauf der Session dürfen keine Credentials und/oder Session-Daten von der abgeschlossenen Session auf dem PSM gespeichert werden. Wenn die Session abgebaut ist, verbleiben keine Credential/Session-Daten auf dem PSM. Monitoring und Logging des privilegierten Zugriffes auf ein Zielsystem darf keine Daten über den PSM hinterlassen. Pro Schicht müssen dedizierte PSM-Systeme verwendet werden.

Nr. 7	Komponente	Zielsysteme
Beschreibung		Als Zielsysteme werden alle IKT-Systeme und -Services verstanden. Cloud Services, die mit privilegierten Credentials aus dem Bundesnetz heraus administriert/verwaltet werden, gehören dazu.
Funktion		- Ermöglicht die Anmeldung mit privilegierten Credentials
Anforderungen		Zielsysteme müssen einen sicheren Kommunikationskanal für die sichere Verwaltung der Services wie auch Credentials ermöglichen. Die Administration der Zielsysteme erfolgt nur noch mittels unpersönlichen Accounts (ausgenommen Domain Administration und Vergleichbares wie bspw. z.T. auch die Cluster Administration).

Nr. 8	Komponente	Gesicherte und isolierte Umgebung
Beschreibung		Die Komponenten in diesem Kontext (grünes Kästchen) sind gesichert und isoliert gegenüber den anderen Komponenten/IKT Systemen und Services. Der Vault Server wird zudem dediziert abgeschottet.
Funktion		- Isolierte und gesicherte Verwaltung und Betrieb dieser Systemkomponenten (entsprechend dem Schichtenmodell) (vgl. AR012 Beilage 1 Tier-Modell MCT [AR012-1])
Anforderungen		Die Komponenten in diesem Bereich werden netzwerktechnisch soweit möglich isoliert und bieten dadurch eine absolut minimale Angriffsfläche. Die Administration dieser Komponenten erfolgt ebenfalls in dieser PAM-Umgebung.
Bemerkungen		Im Notfall können Administratoren gegebenenfalls über einen sicheren Arbeitsplatz für Administratoren mit Break Glass Accounts oder physisch mit Notfallkonten vor Ort auf die Systeme zugreifen.

Nr. 9	Komponente	Überwachung und Kontrolle
Beschreibung		Die PAM-Umgebung und deren Komponenten sowie insbesondere die darin verwalteten und genutzten privilegierten Accounts werden perma-

Nr. 9	Komponente	Überwachung und Kontrolle
		nent überwacht und bei Vorkommnissen, die von LE-definierten Standards abweichen, wird sofort alarmiert.
Funktion		- Monitoring der PAM Lösung - Detektion und Alarmierung beim Versuch und bei der missbräuchlichen Nutzung der durch die PAM-Lösung verwalteten privilegierten Accounts. (u.a. Umgehungserkennung) - Detektion von anomalem Verhalten eines privilegierten Benutzers - Detektion von privilegierten Accounts, welche noch nicht in der PAM-Lösung integriert sind.
Anforderungen		Ein Vergleich der Aktivitäten in Echtzeit (Sitzungsanalyse) zu Aktivitäten der Vergangenheit muss bei der Detektion einbezogen/berücksichtigt werden können. Anomales Verhalten eines Benutzers soll erkannt werden. Der Einsatz von «Break Glass» Accounts muss ebenfalls detektiert werden können. Bei der Verwendung eines «Break Glass» Accounts muss eine Auswahl an Sicherheits-geschulten Personen alarmiert werden.
Bemerkungen		Diese Komponente bedient sich auch PAM-externen Komponenten wie bspw. SIEM-Log-Informationen.

Nr. 10	Komponente	Management
Beschreibung		Die PAM-Umgebung verfügt über ein Management der PAM-Lösung.
Funktion		- Sichere PAM-Verwaltung (z.B. Erstellung und Umsetzung von Richtlinien) - Management-Oberfläche - Reporting - Workflows - Monitoring inkl. Alarming - Logging - SIEM Anbindung - Versenden von Mails - API-Schnittstelle, über welche die PAM-Umgebung bspw. automatisiert werden kann - abgesichertes, verschlüsseltes Backup der PAM-Daten und Konfigurationsdaten
Anforderungen		Sichere PAM-Administration. Die Administration der PAM-Komponenten muss ebenfalls über die PAM-Lösung erfolgen können. Die PAM-Lösung muss ständig überwacht werden können, damit missbräuchliche Aktivitäten, Fehlmanipulationen, sonstige Unregelmässigkeiten oder Fehler festgestellt werden können und eine Alarmierung stattfinden kann. Manuelles, automatisches und teilautomatisches Onboarding von neuen privilegierten Accounts. Möglichkeit der Massenmutation über alle Attribute hinweg. Es muss ein Weg bestehen, um im Notfall die PAM-Umgebung wiederherstellen zu können.

Nr. 10	Komponente	Management
		Die Nachvollziehbarkeit (Auditierung) muss garantiert werden.
Bemerkungen		Diese Komponente bedient sich auch PAM-externer Komponenten wie bspw. SIEM-Log-Informationen. Deshalb ist das Kästchen auch ausserhalb PAM eingezeichnet.

Nr. 11	Komponente	Monitoring, Logging und Alarming
Beschreibung		Die PAM-Umgebung ist in die übergeordneten Monitoring-, Logging- und Alarming-Prozesse eingebunden und behält dabei die administrative Eigenständigkeit.
Funktion		- Monitoring inkl. Alarming - Logging (SIEM Anbindung)
Anforderungen		Die PAM-Lösung muss in die bestehenden Monitoring-, Logging- und Alarming-Prozesse integriert werden, damit man feststellen und alarmieren kann, wenn etwas nicht läuft oder Unregelmässigkeiten über alle Systemlandschaften hinweg stattfinden. Die Nachvollziehbarkeit über alle Systemlandschaften hinweg muss garantiert werden.

Nr. 12	Verbindung	Zugang PAM: Administrator
Beschreibung		Ein Administrator eines Zielsystems oder der PAM-Umgebung meldet sich über einen sicheren Arbeitsplatz an der PAM-Umgebung mittels MFA an.
Funktion		- Sichere Authentisierung an den Komponenten der PAM-Umgebung - MFA
Anforderungen		Die Authentisierung am PAM darf nur über MFA erfolgen (ausgenommen «Break Glass» Accounts und Notfallkonten).

Nr. 13	Verbindung	Zugang PAM: «Technische Instanz»
Beschreibung		Eine «Technische Instanz», welche sich mit privilegierten Credentials auf ein Zielsystem verbinden muss, meldet sich über eine sichere Umgebung sicher an der PAM-Umgebung an.
Funktion		- Sichere Authentisierung an der PAM-Umgebung
Anforderungen		- Es müssen Zeitintervalle für Authentifizierungen eingestellt werden. - Es muss eine angemessene Verschlüsselung bei der Übertragung der Authentisierungsdaten genutzt werden.

Nr. 14	Verbindung	Credential-Nutzung
Beschreibung		Die PAM-Umgebung resp. deren Komponenten melden sich mit den Credentials der Zielsysteme automatisch an den Zielsystemen an.
Funktion		Sichere Nutzung der Credentials der Zielsysteme Sicheres Auslesen der Credentials-Informationen
Anforderungen		Die Nutzung der Credentials der Zielsysteme erfolgt prinzipiell über die

Nr. 14	Verbindung	Credential-Nutzung
		PAM-Umgebung resp. deren Komponenten automatisch und abgesichert.

Nr. 15	Verbindung	Credential Cycle
Beschreibung		Die PAM-Umgebung resp. deren Komponenten melden sich an den Zielsystemen an und ändern die Credentials in einem vordefinierten Zyklus.
Funktion		Ändern der Credentials der Zielsysteme auf dem Zielsystem sowie auch in der PAM-Umgebung (Vault)
Anforderungen		Die Änderung der Credentials der Zielsysteme erfolgt prinzipiell über die PAM-Umgebung resp. deren Komponenten automatisch.

Nr. 16	Verbindung	Zugang Zielsystem
Beschreibung		Die PSM-Komponente in der PAM-Umgebung (5) meldet sich für den Administrator (2) mit den entsprechenden Credentials der Zielsysteme automatisch an. Die Session wird vom PSM zum Zielsystem über die PAM-Umgebung gesichert und isoliert neu aufgebaut.
Funktion		- Gesicherte und isolierte Zugriffe/Sessions auf die Zielsysteme - Überwachte und kontrollierte Sessions
Anforderungen		Die Zugriffe auf die Zielsysteme erfolgen gesichert und isoliert: • Die Sessions sind überwacht und kontrolliert. • Die verwendeten Credentials werden via PAM-Umgebung verwaltet und angewendet. • Die Sessions können nicht missbraucht werden (bspw. PtH und PtT nicht möglich). • Wenn die Session abgebaut ist, verbleiben keine Credentials/Session-Daten auf dem PSM. Die Überwachung erfolgt ohne Fussabdruck auf dem Zielsystem. Die Sessions können aufgezeichnet werden.

5 Optional: Privilegierte Accounts / Credentials

Nachfolgende Tabelle gibt einen Überblick darüber, was privilegierte Accounts und Credentials sein können. Diese Tabelle ist nicht abschliessend zu verstehen und soll als Wegweiser dienen.
(vgl. hierzu auch *Referenz AR012 Beilage 1 - Schichten-Modell MCT*) [AR012-1]

Account-Kategorien und –Typen	Systeme/Devices [1]	Accounts/Konten[1]
1) Lokale System Accounts - Local System Accounts auf Systemen /Hardware/Device/Firmware - Operator Accounts - Service Accounts **2) Verzeichnisdienste Accounts** - Verzeichnisdienst-Administratoren - Verzeichnisdienst-Operatoren - Verzeichnisdienst-Service Accounts **3) Applikations-Accounts** - Privilegierte Applikations-Accounts, die auf Systemen/Applikationen laufen **4) Notfall Accounts** - BreakGlass Accounts - Notfall Accounts	- Domain Controller - PAM - IAM (MIM/IDM/...) - Management - Hypervisor - Public Cloud (Systeme, Services) - Applikations-Server (SAP ...) - Netzwerk-Infrastruktur (Firewall, RAS/VPN, SDN, Switches …) - Haustechnik (Domotik) - Backend-Systeme - APS/BA Clients - Drucker ...	- Active Directory Domain Admin - PAM Administrator - Management Administrator - Hypervisor Administrator - Cloud Admin / Cloud: Privilegierte Rollen - Server-Administratoren - Netzwerk-Administratoren - Haustechnik Administrator - Backend System Administrator - APS-Administratoren - Drucker-Administrator ...

[1] Es sind jeweils die Administratoren- und die Operatoren-Konten gemeint

Tabelle 1: Privilegierte Accounts / Credentials

6 Schlussbestimmungen

6.1 Aufhebung bisheriger Vorgaben

1. Keine. Dies ist eine neue Vorgabe.

6.2 Übergangsbestimmungen

1. Diese IKT-Vorgabe muss angewendet werden, wenn ein Leistungserbringer ein PAM Tool einführt und betreibt.

6.3 Einhaltung

1. Die Departemente und die Bundeskanzlei sind gemäss VDTI [VDTI] für die Umsetzung dieser Weisungen in ihrem Zuständigkeitsbereich verantwortlich.

6.4 Überprüfung

1. Die BK(DTI) überprüft die Aktualität und Zweckmässigkeit dieser IKT-Vorgabe spätestens vier Jahre nach der Inkraftsetzung der vorliegenden Version.

6.5 Inkrafttreten

1. Diese Beilage zur IKT-Vorgabe tritt mit der Hauptversion in Kraft.

7 Anhänge

A. Änderungen gegenüber Vorversion

B. Referenzen

ID	Referenz[2]
[ISchV]	Verordnung vom 4. Juli 2007 (Stand am 1. Januar 2018) über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV; SR 510.411)
[SB000]	SB000 – IKT-Strategie des Bundes 2016–2019 vom 4. Dezember 2015
[VDTI]	Verordnung vom 12. Januar 2021 (Stand am 1. April 2018) über die digitale Transformation und die Informatik, VDTI; SR 172.010.58)

C. Abkürzungen

Kürzel	Bedeutung
AAPM	Application-to-Application Password Management
APS	Arbeitsplatzsystem (Client Workstations)
BA	Büro Automatisation
CA	Certificate Authority – Zertifizierungsstelle für digitale Zertifikate
CIS	Central Identity Store (IAM Bund)
CPEDM	Controlled Privilege Escalation and Delegation Management
EPM	Endpoint Privilege Management
HSM	Hardware Security Module
IAM	Identity And Access Management
IDM	Identity Managment
JEA	Just Enough Administration
JIT	Just in Time

[2] Erlasse auf Bundesstufe werden gemäss der «Systematischen Rechtssammlung» referenziert. In Anhang C wird zu einem referenzierten Erlass jeweils auch der zum Zeitpunkt des IKT-Beschlusses der IKT-Vorgabe (vgl. Metadaten) gültige Stand vermerkt. Bei referenzierten IKT-Vorgaben des Bundes wird die zum Zeitpunkt des IKT-Beschlusses gültige Version angegeben.

MFA	Multi-Factor Authentication
MIM	Microsoft Identity Manager
PAM	Privilege Access Management
PAW	Privileged Access Workstation – sicherer Arbeitsplatz für Administration
PKI	Public Key Infrastruktur
PoLP	Principle of least Privilege
PSM	Privilege Session Manager
PtH	Pass the Hash
PtT	Pass the Ticket
RAS	Remote Access Service
SAPM	Shared Account Password Management
SDN	Software Defined Network
SIEM	Security Information and Event Management
SRM	Session Recording and Monitoring
VPN	Virtual Private Network
WinRM	Windows Remote Management

D. Erläuterungen zu PAM?

Die für die sichere Verwaltung des privilegierten Zugriffs verwendeten Lösungen werden als "Privileged Access Management" oder "PAM-Lösungen" bezeichnet. Sie behandeln den Aspekt der "Zugriffsverwaltung", der sich in erster Linie auf die Verwaltung des privilegierten Zugriffs von Benutzern und IT-Administratoren durch individuelle oder gemeinsame Konten und andere Mechanismen zur Delegation und Erweiterung/Erhöhung von Privilegien konzentriert. Die Einführung der PAM-Lösung hilft der Bundesverwaltung dabei, die mit einem privilegierten Zugang verbundenen Risiken nach heutigen «Best Security Practices» bestmöglich zu reduzieren.

Privileged Access Management-Lösungen (PAM) beinhalten in der Regel folgende technologischen Schlüsselfunktionen:

Passwortverwaltung für gemeinsam genutzte Konten (Shared Account Password Management SAPM): Die Passwortverwaltung für gemeinsam genutzte Konten bietet eine Technologie zur sicheren Verwaltung privilegierter Credentials, einschliesslich Systemkonten, Dienstkonten oder Anwendungskonten, die im Allgemeinen gemeinsam genutzt werden. Kernstück der SAPM-Komponente ist ein verschlüsselter und gehärteter Passwort-Tresor (auch Vault genannt) zur Speicherung von Passwörtern, Schlüsseln und anderen privilegierten Credentials (Zugangsdaten) für eine kontrollierte, geprüfte und richtliniengesteuerte Freigabe und Aktualisierung. Die SAPM-Komponente ist daneben für die periodische, planmäßige oder ereignisgesteuerte Randomisierung von Kennwörtern und anderen Credentials verantwortlich und erfüllt damit eine der grundlegendsten Sicherheitsanforderungen.

Verwaltung privilegierter Sitzungen (Privileged Session Management, PSM): Privileged Session Management bietet die Technologie zur Einrichtung einer privilegierten Sitzung zu Zielsystemen einschliesslich grundlegender Auditierung und Überwachung privilegierter Aktivitäten. PSM-Werkzeuge bieten auch Authentifizierung, Autorisierung und Single Sign-On (SSO) für die Zielsysteme.

Application-to-Application Password Management (AAPM): AAPM ist eine Erweiterung der SAPM-Werkzeuge zur Verwaltung von Konten, die von einer Anwendung oder einem System zur Kommunikation mit anderen Anwendungen oder Systemen (wie Datenbanken usw.) verwendet werden. Dazu gehört auch die Verwendung von Dienstkonten, die zur Ausführung bestimmter Funktionen oder zum Auslösen von Prozessen mit den für eine erfolgreiche Ausführung erforderlichen Privilegien verwendet werden. AAPM-Werkzeuge sorgen für die Eliminierung hartkodierter Credentials in Anwendungscode, Skripten und anderen Konfigurationsdateien, indem sie einen Mechanismus (in der Regel APIs) bieten, um Credentials beim Aufruf sicher verfügbar zu machen.

Sitzungsaufzeichnung und -überwachung (Session Recording and Monitoring SRM): SRM ist eine Erweiterung der PSM-Tools, um erweiterte Auditing-, Überwachungs- und Überprüfungsmöglichkeiten für privilegierte Aktivitäten während einer privilegierten Sitzung zu bieten, einschließlich, aber nicht beschränkt auf Tastenanschlagsprotokollierung, Videositzungsaufzeichnung, Screen Scraping, OCR-Übersetzung und andere Sitzungsüberwachungstechniken.

Controlled Privilege Elevation and Delegation Management (CPEDM): Die CPEDM-Komponente ist die Technologie, die sich mit der kontrollierten Erweiterung/Anhebung und richtlinienbasierten Delegation der Privilegien eines Benutzers an Super-User-Privilegien für administrative Zwecke befasst.

Analyse des Verhaltens von privilegierten Benutzern (Privileged User Behavior Analytics PUBA): PUBA verwendet datenanalytische Techniken zur Erkennung von Bedrohungen, die auf anomalem Verhalten gegenüber etablierten Verhaltensprofilen von administrativen Benutzern sowie Benutzergruppen und Administratorrollen basieren.

Privileged Account Discovery and Lifecycle Management (PADLM): PADLM sorgt mit Erkennungsmechanismen für die Identifizierung gemeinsam genutzter Konten, Software-Konten,

Dienstkonten und anderer unverschlüsselter / Klar-Text-Credentials in der gesamten IT-Infrastruktur. PADLM-Tools bieten Workflow-Funktionen zur Identifizierung und Verfolgung der geschäftlichen und technischen Eigentümer des Kontos während seines gesamten Lebenszyklus und können Änderungen in seinem Zustand erkennen, um Benachrichtigungen und notwendige Abhilfemaßnahmen zu veranlassen.

Endpunkt-Privilegienverwaltung (Endpoint Privilege Management EPM): EPM bietet Funktionen zur Verwaltung von Bedrohungen im Zusammenhang mit lokalen Administratorrechten auf Windows, Mac oder anderen Endpunkten. EPM-Tools bieten im Wesentlichen eine kontrollierte und überwachte Eskalation der Benutzerrechte auf Endpunkten und umfassen Funktionen wie z. B. Anwendungs-Whitelisting für den Endpunktschutz. Die EPM-Lösungen sind in die folgenden drei Technologien klassifiziert:

a. Application Control (Anwendungskontrolle)**:** Damit können Organisationen kontrollieren, welche Anwendungen auf einem Endpunkt ausgeführt werden dürfen. Dies wird in der Regel durch Application Whitelisting erreicht, bei dem nur bekannte und zugelassene Anwendungen auf eine vorab genehmigte Liste gesetzt und zum Ausführen zugelassen werden. Die Anwendungskontrolle bietet Unternehmen einen wirksamen Schutz vor Schatten-IT-Herausforderungen.

b. Sandboxing: Bei dieser Technologie wird der Ansatz verwendet, die Ausführung unbekannter Anwendungen oder Programme zu isolieren, indem die Ressourcen, auf die sie zugreifen können (z.B. Dateien, Register usw.), eingeschränkt werden. Diese Technologie, die auch als Anwendungsisolation bezeichnet wird, bietet einen wirksamen Schutz vor Cyberattacken, indem sie die Ausführung von bösartigen Programmen einschränkt und ihre Mittel zur Schadensverursachung begrenzt.

c. Privilege Management (Verwaltung von Privilegien): Diese Technologie umfasst die Verwaltung von Benutzer- und Anwendungsprivilegien. Bei der Verwaltung von Benutzerprivilegien handelt es sich um die kontrollierte und überwachte Erweiterung/Erhöhung der lokalen Administratorrechte. Die Verwaltung von Anwendungsprivilegien befasst sich mit der ausnahme- oder richtlinienbasierten Erweiterung/Erhöhung der Administratorrechte, damit bekannte und genehmigte Anwendungen erfolgreich ausgeführt werden können.

Privileged Access Governance (Verwaltung des privilegierten Zugriffs PAG): PAG befasst sich damit, wertvolle Einblicke in den Zustand des privilegierten Zugangs zu gewähren, der zur Unterstützung des Entscheidungsprozesses erforderlich ist. PAG umfasst Zertifizierungen für privilegierten Zugang und Bestimmungen für anpassbare Berichterstattung und Dashboarding.

Das nachfolgende Bild zeigt die grundlegenden Werkzeuge und Technologien einer PAM-Lösung:

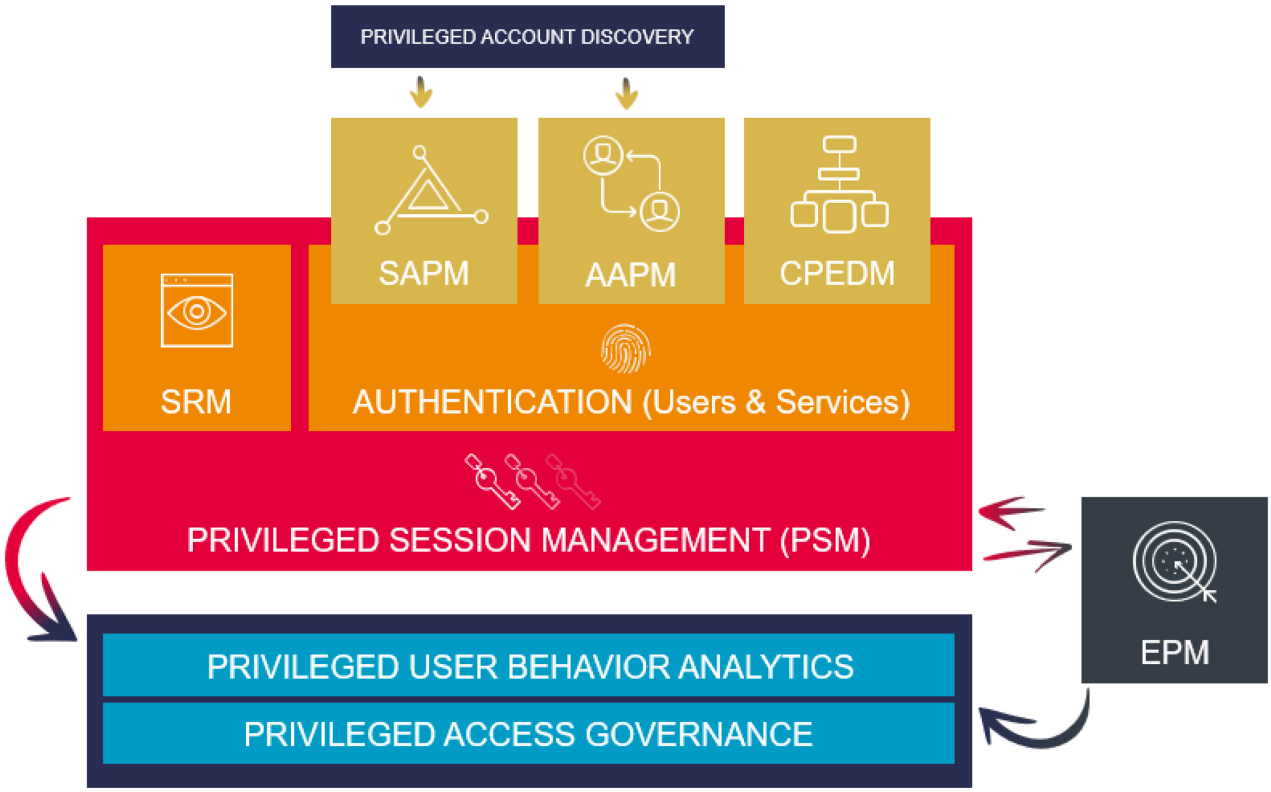

Abbildung 2: Blueprint Architektur PAM-Lösungen (Quelle: Kuppingercole Analysts - www.kuppingercole.com)

SAPM = Shared Account Password Management
SRM = Session Recording and Monitoring
AAPM = Application-to-Application Password Management
CPEDM = Controlled Privilege Escalation and Delegation Management
EPM = Endpoint Privilege Management