CYBERARK®

WHITE PAPER

DAS PROGRAMM FÜR PRIVILEGED-ACCOUNT-SICHERHEIT:

Best Practices für den Weg zum Erfolg

www.cyberark.de

Inhaltsverzeichnis

Beschreibung

Dieses Dokument beinhaltet einen umfassenden Plan zur Bereitstellung der **CyberArk Privileged Account Security** Lösung in Unternehmen, der auf der tiefgreifenden Erfahrung von CyberArk Security Services mit Implementierungen basiert. In diesem fünfphasigen Überblick werden Empfehlungen für die Risikobewertung, Identifizierung kritischer Kontrollen, Planung von Programm und Umfang, schnelle Risikominderung sowie Programmausführung und -bereitstellung besprochen.

Anhand dieser Richtlinien können Unternehmen ein erfolgreiches und letztlich ausgereiftes Programm für Privileged-Account-Sicherheit aufbauen.

Phase 1 – Bestimmung und Initiierung

Die erste Phase des Programms besteht darin, Unternehmens- und Sicherheitsanforderungen zu bestimmen, die Risiken zu analysieren, kritische Kontrollen zu definieren und umfassende Zeitpläne auszuarbeiten. Es ist meist schwierig zu definieren, welche die „Schlüssel zum Allerheiligsten" eines Unternehmens sind. Firmen sagen normalerweise, „wir wollen alles schützen". Durch die Zusammenarbeit mit den Experten von CyberArk Security Services oder den zertifizierten CyberArk Servicepartnern können Unternehmen von den Erfahrungen der Sicherheitsprofis und Technikexperten profitieren, die bei der Abwehr von Bedrohungen an vorderster Front kämpften.

Schritt 1: Treiber und Erfolgskriterien identifizieren

- **Wie lauten die geschäftlichen Treiber für das Projekt?** Zu Anfang sollten Sicherheitsziele in den Bereichen Audit (SOX, PCI usw.), Compliance, Bedrohungen und Best Practices oder auch andere Treiber für das Projekt berücksichtigt werden. Dazu gehören anfängliche Anwendungsfälle, Ziele und Zeitpläne, mithilfe derer die Priorität und Reihenfolge der zu verwaltenden privilegierten Anmeldedaten bestimmt werden können, einschließlich Aufbewahrung, Rotationshäufigkeit der Anmeldeinformation usw. Die Geschäftsleitung sollte an der Definition der Unternehmensziele im Einklang mit dem Sicherheitsprogramm beteiligt sein.

Schritt 2: Kritische und hochwertige Assets definieren

- **Identifizieren Sie die wichtigsten Ressourcen und Systeme, die die sensibelsten Informationen in Ihrem Unternehmen enthalten.** Die Beteiligung der Geschäftsleitung an der Risikobewertung ist sehr wichtig in diesem Schritt, denn hierbei werden wichtige Ressourcen identifiziert. Die Ergebnisse sollten an der allgemeinen Risikomanagementstrategie des Unternehmens ausgerichtet werden.
  - **Welches sind die sensibelsten Informationen?** Sie reichen von persönlich identifizierbaren Informationen, Kreditkartendaten, geistigem Eigentum und ICS-Systemen bis zu ERP-Systemen und Middleware. Es müssen unbedingt die unterstützende Architektur und Infrastruktur von On-Premise- und Cloud-Umgebungen berücksichtigt werden: von Domänencontrollern, Hypervisoren und DevOps-Tools bis zu privilegierten Keys und Anmeldedaten für die Cloud-Infrastruktur.
  - **Bei der Betrachtung dieser Ressourcen und Systeme müssen Sie sich folgende Frage stellen: „Wie denkt und verhält sich ein Angreifer in jeder Situation?"** (siehe Schritt 4). Konzentrieren Sie sich auf einen unternehmensweiten Risikomanagementansatz, indem Sie die Geschäftsprozesse im Zusammenhang mit den wichtigen Ressourcen herausarbeiten und wie ein Angreifer denken. Wo sind die Daten? Wie werden sie gespeichert? Wie werden sie übertragen?
- Tier-0-Ressourcen wie Domänencontroller (DCs) müssen immer als kritisch eingestuft werden und sollten in Phase 1 im Fokus stehen:
  - Tier 0 (Konten von Domänen- und Gesamtsystemadministratoren);
  - **CyberArk Vault-Administratoren;**
  - Wenn die DCs virtuell sind, werden die zugrundeliegenden Hypervisoren/VM-Technologien ebenfalls zu entscheidenden Ressourcen. Nahezu bei allen großen Datendiebstählen versucht der Angreifer, sich Zugriff auf den DC zu verschaffen, um die Kontrolle über das Netzwerk zu erhalten und uneingeschränkten Zugriff auf verschiedene Privileged Accounts und Systeme zu bekommen.
- Tier 1 und Tier 2 sollten in den darauffolgenden Phasen angegangen werden. Es sollte aber bereits ein taktischer Prozess in die Wege geleitet werden, um so schnell wie möglich Grenzen für die Anmeldeinformationen aufzubauen. Ein Beispiel:
  - Tier 1 (Server-Administratorkonten);
  - Tier 2 (Workstation-Administratorkonten).

Schritt 3: Privileged Accounts bestimmen

- **Bei CyberArk Discovery & Audit (CyberArk DNA®)** handelt es sich um eine einfach ausführbare Datei, die Systeme basierend auf Active Directory oder einer Eingabedatei scannt. Nach dem Scan liefert **CyberArk DNA** einen umfassenden Bericht, in dem die Anzahl der gescannten Systeme und der Prozentanteil der Systeme angezeigt werden, die nicht mit Ihrer Passwortrichtlinie konform sind. Diese kann vor dem Scan in **CyberArk DNA** definiert werden. Die Managementzusammenfassung gibt Ihnen einen Überblick über Ihre Umgebung, einschließlich einer Übersicht zu Pass-the-Hash-Anfälligkeiten in Windows-Umgebungen und SSH-Key-Vertrauensbeziehungen in Unix-Umgebungen. Die Details zu den erkannten Konten und Anmeldeinformationen werden in Tabellen bereitgestellt, in denen alle verfügbaren Informationen für jedes Konto enthalten sind

Schritt 4: Zu schützende Privileged Accounts identifizieren und priorisieren

Es gibt verschiedene Ansätze für das Einschätzen von Risiken und das Festlegen von Prioritäten mithilfe der **CyberArk DNA** Berichts- und Übersichtsfunktion. So können Unternehmen direkt sehen, welche Rechner und Konten das höchste Risiko darstellen und welche Rechner den umfassendsten Risiken im Zusammenhang mit lateraler Bewegung ausgesetzt sind. Auf Grundlage dieser Pass-the-Hash-Übersicht können Unternehmen die Sicherheit und Verwaltung von Privileged Accounts auf den risikobehaftetsten Systemen priorisieren.

- Der Zugriff auf die **CyberArk Privileged Account Security** Lösung ist entscheidend – für interne und externe Benutzer. Neben den internen Mitarbeitern müssen auch externe Remote-Anbieter (Drittanbieter) berücksichtigt werden, die auf Netzwerk und Anwendungen zugreifen, um Aufgaben und Transaktionen durchzuführen.
  - **Identifizieren Sie die Konten schnell.** Spüren Sie die Administratorkonten in Windows
    - Für eine Fast-Track-Initiative auf. Die Idee dahinter ist, nicht zu viel Zeit mit Analysen im Voraus zu verbringen, da die Konten innerhalb von Active Directory (AD) und lokalen Administratorgruppen relativ leicht zu finden sind.
  - **Gewähren Sie den risikobehafteten Konten die höchste Priorität.** Implementieren Sie die Kontrollen zuerst auf den leistungsstärksten Konten, indem Sie die Kritikalität der Systeme/Daten und die Risiken bewerten, sollten diese kompromittiert oder gestohlen werden. Unternehmen, die eine vollständige Risikobewertung durchgeführt haben, wissen in der Regel, welche Systeme die sensibelsten Daten und geschäftskritischsten Anwendungen enthalten. Je kritischer das System, desto höher ist das Risiko und desto dringender ist der Bedarf an einem streng kontrollierten Zugriff. **CyberArk DNA** kann alle Konten auf diesen Systemen finden. So sind die Sicherheitsteams in der Lage, zuerst alle unnötigen Konten zu entfernen und anschließend die verbleibenden Konten in der ersten Phase eines Projekts für Privileged-Account-Sicherheit zu priorisieren, z. B.:
    - Domänenadministrator- und Administratorkonten mit Zugriff auf eine große Anzahl von Maschinen, insbesondere Server, sowie Anwendungskonten, die Domänenadministratorberechtigungen nutzen.
  - **Seien Sie realistisch bei der Menge an Konten, die Sie angehen möchten.** Arbeiten Sie schnell, um Kontrollen einzurichten, und nehmen Sie Verbesserungen im Laufe der Zeit vor, z. B.:
    - Idealerweise sollten Konten für Workstation-Benutzer keine Administratorberechtigungen haben. Betroffene von Datendiebstählen sagen jedoch, dass dies aufgrund der schieren Menge an Workstations schwer umzusetzen und aufrechtzuerhalten ist.

Zusätzlich zur Priorisierung der Ergebnisse anhand der Unternehmensanforderungen und wichtigen Ressourcen können Unternehmen das **Hygieneprogramm von CyberArk Privileged Account Security** nutzen, um den Umfang der potenziellen Risiken im Zusammenhang mit den bekanntesten Arten von Angriffen auf Privileged Accounts zu berücksichtigen. Während die Privileged-Account-Sicherheitsposition jedes Unternehmens einzigartig ist, werden beim **Cyber Hygiene Program von CyberArk** die umfassenden Erfahrungen genutzt, die bei der Reaktion auf erhebliche Datendiebstähle gewonnen wurden, um das höchste Schutzniveau aufzubauen.

> Weitere Informationen finden Sie im Whitepaper zum Cyber *Hygiene Program von CyberArk für Privileged Account Security.*

- **Eliminieren Sie irreversible Netzwerkübernahmeangriffe,** damit sich Angreifer nicht im Unternehmen festsetzen können, beispielswiese durch einen Angriff per Golden Ticket von Kerberos:
  - Alle Domänencontroller und Privileged Accounts von Tier-0- und Tier-1-Assets werden vom **CyberArk Privileged Session Manager** isoliert und überwacht.
  - Für jeglichen Zugriff auf die **CyberArk Privileged Account Security** Lösung ist eine Multifaktor-Authentifizierung (MFA) erforderlich.

  - Laufende Kerberos-Angriffe auf Domänencontroller und Tier-0-Assets werden mithilfe von **CyberArk Privileged Threat Analytics** identifiziert und blockiert.
  - Die Erstellung von „Hintertür"-Konten auf Tier-0-Assets wird vom **CyberArk Endpoint Privilege Manager** blockiert.
- **Kontrollieren und sichern Sie bekannte Infrastrukturkonten,** um zu verhindern, dass Angreifer durch eine einzige eingebaute „Hintertür" und dieselben Passwörter auf ähnlichen Ressourcen den gesamten Technologiebestand in Besitz nehmen:
  - Achten Sie auf das Alter von Passwörtern. Je älter das Passwort ist, umso größer ist das Risiko, dass mehrere Benutzer innerhalb und außerhalb des Unternehmens Zugriff darauf haben. Alte Passwörter können auch auf inaktive Konten hinweisen, die nicht deaktiviert wurden.
  - Sichern Sie alle integrierten Hintertür-Konten mit einem Vault durch **CyberArk Enterprise Password Vault**.
  - Lassen Sie Passwörter automatisch rotieren – regelmäßig und nach jeder Verwendung.
- **Schränken Sie laterale Bewegungen ein,** um zu verhindern, dass Angreifer einen Endpunkt infiltrieren, Anmeldeinformationen stehlen und sich lateral zur IT-Windows-Workstation bewegen, um sich erweiterte Berechtigungen anzueignen:
  - Richten Sie Windows-Workstations mit CyberArk Endpoint Privilege Manager ein, um lokale Administratorrechte zu entfernen und den Diebstahl von Anmeldedaten zu stoppen. Beginnen Sie mit der IT-Windows-Workstation und fahren Sie dann mit allen Benutzer-Workstations fort.
- **Schützen Sie die Privileged Accounts in Drittanbieteranwendungen,** um zu verhindern, dass Angreifer Drittanbieterlösungen kompromittieren, die z. B. für Deep Scans verwendet werden, und die von ihnen verwendeten privilegierten Anmeldedaten stehlen:
  - Entfernen Sie die fest programmierten Passwörter in Scan-Engines, Bestandsmanagement-Agenten und Anwendungsservern mit **CyberArk Application Identity Manager**.
  - Lassen Sie Passwörter automatisch rotieren – regelmäßig und nach jeder Verwendung.
- **Verwalten Sie die SSH-Keys auf kritischen UNIX-Servern.** Die Risiken im Zusammenhang mit SSH-Keys werden oft unterschätzt. Einzelne private SSH-Keys können für den Zugriff auf mehrere Zielsysteme und -konten genutzt werden. Außerdem können die Zielsysteme zusätzliche SSH-Keys enthalten, die den Zugriff auf sogar noch mehr Systeme ermöglichen. Oft können einige „allgemeine" Key-Paare gefunden werden, die Zugriff auf eine Vielzahl von Zielsystemen bieten und somit Schwachstellen ähnlich Pass-the-Hash in Windows verursachen. So verhindern Sie, dass Angreifer nicht verwaltete SSH-Keys für die Anmeldung mit Root-Zugriff und die Inbesitznahme des UNIX-Technologiestapels verwenden:
  - Schützen Sie SSH-Key-Paare auf UNIX-Produktionsservern mit einem Vault, rotieren Sie sie und sichern Sie sie mithilfe von **CyberArk SSH Key Manager** mit Richtlinien.
- **Verteidigen Sie Cloud- und DevOps-Anmeldeinformationen,** um zu verhindern, dass Angreifer hochgradig privilegierter API-Keys kompromittieren, die in Continuous Integration (CI)/Continuous Deployment (CD) Tools eingebettet sind, und die gesamte Cloud-Umgebung in Besitz nehmen:
  - Schützen Sie Root-Konten, Root-Keys und API-Keys durch **CyberArk Enterprise Password Vault** mit einem Vault.
  - Nutzen Sie **CyberArk Conjur**, um vertrauliche Zugangsdaten zu sichern, die von Maschinenidentitäten und Benutzern in DevOps-Umgebungen (z. B. in CI/CD-Tools eingebettete Anmeldedaten) verwendet werden.
  - Verwenden Sie **CyberArk Application Identity Manager** für On-Premise-Anwendungen.
- **Sichern Sie gemeinsam genutzte IDs für Geschäftsanwender, um zu verhindern,** dass Angreifer Anmeldeinformationen stehlen, die von mehreren Geschäftsanwendern gemeinsam verwendet werden, um sich umfassenden Zugriff auf empfindliche Systeme zu verschaffen:
  - Jeglicher Zugriff auf die CyberArk Lösung erfordert MFA.
  - Alle gemeinsam verwendeten IDs mit **CyberArk Privileged Session Manager** schützen, der zugriffssichere Audit-Aufzeichnungen, obligatorische Überwachung und Aufzeichnung sowie Session-Isolation ermöglicht.

Schritt 5: Wichtige Kontrollen und Zeitpläne festlegen

Sobald die Risiken für die Privileged-Account-Sicherheit bewertet wurden, besteht der nächste Schritt darin, die kritischen Kontrollen und einen Zeitplan zu erstellen. Wie im aktuellen CISO Report von CyberArk beschrieben, nutzen Angreifer häufig Schwachstellen bei Windows-Administrator-Anmeldeinformationen aus, um sich Zugriff auf wichtige Ressourcen zu verschaffen.

Die folgenden empfohlenen Verfahren sollten als Fundament für das Kontroll-Framework in Betracht gezogen werden:

- Die Offenlegung privilegierter Anmeldedaten einschränken;
- Starke Passwörter durchsetzen und in einem verschlüsselten Vault speichern;
- Die Anzahl von Administratorkonten minimieren;
- Die Überwachung auf Diebstahl von Anmeldedaten erhöhen.

Empfohlene kritische Kontrollen müssen identifiziert werden, um die Reihenfolge für die Implementierung festzulegen. Unternehmen können die risikobehafteten Konten umgehend deaktivieren und erfolgreich eine schnelle Risikominderung vornehmen, indem sie das **SPRINT-Framework** für Privileged Accounts nutzen. Dabei handelt es sich um ein kurzes, schnelles Projekt, bei dem die risikobehafteten Konten identifiziert und als erstes deaktiviert werden, z. B. diejenigen mit Zugriff auf Domänencontroller. Sobald das Framework definiert wurde, können Unternehmen einen längerfristigen Plan erstellen – einen Privileged-Account-„Countdown" – um diese Kontrollen in der gesamten Infrastruktur im Rahmen eines laufenden, proaktiven und messbaren Sicherheitsprogramms einzuführen.

Berücksichtigen Sie zu Beginn die folgenden Best-Practice-Kontrollen und definieren Sie den Zeitplan mithilfe des CyberArk Frameworks. Fangen Sie dabei mit den wichtigsten Kontrollen an:

Weitere Informationen finden Sie im aktuellen CISO Report von CyberArk.

- **Konfigurieren Sie Konten neu, um Aufgaben voneinander zu trennen.** Dadurch wird die Möglichkeit für Angreifer, gestohlene Anmeldeinformationen auf verschiedenen Maschinen zu benutzen, eingeschränkt. Versuchen Sie, Modelle für die Zugriffskontrolle zu implementieren, um die Anmeldedaten für diese Konten innerhalb kürzester Zeit, z. B. 30 Tage, voneinander zu trennen, dazu gehören auch:
  - Domänenadministratorkonten (die nur für die Anmeldung bei Domänencontrollern verwendet werden)
  - Server-Administratorkonten (die nur für die Anmeldung bei Servern verwendet werden)
  - Workstation-Administratorkonten (die nur für die Anmeldung bei Workstations verwendet werden)
- **Schränken Sie die Offenlegung privilegierter Anmeldedaten anhand von taktischen Prozessen ein.** Erstellen Sie Grenzen für die Anmeldeinformationen, sodass jedes Tier seine eigenen Anmeldedaten besitzt:
  - Trennen von Identitäten im Vergleich zu Konten: Stellen Sie auf funktionale Konten um, anstatt individuelle zu verwenden.
  - Wiederholen Sie dies auf allen Plattformtypen und befolgen Sie dabei dasselbe Verfahren. Zu den anderen Plattformtypen zählen Datenbanken, Netzwerkgeräte, Sicherheitsgeräte usw.
  - Sobald es flächendeckend ein einheitliches Zugriffskontrollen-Modell für andere Benutzergruppen und Technologien gibt, sollte der Workflow für den persönlichen privilegierten Zugriff und den gemeinsamen Zugriff derselbe sein. Das Identitätszugriffsmanagement für den Endpunkt ist statisch. Bereitstellungs- und Deaktivierungsrisiken sowie Auditanforderungen werden infolge dessen minimiert.
- **Das Administrator-Passwort mit einem Vault sichern.** Durch die Verwendung eines Passwort-Vaults werden automatisch Passwortrichtlinien durchgesetzt und administrative Aktivitäten auf den Diebstahl von Anmeldedaten hin überwacht. Der CyberArk Digital Vault ist manipulationssicher und nutzt eine Verschlüsselung auf militärischem Niveau für die Speicherung von Passwörtern.
- **MFA für den Zugriff auf Anmeldeinformationen im Vault durchsetzen.**
- **Richten Sie eine automatische Randomisierung der Passwörter für Administratorkonten ein.** Dadurch werden sie eindeutig und komplex und die Möglichkeit des Angreifers, mit einem gestohlenen Passwort mehrere Rechner zu kompromittieren, wird eingeschränkt.

  - In den meisten Fällen zählen zu den Quick Wins lokale Administratorkonten auf Servern, Domänenadministratorkonten und Root-Konten. Im Rahmen der Best Pratices sollten diese Konten nicht für reguläre administrative Arbeiten verwendet werden – dies ist jedoch häufig der Fall. Diese Konten werden oftmals übermäßig verwendet und ihre Passwörter sind häufig auf allen Rechnern dieselben und werden fast nie geändert. In der Folge ist das Risiko im Zusammenhang mit diesen Konten meist hoch.
  - Die Integration dieser Konten ist ziemlich unkompliziert, da sie normalerweise keine komplexe sichere Struktur erfordern. Die meisten Unternehmen:
    - Wissen, wo sich die Konten befinden;
    - Wissen, wer sie verwenden „sollte".

- **Gewähren Sie keinen Administratorzugriff auf sensible Ressourcen von vernetzten Workstations.**
- **Minimieren Sie die Nutzung individuell zugewiesener Administratorkonten, um die Anzahl an Konten zu reduzieren.**
- **Ziehen Sie die Workstation-Administratorberechtigungen von Endbenutzern zurück.**
- **Implementieren Sie Erkennungstools, die in Echtzeit nach Anzeichen für laterale Bewegungen oder Rechteausweitung suchen.**
- **Sollte eine Anwendung Domänenadministratorberechtigungen verwenden, z. B. Domänenrechte für mehrere Server, ziehen Sie diese Berechtigungen zurück.**
  - Berücksichtigen Sie empfindliche Konten wie Service-Accounts. Ein bekannter zweiter Schritt bei der Implementierung beinhaltet das Sichern von Windows-Servicekonten und geplanten Aufgaben. **CyberArk DNA** kann einen vollständigen Überblick über diese Konten und ihre „Verwendung" auf den Zielsystemen erstellen. Das Integrieren lokaler Servicekonten ist oft einfach und somit ein weiterer Quick Win bei Ihrem Programm für Privileged-Account-Sicherheit

Phase 2 – Definition und Planung

Die zweite Phase des Programms für Privileged-Account-Sicherheit besteht in der Definition des Projektumfangs. CyberArk empfiehlt für den Anfang einen geringen Umfang. Wenn Sie gleich zu Beginn zu viel umsetzen möchten, kann das den Erfolg des gesamten Projekts gefährden. Der Schlüssel liegt im Aufbau eines wiederholbaren Prozesses mithilfe des Framework für Privileged Accounts. Dabei wird zunächst mit den kritischsten privilegierten Anmeldedaten begonnen und der Prozess dann Schritt für Schritt wiederholt. Durch Ausarbeitung von Anwendungsfällen für jede kritische Kontrolle können Unternehmen die Umsetzung visuell darstellen.

Schritt 1: Unternehmensführungs- und Technologieteams in interne Veränderungen einbeziehen

- Indem von ganz oben der richtige Weg vorgegeben wird, können Firmen sicherstellen, dass sie schnell und erfolgreich neue Sicherheitskontrollen im ganzen Unternehmen einführen können. Diese Methode ist eine der wichtigsten Faktoren für eine schnelle Risikominderung. Unternehmen müssen versuchen, dasselbe Gefühl von Dringlichkeit und Fortschritt zu erzielen, das oftmals bei tatsächlichen Sicherheitsverletzungen aufkommt – ohne den überwältigenden Druck, wirklich eine Schwachstelle beheben zu müssen. Die Richtungsweisung der Führungsebene ist wichtig, um schnell handeln zu können.
- Auch wenn sich die Sicherheitsabteilung um das Projekt kümmert, gehören die betroffenen Systeme dem Unternehmen. Für ein erfolgreiches Projekt ist die Unterstützung auf allen Funktionsebenen erforderlich. Bevor Sie eine **CyberArk Privileged Account Security** Lösung implementieren, müssen auch andere Teams und Technologien in Ihrem Unternehmen berücksichtigt werden, auf die diese neue Lösung Auswirkungen hat. Je früher Sie mit den funktionsübergreifenden Teams sprechen, Unternehmensrichtlinien vereinbaren und die Integration planen, umso wahrscheinlicher ist eine reibungslose und erfolgreiche Implementierung.
- Sobald die Geräte und Konten definiert wurden, müssen Sie sich so früh wie möglich an die Technologieteams wenden, denen diese Geräte gehören. Diese Teams müssen darüber informiert werden, was die **CyberArk Privileged Account Security** Lösung tut und wie sie ihr alltägliches Arbeitsleben verändert. Überlegen Sie während dieser frühzeitigen Gespräche, wie Sie so viele der bestehenden Workflows wie möglich in die Master Policy aufnehmen können. Legen Sie ebenfalls fest, welche Integrationen für die korrekte Funktionsweise dieser Workflows erforderlich sind.
- Bedenken Sie die Unternehmenskultur. Es wird empfohlen, mit jedem Team Workshops durchzuführen, um zu erfahren, wie sie derzeit mit ihrer jeweiligen Technologie interagieren und wie sich dies nach der Implementierung der CyberArk Lösungen verändern kann. Stimmen Sie die Informationen aus den Workshops auf einander ab und überprüfen Sie die Plattform- und Anwendungsanforderungen.

Schritt 2: Umfang, Rollen und Verantwortlichkeiten definieren

- **Festlegung der Produktstruktur.**
  - Unternehmen können die Produktstruktur der **CyberArk Privileged Account Security** Lösungskomponenten auf Grundlage der definierten kritischen Kontrollen und Zeitpläne definieren. Sie müssen dabei die festgelegten Funktionen, die anvisierten Anwendungsfälle sowie die Lizenzanforderungen jedes relevanten Produkts überprüfen und verstehen.
- **Identifizierung der zu integrierenden Unternehmenstechnologien.**
  - CyberArk verfügt über eine begrenzte Liste an Geräten, die betriebsfertig unterstützt werden. „Allgemein verfügbarer Gerätesupport" bedeutet, dass das Gerät von CyberArk und dem jeweiligen Partneranbieter getestet wurde. Die Kontoverwaltung auf diesen Geräten ist gemäß Zertifizierung betriebsfertig eingerichtet. Es ist wichtig, die Versionsnummern zu prüfen, um sicherzugehen, dass die ausgeführte Version unterstützt wird.
  - Listen mit den aktuellen betriebsfertig unterstützten Plattformen finden Sie in den Dokumenten „Privileged Account Security System Requirements" und „CPM Supported Devices".
  - Damit diese Integrationen so nahtlos wie möglich über Bühne gehen, hat CyberArk das **C3 Alliance Programm** ins Leben gerufen. Daran beteiligt sind verschiedene komplementäre Anbieter, die zertifizierte, betriebsfertige Integrationen für teilnehmende Kunden anbieten. Weitere Informationen zu den C3-Partnern von CyberArk und den zertifizierten Integrationen finden Sie hier: http://www.cyberark.com/partners/technology-partners/
  - „Controlled Availability (CA) device support" bedeutet, dass der Gerätesupport für einen spezifischen Kunden mit speziellen Anforderungen entwickelt wurde. Die Kompatibilität außerhalb dieser bestimmten Anforderungen wird möglicherweise nicht gewährleistet. Unternehmen müssen alle Geräte testen, bevor sie die Gerätekonten in die Produktion überführen. Für Geräte, die nicht auf der Liste unterstützter Geräte zu finden sind, kann ein CyberArk Vertreter den Prozess für die Anforderung eines kundenspezifischen Central Policy Manager Plug-ins in die Wege leiten.
  - Für die automatische Verbindung mit anderen Unternehmensplattformen mithilfe von **CyberArk Privileged Session Manager** ist möglicherweise die Erstellung kundenspezifischer Verbindungskomponenten erforderlich (wenn sie nicht betriebsfertig unterstützt werden). Dies kann entweder unternehmensintern oder über einen CyberArk Vertreter erfolgen, der den Prozess für die Anforderung einer kundenspezifischen Verbindungskomponente einleiten kann.
- **Rollen und Verantwortlichkeiten definieren.**
  - Ein kleines Team kann ziemlich schnell Kontrollen für die wichtigsten Privileged Accounts einrichten. In einem Fall konnte ein Team aus nur acht Mitgliedern nach einer Datenschutzverletzung in Zusammenarbeit mit einem Sicherheitsberater die Administratorkonten für 20 Domänen und 6.500 Server in vier Wochen mit einem Vault schützen. Im Vergleich zur Implementierung von Kontrollen in einer gefährlichen Umgebung nach einer Datenschutzverletzung geht die proaktive Arbeit höchstwahrscheinlich relativ reibungslos von statten.
- **Kern-Teammitglieder für die Bereitstellung und Verwaltung der CyberArk Lösung identifizieren.**
  - Wenn die Bereitstellungen der **CyberArk Privileged Account Security** Lösung erweitert werden, muss ein Team um das Produkt herum aufgebaut werden. Dabei ist es wichtig, das Ganze als „Programm" und nicht nur als „Projekt" zu betrachten. Das bedeutet, dass Privileged-Account-Sicherheit als sich kontinuierlich weiterentwickelnde und bestehende Komponente innerhalb eines Unternehmens angesehen werden muss. Um das Programm wirksam zu unterstützen, muss das CyberArk Team im Hinblick auf ein langfristiges Wachstum strukturiert werden. Durch die Erstellung verschiedener Rollen – wie in diesem Dokument beschrieben – können Unternehmen hochgradig spezialisierte Gruppen aufbauen, die für bestimmte Elemente des Programms zuständig sind. Dies ermöglicht ebenfalls einen besseren Fokus sowie weniger Engpässe, die traditionell bei vielen Bereitstellungen auftauchen (z. B. müssen Vault-Administratoren alle Aufgaben erledigen, wodurch die Implementierung verlangsamt wird). Dedizierte interne CyberArk Ressourcen können zu den Champions für Privileged-Account-Sicherheit des Unternehmens ernannt werden und sich um die internen Veränderungen kümmern. Dabei müssen sie auch die Technologieteams mit einbeziehen, die über die Funktionsweise der CyberArk Lösungen und die Änderungen, die diese mit sich bringt, informiert werden müssen.

- **Rolle 1. CyberArk Subject Matter Expert (SME).** Der CyberArk SME bestimmt den Umfang, das Design, die Architektur und die Bereitstellung aller Aspekte und Phasen des Rollouts der **CyberArk Privileged Account Security** Lösung. Wenn es neue Projekte im Unternehmen gibt, kann der SME Vorschläge zur Nutzung von CyberArk machen und die erforderlichen Schritte ausarbeiten. Der SME kann mit den internen Stakeholdern interagieren, wenn sie sich an der Managementinitiative für Privileged-Account-Sicherheit des Unternehmens beteiligen möchten. CyberArk SMEs sind sozusagen interne Berater, die in vielen Situationen eingesetzt werden können, darunter:
  - Anfängliche Projektplanung;
  - Lösungsdesign und –architektur;
  - Sicherheitsprozessdesign und –entwicklung;
  - Kapazitätsplanung;
  - Lösungskonfiguration und –anpassung;
    - Benutzerauthentifizierung und –bereitstellung;
    - Sichere Struktur, Benennungskonventionen und Berechtigungsdesign;
    - Master Policy;
    - Integration in unternehmensweite Technologien.
  - Installation, Upgrade und Migration
  - Integration neuer Plattformen und Geräte
  - Ausweitung der Bereitstellung auf zusätzliche CyberArk Module und Komponenten (z. B. **CyberArk Privileged Session Manager**, CyberArk Application Identity Management usw.)
  - Analysen und Zustandsprüfungen nach der Bereitstellung

CyberArk SMEs können vertrauenswürdige Experten aus dem CyberArk Security Services Team, zertifizierte CyberArk Channel Partner oder zertifizierte CyberArk Inhouse-Ressourcen sein. Dies hängt von der Aktivitätsebene in Ihrem Unternehmen ab. Durch die Zusammenarbeit mit CyberArk SMEs können Unternehmen Kenntnisse und praktische Erfahrung mittels eines integrierten Wissenstransferprozesses sammeln. Die Experten von CyberArk Security Services fördern Programme für Privileged-Account-Sicherheit, indem sie die Expertise für die Identifizierung und Priorisierung der wichtigsten Privileged Accounts bereitstellen. Im Einklang mit den Kunden kümmern sich unsere Technikexperten dann um das Design, die Implementierung und das Projektmanagement des optimalen Programms für Privileged-Account-Schutz. Kurz gesagt hilft CyberArk Security Services Unternehmen dabei, den realen Wert schneller zu maximieren.

- **Rolle 2. CyberArk Vault-Administrator.** Die **CyberArk Vault-Administratoren** (technische Leiter) sind für die Wartung der Anwendungsschicht der **CyberArk Privileged Account Security** Lösung verantwortlich. Bei ihnen handelt es sich normalerweise um Personen, die aus dem Sicherheits- oder Betriebsbereich kommen. Es wird empfohlen, dass sie an der CyberArk Produktschulung teilnehmen und die CyberArk Zertifizierung erlangen, um Anwendungsfälle erstellen und den CyberArk Digital Vault sowie andere Komponenten warten zu können. Zu den Aktivitäten des **CyberArk Vault-Administrators** zählt typischerweise:
  - Sicherstellen der vollständigen Betriebsfähigkeit, des Funktionszustands, der Fehlertoleranz und Leistung der Anwendung;
  - Gewährleisten, dass installierte Komponenten und integrierte Technologien wie CPM und LDAP-S bestimmungsgemäß funktionieren;
  - Verwaltung der Benutzer- und Gruppenbereitstellung;
  - Erstellung von Richtlinien und Berichten gemäß Risiko/Audit/IT-Sicherheit;
  - Ausführung der vom CyberArk SME in der Design-/Architekturphase definierten Projektaufgaben;
  - Ausweitung der Integration von Privileged-Account-Anmeldedaten per Accounts Feed oder Massenupload.

CyberArk Vault-Administratoren leiten das CyberArk Supportteam eines Unternehmens und arbeiten eng mit den CyberArk SMEs zusammen, um alle Aktivitäten im Rahmen der Unternehmensinitiativen oder Integration neuer CyberArk Module zu verstehen und durchzuführen. **CyberArk Vault-Administratoren** können Teilzeit- oder Vollzeitmitarbeiter sein, je nach Umfang der Umgebung. Normalerweise haben die meisten Unternehmen zwei solcher Administratoren, einen primären und einen Vertretungsadministrator.

- **Rolle 3. IT Operations-Team.** Das IT Operations-Team ist für das zugrundeliegende Betriebssystem und die Infrastruktur verantwortlich, die die CyberArk Software unterstützt. Das Team sorgt dafür, dass die Infrastruktur und das BS innerhalb der Spezifikationen arbeiten. Außerdem überwacht es die Dienste, prüft die Systemverfügbarkeit, führt Backup-Verfahren aus und hilft bei der Behebung von Infrastrukturproblemen. Dieses Team ist auch an Upgrades/Migrationen sowie BS-Patching beteiligt, die während der Nutzung der CyberArk Software notwendig sind. Diese Rolle ist normalerweise Teil des bestehenden IT-Betriebs und der IT-Infrastrukturteams in Ihrem Unternehmen und erfordert wahrscheinlich keine spezielle Vollzeitressource.
- **Rolle 4. CyberArk Datenadministrator.** Bei großen Unternehmensumgebungen kümmert sich der CyberArk Datenadministrator um die wiederkehrenden und alltäglichen Aufgaben im Zusammenhang mit der Verwaltung der **CyberArk Privileged Account Security** Lösung. Zu den Aufgaben zählen:
  - Safe-Erstellung;
  - Uploads von Konten/ Passwörtern/ Anmeldeinformationen;
  - Anwendungsdefinition (**CyberArk Application Identity Management**).

Bei dieser Rolle wird nach einem Inbox-/ Outbox-Prinzip gearbeitet: Interne Kunden reichen Anfragen nach Aktivitäten ein (z.B. „Ich brauche einen neuen Safe für die Unix-PCI-Root-Konten“) und das Team kümmert sich darum. Für die Implementierung dieser Rolle wird gewöhnlich gern ein bestehendes Team eingesetzt, z. B. eine Gruppe aus Zugriffskontrollen-Administratoren. Diese Rolle kann je nach Umgebung auch mit dem **CyberArk Vault-Administrator** zusammengelegt werden.

- **Rolle 5. CyberArk Projektmanager.** Jedes erfolgreiche CyberArk Programm beginnt mit einem erfolgreichen Projekt. Um alle Ressourcen (Personal, Systeme, Informationen und Software) für ein CyberArk Projekt zeitnah bereitzustellen, muss ein Projektmanager bestimmt werden, der sich um Folgendes kümmert:
  - **Integrationsmanagement:**
    - Definition der Projektcharter;
    - Definition des Projektmanagementplans;
    - Projektabschluss und Unterstützung bei der Umstellung.
  - **Umfangsmanagement:**
    - Validierung und Verfeinerung des Projektumfangs;
    - Verwaltung von Änderungen am Umfang (Änderungsanfragen)
  - **Zeitmanagement:**
    - Vorbereitung des Projektzeitplans;
    - Koordinierung aller CyberArk, unternehmens- und drittanbieterinternen Abhängigkeiten und Behebung von Konflikten beim Zeitplan;
    - Anpassung und Neubewertung aller Änderungen am Projektzeitplan je nach Bedarf.
  - **Kostenmanagement:**
    - Management und Nachverfolgung der Kosten;
    - Validierung von Beschaffungen je nach Bedarf.
  - **Qualitätsmanagement:**
    - Anpassung und Kontrolle von Projektabhängigkeiten zur Gewährleistung der richtigen Qualität;
    - Definition und Überwachung der Projekt-KPIs und Implementierung aller erforderlichen Maßnahmen zur Gewährleistung hoher Qualität.
  - **Human-Resources-Management:**
    - Planung der Ressourcenzuweisung;
    - Bereitstellung einer Lösung für Änderungen und Anforderungen im Zusammenhang mit der Ressourcenzuweisung

- **Kommunikationsmanagement:**
  - Primärer Ansprechpartner (Projekteigentümer);
  - Bereitstellung des Projektkommunikationsplans;
  - Durchführung von Meetings: beim Auftakt, vor dem Start, wöchentlich und ad hoc;
  - Stetes Sicherstellen, dass alle Parteien hinsichtlich Erwartungen und Fortschritt an denselben Zielen ausgerichtet sind.
- **Risikomanagement:**
  - Erkennung von Risiken im Voraus, bei Bedarf Bereitstellung von Risikominderungsplänen;
  - Regelmäßige Risikoregister-Updates.
- **Stakeholder-Management:**
  - Identifizierung von Projekt-Stakeholdern und zugewiesenen Pflichten;
  - Gewährleistung der Projektakzeptanz durch die Stakeholder und Förderung des gegenseitigen Fortschritts.

- **Interne Stakeholder der CyberArk Lösung identifizieren.** Es ist wichtig, die Anwender und Stakeholder der CyberArk Lösung zu identifizieren. Es wird empfohlen, dass Unternehmen vor einer Implementierung vereinbaren, welche Benutzer welche Rollen einnehmen werden. Sie sollten auch einen Prozess für das Hinzufügen neuer Benutzer zu den jeweiligen Rollen nach dem anfänglichen Rollout in Betracht ziehen.
  - **Rolle 1. Endbenutzer.** Endbenutzer sind die Anwender der **CyberArk Privileged Account Security** Lösung. Diese Personen nutzen CyberArk Lösungen, um mittels im CyberArk Digital Vault gespeicherten Anmeldeinformationen auf Privileged Accounts zuzugreifen.
  - **Rolle 2. Prüfer.** Prüfer sind Benutzer mit der Fähigkeit, Aufzeichnungen und Protokolle einzusehen sowie Berichte anhand dieser Informationen zu erstellen. Prüfer haben umfassendere Berechtigungen als Endbenutzer. Bei großen Implementierungen werden die Prüferrechte normalerweise auf Safe-pro-Safe-Basis vergeben.
  - **Rolle 3. Safe-Eigentümer.** Safe-Eigentümer sind für gewöhnlich die Eigentümer der Technologie, die der Safe schützt. Diese Benutzer sind dafür verantwortlich, zu prüfen, wer Zugriff auf ihren Safe hat, und Zugriffsanfragen auf Zielgeräte anzunehmen.
- **Den Arbeitsumfang mit vertrauenswürdigen Experten bestimmen.** Sobald ein Unternehmen die Produktstruktur sowie die Rollen und Verantwortlichkeiten berücksichtigt hat, müssen im nächsten Schritt die zertifizierten CyberArk Experten und SMEs einbezogen werden, um den Umfang aus der Perspektive von CyberArk Security Services zu definieren. In diesem Schritt werden Erwartungen seitens des Unternehmens und der zertifizierten CyberArk Experten geäußert, die in den Arbeitsumfang involviert sind. Sie fördern die Entwicklung eines optimalen Programms für Privileged-Account-Sicherheit, indem sie ihre Expertise und Erfahrung einbringen, wann immer sie benötigt werden – um die maximale Investitionsrendite durch die CyberArk Lösungen zu gewährleisten. Zur selben Zeit stellen die zertifizierten CyberArk Experten Methoden bereit und helfen beim Aufbau interner Expertise, die für den Schritt in Richtung eines ausgereiften Programms für Privileged-Account-Sicherheit notwendig ist. Ziehen Sie CyberArk Services in den Bereichen Beratung, Implementierung, Integration, Projektmanagement, Erweiterungsmanagement, Red Team, Schulung/Zertifizierung und Kundensupport in Betracht. CyberArk hilft Unternehmen dabei, sich auf die im Projektumfang anvisierten Anmeldeinformationen zu konzentrieren, die verschiedenen Arten von Anmeldeinformationen und groben Mengen zu bestimmen sowie zu verstehen, wie die für die Produktstruktur definierten Anwendungsfälle mit dem Projektumfang erreicht werden können.

Phase 3 – Start und Ausführung

Schritt 1: Projektstart

Sobald Team, Umfang, Projektziele, Produktstruktur, Anwendungsfälle, Zeitplan und Budget vorbereitet wurden, muss ein Kick-off-Meeting abgehalten werden, damit alle Stakeholder informiert und bereit für die Mitarbeit sind. Dadurch werden die Erwartungen aller beteiligten Parteien aufgestellt und die Verantwortlichkeiten für die Förderung des Fortschritts definiert.

Schritt 2: Architekturdesign

Der CyberArk Digital Vault beherbergt die sensibelsten Anmeldeinformationen des Unternehmens, die Zugriff auf die sensibelsten Daten und geschäftskritischsten Systeme gewähren. Die **CyberArk Privileged Account Security** Lösung befindet sich zwischen Ihren privilegierten Benutzern und Ihren hochgradig sensiblen Systemen. Sie ermöglicht es den Benutzern, extrem wichtige Aufgaben sicher auszuführen. Daher sind die Sicherheit der **CyberArk Privileged Account Security** Lösung und die Stabilität der Plattform von wesentlicher Bedeutung.

- **Systemanforderungen und gesicherte Plattformen.** Um die Sicherheit der **CyberArk Privileged Account Security** Lösung zu maximieren, hat CyberArk eine Sicherheitsnorm und Härtungsverfahren für den CyberArk Digital Vault und seine Komponenten entwickelt. Lesen Sie in jedem Fall die folgenden Dokumente vor der Implementierung:
  - *Privileged Account Security System Requirements.* Prüfen Sie die CyberArk Systemanforderungen für den CyberArk Digital Vault Server und den Komponentenserver. Stellen Sie sicher, dass die dedizierten Server entsprechend bereitgestellt werden und bestimmten Sie die Systemkapazität auf Grundlage von Designanforderungen.
  - *CyberArk Digital Vault Server Security Standard.* Dieses Dokument enthält Informationen von CyberArk zum richtigen Sichern des CyberArk Digital Vault Server. Beachten Sie, dass Drittanbieter-Verbindungen vom CyberArk Digital Vault Server zu externer Software die Angriffsfläche des CyberArk Digital Vault Server vergrößern können. Aus diesem Grund bietet CyberArk integrierte Tools an, die sichere Backups und Überwachung ermöglichen und somit Drittanbieter-Software überflüssig machen.
  - *Security Fundamentals for Privileged Account Security.* Die in diesem Dokument beschriebenen Kontrollen werden alle dringend für den Schutz Ihrer CyberArk Bereitstellung und somit Ihrer Privileged Accounts empfohlen.
  - *Hardening Procedures for CyberArk Components.* In diesen Dokumenten wird erklärt, wie die CyberArk Digital Vault Komponenten gehärtet werden, um ihre Angriffsfläche zu verkleinern und somit auch die Angriffsfläche des CyberArk Digital Vault weiter zu reduzieren. Diese Dokumente liegen den Installationsmedien bei. Den Unternehmen wird empfohlen, sich strengstens daran zu halten. Lesen Sie vor der Implementierung diese Dokumente:
    - *Hardening the CyberArk CPM and PVWA Servers;*
    - *Hardening the CyberArk PSM Server.*
- **Business Continuity und hohe Verfügbarkeit.** Um die Zuverlässigkeit des CyberArk Digital Vault und seiner Komponenten sowie die Verfügbarkeit zu maximieren, sich auf unerwartete Ausfälle vorzubereiten und potenzielle Probleme wirksam zu beheben, empfiehlt CyberArk die folgenden Verfahren.
  - **CyberArk Digital Vault Server** müssen widerstandsfähig sein und mindestens einen einzelnen physischen Disaster-Recovery-Vault (DR) besitzen, der an einem anderen Ort gespeichert ist als der primäre Vault. Die Größe des Vaults hängt von den speziellen Aufbewahrungsanforderungen des Unternehmens an die Session-Aufzeichnung ab. Eine einfache Schätzung sind normalerweise 250 kb/min pro aufgezeichneter RDP-Session und 60 kb/min pro aufgezeichneter SSH-Session.
  - **Komponentenserver** (PVWA, CPM, PSM, PSMP) müssen hochgradig widerstandsfähig und auf die Anforderungen des Unternehmens ausgerichtet sein und sie dürfen keine einzelnen Fehlerpunkte enthalten. Hochgradig verwendete Systeme wie PVWA und PSM/PSMP sollten sich hinter Hardware-Loadbalancern befinden. Bei einer Bereitstellung der **CyberArk Privileged Account Security** Lösung im Unternehmen ist ein Lastenausgleich unerlässlich. Ebenso ist eine frühzeitige Zusammenarbeit mit den relevanten Teams innerhalb des Unternehmens wichtig.
  - **Notfallprozessdesign und -verfahren.** . Aufgrund der kritischen Natur des Systems muss ein gut definierter Prozess für den Schutz der Master-Keys und Anmeldeinformationen für die **CyberArk Privileged Account Security** Lösung eingerichtet werden.
  - Überlegungen vor der Bereitstellung des Digital Vault und der Komponentenserver:
    - **Überwachung.** Unternehmen wird dringend empfohlen, die integrierten SNMP- und Syslog-Tools zur Überwachung des Funktionszustands des CyberArk Digital Vault Server sowie aller Aktivitäten auf dem Server zu nutzen.
    - **Fehlerbehebung.** Die *Sicherheitsnorm für den CyberArk Digital Vault* besagt, dass keine Drittanbieter-Software auf dem CyberArk Digital Vault Server installiert werden darf. Um Protokolle für die Fehlerbehebung abzurufen und gleichzeitig diese Norm einzuhalten, wird Ihnen die Verwendung des PrivateArk Client empfohlen, mit dem Sie Protokolle vom CyberArk Digital Vault Server abrufen und dann mithilfe von Notepad ++ auf Ihrem Desktoprechner anzeigen können.
    - **Lastenausgleich.** CyberArk empfiehlt Unternehmen, einen hardwarebasierten Loadbalancer ihrer Wahl zu verwenden. Wenn das Unternehmen keinen vorhandenen Loadbalancer nutzen kann, kann es auch auf den Microsoft Netzwerklastenausgleich (NLB) zurückgreifen, der in jedem Betriebssystem enthalten ist. Für diejenigen, die sich für diese Option entscheiden: Die CyberArk Dokumentation enthält Informationen zur Konfiguration von NLB für CyberArk Lösungen.
    - **Firewall-Datenverkehr.** Unternehmen sollten im Voraus bestimmen, welche Ports offen sein müssen, und sich an die Firewall-Teams wenden, um die erforderlichen Regeln durchzugehen. Aufgrund der Art und Weise, wie CyberArk seinen Digital Vault Server sichert, verläuft die Kommunikation zwischen dem Vault-Server und den Komponentenservern über einen einzigen Port (TCO/1858). Für die CyberArk Komponenten müssen möglicherweise zusätzliche Ports geöffnet sein, je nachdem, wo und wie sie bereitgestellt werden. In der Dokumentation sind Informationen dazu enthalten, welche Ports auf den Komponentenservern geöffnet sein müssen. Wichtige Überlegungen in Bezug auf die Firewall:

- PVWA muss für alle CyberArk Benutzer auf Port 443 verfügbar sein.
- CPM- und PSM/PSMP-Server brauchen klare Firewall-Regeln, da sie mit Ihrem gesamten Bestand kommunizieren.
- Wenn Sie PSM verwenden, muss das RDP-Protokoll (TCP/3389) seitens des Endbenutzers geöffnet sein. Bei der RemoteApp-Funktion der Remote-Desktop-Server (RDS) ist das allerdings nicht erforderlich. RemoteApp nutzt TCP/443 für die Kommunikation mit dem PSM-Server und der Datenverkehr vom PSM-Server zu dem geschützten Gerät nutzt das von diesem Gerät ausgewählte Protokoll.

- **Prüfung von Umgebung und Netzwerk.** Unternehmen müssen die zu berücksichtigenden sicheren Bereiche, DMZs, Rechenzentren und Ressourcen an allen geografischen Standorten identifizieren, einschließlich On-Premise-, Cloud- und Hybrid-Infrastruktur:
  - Standorte der Benutzer identifizieren und bestimmen, wie diese auf die **CyberArk Privileged Account Security** Lösung zugreifen
  - Standorte der zu verwaltenden Geräte und Konten identifizieren;
  - Standorte der CyberArk Server identifizieren;
- **Integrationen in das Unternehmen.** Die **CyberArk Privileged Account Security** Lösung wird höchstwahrscheinlich eine Tier-1-Anwendung innerhalb des Unternehmens und erfordert somit eine umfassende Integration in anderen Unternehmenstools. Die Integration der folgenden Tools in die **CyberArk Privileged Account Security** Lösung wird dringend empfohlen:
  - **MFA** zur Validierung der Benutzeridentitäten vor dem Zugriff auf PVWA. Prüfen Sie die Liste der unterstützen Authentifizierungsoptionen (RADIUS, SAML, RSA usw.) im Dokument *Privileged Account Security System Requirements;*
  - **HSMs** zum sicheren Speichern des CyberArk Digital Vault Server-Key;
  - **SNMP** zur Überwachung des Funktionszustands des CyberArk Digital Vault und seiner Komponenten sowie zur Ausgabe entsprechender Warnungen;
  - **SIEM- oder SYSLOG**-Lösungen zur Überwachung der Aktivität auf dem CyberArk Digital Vault Server, auf den Komponentenservern und innerhalb der **CyberArk Privileged Account Security** Lösung selbst. Warnungen zu Privileged Accounts (von einem SIEM an **CyberArk Privileged Threat Analytics** gesendet oder direkt von einem SIEM generiert) sollten streng überwacht werden, um die Sicherheit der **CyberArk Privileged Account Security** Lösung und Ihrer Privileged Accounts zu gewährleisten;
  - **Ticketing-Systeme** zur Nutzung bestehender Prozesse für kontrollierte Änderungsanfragen auf Zielsystemen;
  - **SMTP** zur Aktivierung von E-Mail-Benachrichtigungen für Berichte und die Integration einer Ereignisbenachrichtigungs-Engine;
  - **NTP** für die Zeitsynchronisierung auf dem Vault und den DR-Vault-Servern;
  - **Digitale Zertifizierungen** zur Sicherung der Kommunikation aller PVWAs.

Sobald Unternehmen bestimmt haben, welche Integrationen bevorzugt werden oder erforderlich sind, müssen umgehend die jeweiligen Technologieteams in den Prozess einbezogen werden. Außerdem muss sichergestellt werden, dass die Firewall-ACLs im Netzwerk die Kommunikation von den CyberArk Servern zulassen, die mithilfe dieser Protokolle mit dem Zielserver des Unternehmens kommunizieren. Je früher das Unternehmen diese Parteien miteinbezieht, umso besser kann die Integration geplant und zeitnah abgeschlossen werden.

Schritt 3: Lösungsdesign

- **Liste mit Zugriffskontrollen für Benutzermanagement entwickeln.** Es wird empfohlen, CyberArk Digital Vault Benutzergruppen basierend auf den Benutzerrollen zu definieren und verwalten.
  - **Vault-Administratoren** sollten native CyberArk Benutzer sein, d. h. sie sollten individuelle Konten besitzen, die direkt innerhalb der **CyberArk Privileged Account Security** Lösung verwaltet werden.
  - **Endbenutzer, Prüfer und Safe-Eigentümer** sollten über ein externes Verzeichnis verwaltet werden (AD, LDAP usw.) Diese Unterteilung ermöglicht ein umfassendes Benutzermanagement über externe Verzeichnisse und bedeutet gleichzeitig zusätzliche Sicherheit für hochgradig privilegierte Benutzer wie Vault-Administratoren. Vault-Administrator-Anmeldeinformationen können im **CyberArk Enterprise Password Vault** gespeichert werden. Auf diese Weise können Unternehmen die Nutzung der Vault-Administratorkonten prüfen und den administrativen Zugriff auf PVWA und PrivateArk Client-Sessions über **CyberArk Privileged Session Manager** sichern.
  - **Transparente Benutzer- und Gruppenzuordnung.** Benutzer und Gruppen aus einem verbundenen Verzeichnisdienst werden zur Gewährung sicheren Zugriffs verwendet. Jede Gruppe wird als „sicheres Mitglied“ mit den entsprechenden Zugriffsrechten konfiguriert. Da die Benutzer zu im Verzeichnis definierten Gruppen hinzugefügt werden, erhalten sie automatisch Zugriff auf die konfigurierten Safes. Auf ähnliche Weise werden Benutzer, die aus den definierten Gruppen entfernt werden, auch automatisch aus dem CyberArk Digital Vault entfernt.

- **Management lokaler Benutzer.** Die **CyberArk Privileged Account Security** Lösung bietet ein umfassendes Management interner Benutzer. Wenn kein Verzeichnisdienst verfügbar ist oder das Unternehmen nicht darauf vertrauen möchte, kann es lokale Benutzer und Gruppen im CyberArk Digital Vault erstellen. Dies kann manuell oder automatisch über eine der vielen APIs erfolgen, die CyberArk anbietet (z. B. REST-API, Kommandozeile usw.). Bei der lokalen Verwaltung von Benutzern kann CyberArk einen lokalen sowie jeden beliebigen externen konfigurierbaren Authentifizierungsdienst unterstützen (LDAP, RADIUS, SAML usw.).

  Beispiel: Ein Endbenutzer kann das funktionale Konto in CyberArk auswählen, das seiner Rolle entspricht. Joe Smith hat dann Zugriff auf Workstation Admin1, ServerAdmin1, und möglicherweise DomainAdmin1. Er wählt das benötigte Konto aus und ist dann durch den PSM-Workflow isoliert. Diese funktionalen Konten, die mit keiner Person verknüpft sind, können öfter geändert werden und werden weniger wahrscheinlich von Social Engineering anvisiert. Einmal-Passwörter und exklusiver Zugang können für diese Konten verwendet werden. Dadurch wird der Gültigkeitszeitraum des Passworts weiter verkürzt und somit auch die Zeitspanne, während der ein Angreifer gestohlene Anmeldeinformationen verwenden kann.

- **Bei der Integration von CyberArk Lösungen in ein externes Verzeichnis muss unbedingt berücksichtigt werden, welche Verzeichnisadministratoren Benutzer zu Benutzergruppen hinzufügen können, die Zugriff auf den CyberArk Digital Vault haben.** Wenn ein nicht autorisierter Benutzer zu einer CyberArk Benutzergruppen hinzugefügt werden würde, könnte er Zugriff auf die in diesem CyberArk Digital Vault gesicherten Privileged Accounts erhalten. Unternehmen sollten mit Verzeichnisadministratoren zusammenarbeiten, um einen vertrauenswürdigen Genehmigungsprozess aufzubauen, bevor ein neuer Benutzer zu einer CyberArk Benutzergruppe hinzugefügt werden kann. Eine SSL-Verbindung vom CyberArk Digital Vault zum Verzeichnis wird dringend empfohlen. Dafür ist dann ein Root-Zertifikat für die CA erforderlich, die das Zertifikat auf dem Verzeichnisserver ausgestellt hat.

- **Safe-Struktur und Benennungskonvention entwickeln.** Safes sind logische Strukturen, mit denen Unternehmen den Zugriff auf sensible Daten (Anmeldeinformationen, Audit-Protokolle, Aufzeichnungen) kontrollieren, die im CyberArk Digital Vault gespeichert sind. Ein schlechtes Safe-Design kann dazu führen, dass entweder zu viele Personen Zugriff auf die sensiblen Daten haben (wodurch das Risiko für schädliche oder versehentliche Fehler steigt) oder zu wenige (was aufgrund der konstanten Anfragen und Genehmigungen zu einer deutlichen Überbelastung des Managements führt).
  - Zwei grundlegende Ansätze für das Safe-Design und die Benennungskonvention lauten 1) nach Plattform (Windows, Unix usw.) oder 2) nach Region (AMER, EMEA usw.). Es gibt nicht den einen idealen Ansatz, aber CyberArk Security Services kann hierzu Hilfestellung anbieten.
  - Weitere Informationen zum Design der Safe-Benennungskonvention finden Sie im Dokument *Safe Naming Convention Creation Procedure*. Safe-Berechtigungen sollten auf Basis von Rollen, LDAP-Gruppen usw. entworfen werden, in die auch technische und geschäftliche Anforderungen integriert werden.

- **Kontrollsets und Master Policy entwerfen.** Sobald die Safe-Struktur entworfen und vereinbart wurde, besteht der nächste Schritt im Design der Master Policy. Die Master Policy sollte normalerweise die IT-Sicherheits- und/oder Passwortrichtlinie eines Unternehmens widerspiegeln. Die Namen der Policy-Einstellungen entsprechen denen einer IT-Sicherheitsrichtlinie, damit die Anforderungen leichter verfasst werden können. Zu den allgemeinen Richtlinien gehört:
  - Passwortalter zwischen 30 und 60 Tagen
  - Auschecken/Einchecken privilegierter Anmeldedaten;
  - Duale Kontrolle beim manuellen Zugriff auf Anmeldeinformationen.

  Beispiel: Erstellen Sie gemeinsame Konten für jede erforderliche Funktion auf Grundlage von logischem stufenweisen Zugriff auf hochwertige Assets. Dadurch wird die Anzahl von Konten in der Domäne eingeschränkt. Dies kann mit eingeschränktem Zugriff auf das Unternehmen erfolgen – durch enge Zusammenarbeit mit dem Domänenadministrator-Team und indem geprüft wird, ob die erforderliche Arbeit auch mit dem neuen Konto mit den geringsten Berechtigungen ausgeführt werden kann. Sobald die Konten überprüft wurden, können die Berechtigungen und Netzwerkregeln dahingehend geändert werden, dass der Zugriff über die alten Konten gesperrt wird.

Um für Konsistenz zu sorgen und die Verwaltung zu vereinfachen, sollten Unternehmen weitere Kontrollsets in Betracht ziehen, z. B. Daten- und Anwendungsklassifizierung sowie Plattformeinstellungen und Plattform-Benennungskonventionen für verwaltete privilegierte Anmeldedaten. Zusammen mit den Eigentümern und Anwendern von Anwendungen und/oder Plattformen können Workshops organisiert werden, bei denen die Anwendungsfälle präsentiert und alle Fragen angesprochen werden, die hinsichtlich Auswirkungen und Veränderungen aufkommen könnten.

- **Workflows für den Zugriff auf höchster Ebene basierend auf Anwendungsfällen zu Kontozugriffen entwerfen.** Zu den Workflows können folgende zählen:
  - **Duale Kontrolle:** Benutzer müssen jedes Mal, wenn ein Konto gebraucht wird, eine Anfrage an das Management schicken.
  - **Ticketing-Integration:** Benutzer müssen zu Informations- oder Prüfungszwecken eine Ticketnummer angeben.
  - **Exklusive Konten:** Konten werden erzwungenermaßen ein- und ausgecheckt und können jeweils nur von einem Benutzer gleichzeitig verwendet werden.
  - **Einmal-Passwörter:** Anmeldeinformationen werden nach jeder Verwendung automatisch geändert.
  - **E-Mail-Benachrichtigungen:** Jedes Mal, wenn ein Konto verwendet wird, wird eine E-Mail-Benachrichtigung an die Abonnenten geschickt.
- **Optionen für den Kontointegrationsprozess prüfen.** Es gibt verschiedene Möglichkeiten, Konten in den **CyberArk Enterprise Password Vault** zu integrieren. Meistens geschieht dies aber per Accounts Feed oder Massenupload:
  - **Der Accounts Feed** scannt Active Directory auf Rechner und anschließend die Rechner auf Konten. Mit dem Accounts Feed kann auch eine definierte Liste an UNIX-Systemen gescannt werden, um Konten und Anmeldeinformationen zu finden. Nach dem Scannen und Auffinden werden die Privileged Accounts und Anmeldeinformationen auf der Seite „Pending Accounts“ platziert. Dort können dann bestimmte Konten ausgewählt werden, die in spezielle Safes integriert werden sollen. Der Accounts Feed scannt OUs und Rechner, um Privileged Accounts von neu erstellten Servern automatisch zu integrieren. Der Accounts Feed ermöglicht eine flexiblere Erkennung der folgenden Konten und verfügt über die Möglichkeit, sie zu analysieren und mit Servicekontoabhängigkeiten bereitzustellen:
    - Lokale Windows-Konten;
    - Domänenkonten;
    - Windows-Dienste und geplante Aufgaben;
    - Lokale UNIX-Konten;
    - SSH-Keys und ihre Vertrauensbeziehungen.
  - **Massenupload – Das Hilfsprogramm für den Passwortupload** verwendet eine .csv-Datei der Konten und platziert sie wie in der Datei selbst definiert in Safes. Dies ist die am häufigsten verwendete Methode, wenn die **CyberArk Privileged Account Security** Lösung eine andere Passwort-Vault-Lösung ersetzt.
  - **Weitere Optionen:**
    - **Automatische Erkennung** für automatische Bereitstellung via:
      - Lokale Windows-Konten;
      - VMWare Unix-/Linux-Gastrechner;
      - VMWare ESX Host-Root-Konten;
      - Nutzung lokaler und Domänenservicekonten;
      - Anwendungskonten basierend auf Verzeichnisabfragen.
    - **Kontoerstellung, -integration** usw. automatisieren via:
      - REST;
      - API;
      - SDK.

Sobald die Lösung und die Prozesse eingerichtet und die anfänglichen Privileged Accounts integriert wurden, wird dringend eine Erweiterung der **CyberArk Privileged Account Security** Lösung empfohlen. Wie bereits oben erwähnt wurde, wird die Kontointegration normalerweise nach Risiko und Aufwand priorisiert. Daher gehört zu den bekannten Szenarien die Sicherheit von Anmeldeinformationen und SSH-Keys für den Zugriff auf Datenbanken, Netzwerkgeräte und Anwendungen – diese sind aber nicht in Stein gemeißelt. Jedes Unternehmen hat unterschiedliche Prioritäten und es gibt keine „falschen“ Ansätze. Den Unternehmen wird empfohlen, einen Ansatz auszuwählen, der am besten an ihren Anforderungen ausgerichtet ist.

- **Prüfung und Berichterstellung zu Best Practices.** Unternehmen sollten die Compliance- und Audit-Anforderungen berücksichtigen und vorkonfigurierte Berichte nutzen, die bei der Erfüllung dieser Anforderungen erstellt werden können. Die Workflows und Rollen der Prüfer, die diese Berichte erstellen, sollten ebenfalls ausgearbeitet werden. Wenn kundenspezifische Berichte erforderlich sind, können sich Unternehmen für Unterstützung an die zertifizierten CyberArk Experten wenden.
- **Überlegungen hinsichtlich CyberArk Privileged Session Manager. Für CyberArk Privileged Session Manager** und Privileged Session Manager SSH Proxy (PSMP) müssen vor der Implementierung zusätzliche Überlegungen angestellt werden. Vor einer Implementierung müssen Unternehmen:
  - Terminalserverlizenzen und CAL-Lizenzen für RDP-Services prüfen und/oder erwerben. **CyberArk Privileged Session Manager** basiert auf der Microsoft-Terminalserver-Technologie und erfordert daher die entsprechenden Microsoft-Lizenzen. Außerdem muss unbedingt sichergestellt werden, dass ausreichend CAL-Lizenzen vorhanden sind und ein Lizenzserver verfügbar ist.
  - Die PSMP-BS-Anforderungen prüfen, um die Ausführung und den Betrieb eines unterstützen BS zu gewährleisten. PSMP ist ein Linux-basiertes System und wird auf einigen – aber nicht allen – Versionen von RHEL, SUSE und CentOS unterstützt. Beachten Sie, dass PSMP nach der Installation ähnlich wie eine Appliance funktioniert. Daher sind für manche Standardmanagementprozesse und -tools möglicherweise bestimmte Ausnahmen (wie OpenSSH) erforderlich, um den PSMP-Server remote zu unterstützen.
  - Unternehmen sollten ausreichend Speicherkapazität für Session-Aufzeichnungen auf dem CyberArk Digital Vault Server und den **CyberArk Privileged Session Manager**/PSMP-Servern sicherstellen. Eine einfache Schätzung zum erforderlichen Speicher sind normalerweise 250 kb/min pro aufgezeichneter RDP-Session und 60 kb/min pro aufgezeichneter SSH-Session. Der Großteil des Speichers wird vom CyberArk Digital Vault Server benötigt. Je nach der Master Policy und der Anzahl der für die Aufzeichnung ausgewählten Sessions ist auf den **CyberArk Privileged Session Manager**/PSMP-Servern jedoch möglicherweise viel Speicher erforderlich.
  - Es sollten Gruppenrichtlinieneinstellungen konfiguriert werden, damit **CyberArk Privileged Session Manager** sicher funktioniert. Da es sich bei diesen Servern für gewöhnlich um Domänenmitglieder handelt, gelten die Gruppenrichtlinienobjekte (GPO) des Unternehmens für sie. Hinweis: Es gibt allgemeine GPO-Einstellungen, die dafür sorgen können, dass **CyberArk Privileged Session Manager** nicht mehr funktioniert. Z. B. sollte in „AllowLogonLocally“ die lokale **CyberArk Privileged Session Manager** Gruppe enthalten sein. CyberArk kann GPO-Dateien bereitstellen, mit denen alle erforderlichen Richtlinien eingerichtet werden können, sodass **CyberArk Privileged Session Manager** richtig funktioniert. Weiter Informationen können bei den CyberArk Security Services Technikern eingeholt werden.
  - Es sollte ein **Lastenausgleich konfiguriert** werden, um Spitzen beim Zugriff zu handhaben. CyberArk Privileged Session Manager wird höchstwahrscheinlich die einzige Möglichkeit für Administratoren sein, remote auf Zielsysteme zu zugreifen. Farmen mit Lastenausgleich können bei der Verarbeitung von Belastungsspitzen helfen und Systemausfälle verhindern.
  - Gehen Sie das Härtungsverfahren des **CyberArk Privileged Session Manager** durch, das im Installationspaket enthalten ist, um die Härtungskonfiguration zu verstehen.
- **Sichern von Anwendungskonten mit CyberArk Application Identity Manager und CyberArk Conjur.** Die meisten Anwendungskonten sind komplex in der Verwaltung und bleiben letztendlich lange Zeit statisch. **CyberArk Application Identity Manager** kann beide Probleme lösen: Er wird in Ihre Anwendungen integriert und verwaltet dann die Anmeldeinformationen, sogar für Anwendungen mit extrem hoher Verfügbarkeit. Anstelle von fest programmierten Anmeldeinformationen wird eine Anfrage zum Vault hinzugefügt, um das erforderliche Passwort dynamisch zu authentifizieren und anschließend abzurufen.
  - Im Laufe der Zeit wird die Sicherheit von Anwendungen immer wichtiger. Obwohl die Integration von Anwendungen aufwendig sein kann, gibt es einige Quick Wins, die schnell zu erreichen sind:
    - **Vulnerability scanners.** CyberArk partners with vulnerability and inventory scanning vendors to deliver out-of-the box integrations for joint customers. These scanning solutions typically need privileged access to run properly, and that access can be securely enabled through the CyberArk Digital Vault with minimal effort;
    - **Application Server Credential Provider (ASCP).** CyberArk bietet vorab zusammengestellte Module für die wesentlichen Java-Anwendungsserver an (WebSphere, JBoss, WebLogic, Tomcat). Mit ASCP muss kein Anwendungscode geändert werden. Es wird einfach ein neuer Authentifizierungsanbieter zum Anwendungsserver hinzugefügt und die Konfiguration vom Standardauthentifizierungsanbieter zum CyberArk ASCP-Modul geändert.
    - **Sicherheit für die Zukunft. Es ist viel einfacher, Sicherheit direkt einzurichten, anstatt bestehende Anwendungen später nachzurüsten.** Unternehmen sollten Richtlinien in Betracht ziehen, die eine Sicherung aller neuen Anwendungsanmeldedaten im CyberArk Digital Vault erzwingen, die zur Kommunikation mit anderen Servern, Diensten, Datenbanken usw. verwendet werden.

- Bei der Anwendungssicherheit besteht einer der wichtigsten Schritte bei jedem dieser Prozesse darin, so früh wie möglich mit den Anwendungsteams (Manager, Entwickler, Eigentümer) zusammenzuarbeiten, um ihnen die Vorteile der Anwendungssicherheit zu präsentieren und ihre bestehenden Prozesse zu verstehen. Ziel ist es, ihre Akzeptanz zu gewinnen, bevor Änderungen vorgenommen werden.
- Bei der Bereitstellung von **CyberArk Application Identity Manager** und/oder **CyberArk Conjur** müssen unbedingt zertifizierte CyberArk Experten für die Durchführung von Workshops einbezogen werden, um die Integration der Lösungen in den Entwicklungslebenszyklus des Unternehmens vorzubereiten. Unternehmen sollten sich einen technischen Überblick über folgende Bereiche verschaffen:
  - Verständnis darüber, wie die Produkte die bestehenden Herausforderungen angehen;
  - Ausstattung der Entwickler mit Best Practices und Entscheidungsmatrix;
  - Definition des Bereitstellungsprozesses für Anbieter, Safes, Konten usw.;
  - Integration in den bestehenden Softwareentwicklungs-Lebenszyklus (SDLC) in den Bereichen Änderungsmanagement, Integration und Bereitstellung;
  - Verwaltung des Projekts hinsichtlich Komponenteninstallation und/oder Abruf von Anmeldeinformationen.
- **CyberArk Application Identity Manager** Prozesse funktionieren sehr ähnlich wie die von Nicht-Anwendungskonten. Der größte Unterschied besteht darin, dass die Entwickler Prozesse (über ein Wrapper-Skript) aufbauen, um Passwortänderungen zu verwalten. CyberArk Security Services bietet einen Workshop zu Best Practices, Wissen und Prozessen beim Rollout von **CyberArk Application Identity Manager** an. Allgemeine Schritte bei der Bereitstellung:
  - Identifizierung der Konten;
  - Identifizierung der Anwendungsmerkmale;
  - Bestimmung des Umfangs von neuen und bestehenden Konten, Push/Pull, Laufzeitanforderungen, Nutzungshäufigkeit, halb-/vollautomatisierte Änderung usw.;
  - Infrastruktur- und Architekturdesign sowie Empfehlungen;
  - Integration von Konten in die **CyberArk Privileged Account Security** Lösung;
  - Aufbau und Konfiguration des Wrappers;
  - Zusammenarbeit mit Entwicklern bei Schulung und Dokumentation;
  - Design für eine Anwendung;
  - Pilot;
  - Validierung in einer TEST-Umgebung;
  - Reibungsloser SDLC;
  - Einführung bis Produktion.

- **Endpunkte mit CyberArk Endpoint Privilege Manager sichern.** Um den Übergang von vollständigen lokalen Administratorrechten zu eingeschränkten Rechten zu erleichtern, nutzen Sie die **CyberArk Endpoint Privilege Manager** Konsole zum Nachverfolgen der am häufigsten mit eskalierten Berechtigungen verwendeten Befehlen und Anwendungen.
  - Unternehmen sollten bestimmen, was innerhalb ihrer Umgebungen berechtigterweise erforderlich ist, und zuerst all das einschränken, das nicht gebraucht wird. Die Regeln können im Laufe der Zeit strenger werden, aber bei Bedarf je nach Richtlinie weiterhin eine nahtlose Ausweitung der Berechtigungen zulassen. Ein unmittelbares Zurückziehen aller Administratorberechtigungen auf einmal kann zu Frustration seitens der Benutzer und einem starken Anstieg der Anruferzahlen beim Helpdesk führen, denn viele Benutzer benötigen eventuell berechtigterweise Administratorprivilegien für ihre alltäglichen Geschäftsaufgaben.
  - Bei der Bereitstellung von **CyberArk Endpoint Privilege Manager** sollten sich Unternehmen an die Best Practices für Privilegmanagement und Anwendungskontrolle halten. Der Anfang kann bei Lösungsarchitektur, Inbox-Einstellungen und Richtlinienerstellung sowie der Bereitstellungs- und Rollout-Methode gemacht werden. Der *CyberArk Endpoint Privilege Manager Quick Start Guide, CyberArk Endpoint Privilege Manager Solution Guide* und *der CyberArk Endpoint Privilege Manager Installation Guide* sind gute Referenzen hierfür.
  - CyberArk empfiehlt, Workstation-Administratorberechtigungen von Endbenutzern zurückzuziehen und die Privilegien bei Bedarf vorübergehend auszuweiten.

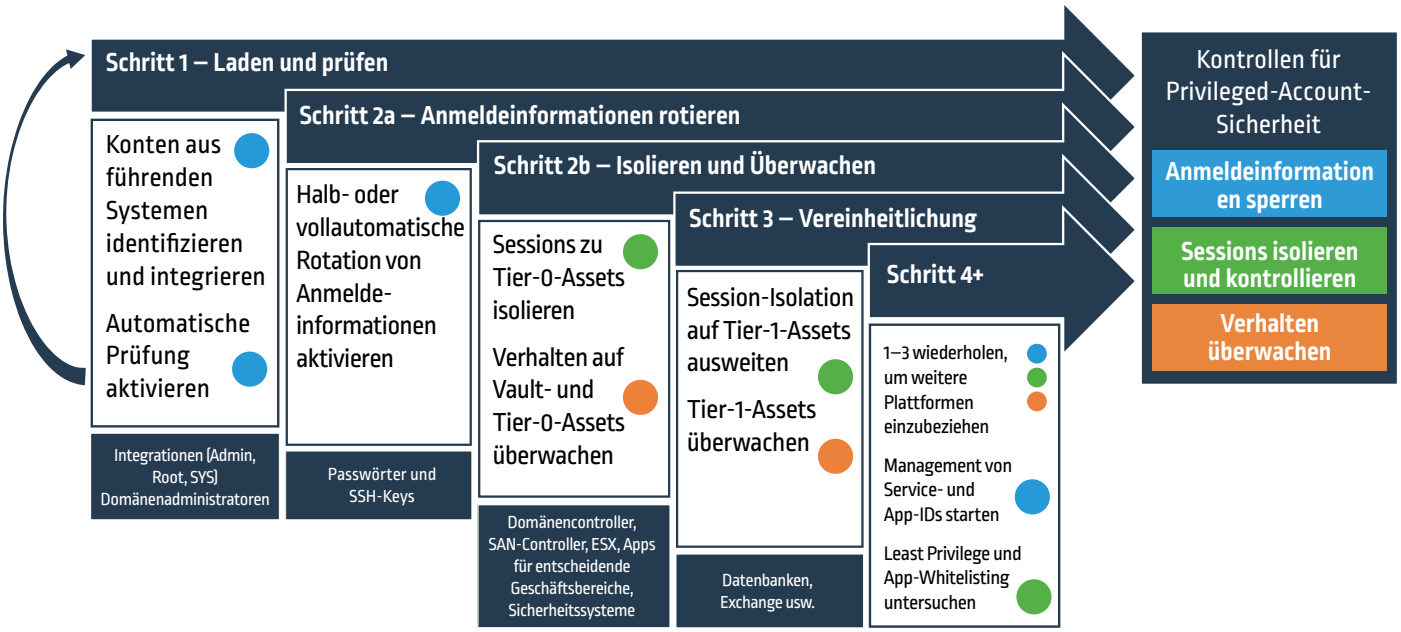
- **Erweiterte Bedrohungen mit CyberArk Privileged Threat Analytics erkennen (wird gemeinhin mit dem CyberArk Enterprise Password Vault bereitgestellt).**
  - **CyberArk Privileged Threat Analytics** sucht in Echtzeit nach Anzeichen für laterale Bewegungen oder Rechteausweitung. Dazu wird eine Baseline für das normale Verhalten erstellt und diese dann anschließend verwendet, um Anomalitäten zu erkennen. Um die bestmöglichen Ergebnisse zu erzielen, wird empfohlen, **CyberArk Privileged Threat Analytics** so früh wie möglich lernen zu lassen.
  - **CyberArk Privileged Threat Analytics** lässt sich auch betriebsfertig in den **CyberArk Enterprise Password Vault** integrieren. So können Unternehmen Bedrohungen automatisch eindämmen und nicht verwaltete Privileged Accounts integrieren. Es liefert einen zentralen Überblick, in dem Informationen vom Management privilegierter Anmeldedaten mit Privileged Threat Analytics korreliert werden. Überlegungen hinsichtlich dieser Integration:
    - **Eindämmung von Bedrohungen.** Da **CyberArk Privileged Threat Analytics** potenziell kompromittierte Anmeldedaten entdeckt, kann es Warnungen an den **CyberArk Enterprise Password Vault** senden, um eine automatische Passwortänderung auszulösen. Je nach der Phase einer Bereitstellung wird möglicherweise bevorzugt, die Warnung einzusehen, zu entscheiden, ob eine Änderung erforderlich ist, und dann manuell die Rotation per Tastenklick anzufordern. (Wenn noch nicht alle Kontoabhängigkeiten integriert wurden, könnte eine automatische Passwortänderung potenziell zu Kontosperren führen). Sobald alle Abhängigkeiten integriert wurden, kann diese automatische Rotation dem Sicherheitsteam jedoch Zeit einsparen.
    - **Kontoerkennung und -integration.** Bei Integration in eine SIEM-Lösung kann **CyberArk Privileged Threat Analytics** privilegierte Anmeldungen erkennen, die von Konten stammen, die nicht vom **CyberArk Enterprise Password Vault** oder **CyberArk SSH Key Manager** verwaltet werden, und diese Kontoinformationen weiterleiten, um die Integration zu erleichtern. Es wird empfohlen, jeden nicht verwalteten Privileged Account zuerst zu evaluieren, um sicherzustellen, dass er nicht schädlich ist. Benutzer sollten im Voraus darüber informiert werden, dass ihre Konten in die **CyberArk Privileged Account Security** Lösung integriert werden. Außerdem muss der erforderliche Zugriff der Benutzer darauf sichergestellt werden.
- **Benutzerberechtigungen in UNIX mit CyberArk On-Demand Privileges Manager kontrollieren.** Beim Verwalten von Berechtigungen mit CyberArk On-Demand Privileges Manager wird empfohlen, zunächst die „destruktiven" Befehle einzuschränken (z. B. „rm –rf /*" oder „visudo" usw.). Wenn ein Unternehmen bereits Sudo verwendet, kann es die vorhandenen Sudo-Regeln einfach erneut in **CyberArk On-Demand Privileges Manager** erstellen.

Schritt 4: Lösungsimplementierung

CyberArk Security Services stellt Unternehmen eine Checkliste mit Voraussetzungen bereit, damit sie sich entsprechend auf die Bereitstellung vorbereiten können. Unter Anleitung zertifizierter CyberArk Experten/SMEs können die technischen Leiter mit der Installation, Konfiguration und/oder dem Upgrade der **CyberArk Privileged Account Security** Lösung fortfahren.

- Unternehmen sollten einen Implementierungsplan entwickeln, in dem die Bereitstellung von Voraussetzungen (Server, Systeme und Ressourcen) und die Planung von CyberArk Security Services oder zertifizierten CyberArk Channel Partnern enthalten ist, die die Implementierung begleiten. Durch die Koordinierung mit den Änderungsmanagement-Teams wird gewährleistet, dass die Arbeit planmäßig fortgeführt werden kann. Dieser Schritt beinhaltet die Bereitstellung der CyberArk Umgebung basierend auf dem Architektur- und Lösungsdesign sowie den Voraussetzungen früherer Phasen.
- Laden Sie die folgenden Dokumente und Ressourcen herunter, in denen Sie weitere Informationen finden:
  - *Privileged Account Security System Requirements*
  - *Pre-Implementation Checklists*
  - *Privileged Account Security Installation Guide*
  - *Privileged Account Security Implementation Guide*
  - *SSH Key Manager Implementation Guide*
  - *CyberArk Endpoint Privilege Manager Installation Guide*
  - *CyberArk Endpoint Privilege Manager Migration Guide*
  - *Central Credential Provider Implementation Guide*

Phase 4 – Schnelle Risikominderung



Erste Schritte mit Privileged-Account-Sicherheit

In der vierten Phase entwickeln Unternehmen einen Rollout-Plan, identifizieren eine kleine Gruppe von Konten, die als „Pilot" verwendet werden, bestimmen (oder erstellen) eine Gruppe von Testkonten für jede Gruppe, identifizieren Probleme und aktualisieren den Rollout-Plan bei Bedarf.

Schritt 1: Laden und überprüfen

- **Tier-0-Konten integrieren**
  - **Ziel:** Füllen Sie den CyberArk Digital Vault mit Privileged Accounts, die in Phase 2 (Schritt 2, Umfang bestimmen) in Systemen mit wichtigen Ressourcen (Tier 0) identifiziert wurden, und richten Sie einen automatisierten Überprüfungsprozess ein, anhand dessen die Richtigkeit der Kontoanmeldeinformationen bestätigt wird.
  - Mit der Funktion *Verify* von **CyberArk Enterprise Password Vault** und **CyberArk SSH Key Manager** können sich Unternehmen rückversichern, dass alle Kontoinformationen im CyberArk Digital Vault richtig sind und dass die Konten bekannt und bereit für die Verwendung oder Änderung sind. Mit der Verify-Funktion werden die Anmeldeinformationen nicht geändert. Sie meldet sich einfach als das entsprechende Konto an, um zu bestätigen, dass die Anmeldeinformationen richtig sind. Dadurch werden sich die Benutzer im Umgang mit CyberArk wohler fühlen. Sie dient außerdem als Vorläufer für ein automatisches Anmeldedaten-Managementprogramm.
  - Beispiele:
    - Diese Konten könnten zuerst in Betracht gezogen werden: Domänen-Administratorkonten, Server-Administratorkonten
    - Danach könnten diese Konten folgen (je nach Unternehmen ist für diese Kontrollen möglicherweise mehr Zeit erforderlich): Lokale Workstation-Administratorkonten, Root, SYS, Enable, SA usw.
- **Connect-Schaltfläche**
  - **Ziel:** Das Konzept der direkten Verbindung mit CyberArk einführen.
  - Zusätzlich zu den Optionen „Show" und „Copy" können sich die Benutzer mittels dieser Funktion und unter Verwendung von Privileged-Account-Anmeldedaten direkt mit Zielgeräten verbinden. Durch die Connect-Schaltfläche werden die Kontoanmeldedaten gesichert und müssen nicht visuell angezeigt werden, um verwendet werden zu können. Dadurch können die Optionen *Show/Copy* in den späteren Phasen entfernt werden.

- **Kontozugriff-Workflows**
  - Die folgenden Workflows können in jeden beliebigen Schritt des phasenweisen Ansatzes integriert werden:
    - Durch die **duale Kontrolle** müssen Benutzer jedes Mal, wenn ein Konto gebraucht wird, eine Anfrage an das Management schicken.
    - Aufgrund der **Ticketing-Integration** müssen Benutzer zu Informations- oder Prüfungszwecken eine Ticketnummer angeben.
    - Durch **exklusive Konten** werden Konten erzwungenermaßen ein- und ausgecheckt und können jeweils nur von einem Benutzer gleichzeitig verwendet werden.
    - **Einmal-Passwörter** sorgen dafür, dass die Anmeldeinformationen nach jeder Verwendung automatisch geändert werden.
    - Jedes Mal, wenn ein Konto verwendet wird, wird eine **E-Mail-Benachrichtigung** an die Abonnenten geschickt.
- **Rollout der Pilotgruppe**
  - Pilotgruppen werden mittels der im Kontointegrationsprozess identifizierten Methode eingeführt.
  - Der Rest der Pilotengruppe wird mittels der identifizierten Methoden eingeführt, z. B. Accounts Feed, Massenupload – Hilfsprogramm für den Passwortupload, automatische Erkennung, REST API SDK usw.

Schritt 2a: Anmeldeinformationen rotieren

- **Ad-Hoc-Änderungen über den Central Policy Manager (CPM)**
  - **Ziel:** Den Prozess für die Verwaltung von Anmeldeinformationen über den CPM starten.
  - Einen Untersatz an Konten auswählen, die manuell über die Schaltfläche „Change Now“ im CyberArk Digital Vault geändert werden. Dadurch wird bestätigt, dass der CPM bereit für das Ändern von Anmeldeinformationen ist, und Administratoren und Benutzer können sich auf die automatischen Anmeldedaten-Änderungen einstellen.
  - Beispiele: Lokale Workstation-Administratorkonten und SSH-Keys.
- **Vollständig automatisiertes Anmeldedaten-Management**
  - **Ziel:** Die automatische Verwaltung von Konten auf Basis der Unternehmensrichtlinien beim CPM einrichten.
  - In dieser Phase aktivieren Unternehmen die Funktion für das automatische Anmeldedaten-Management von CPM. Je nach den Anforderungen des Unternehmens kann dies anhand eines feststehenden Zeitplans erfolgen (z. B. alle 90 Tage) oder jedes Mal, wenn ein Konto verwendet und wieder eingecheckt wird (z. B. mittels Einmal-Passwörtern). Dadurch wird sichergestellt, dass die Systeme mit internen und externen Anforderungen konform sind, und die Sicherheit der Privileged Accounts wird erhöht.

Beispiel mit Datenbanken: Mit CyberArk Privileged Session Manager können Sie mit FW-Konfigurationen ganz leicht umfassende Grenzen für Anmeldeinformationen aufbauen und die Möglichkeiten für laterale Bewegungen einschränken. CyberArk Privileged Session Manager ermöglicht einfachere und stärkere Firewall-Regeln, indem die Verwaltungsschnittstellen konsolidiert werden. Dank CyberArk Privileged Session Manager sind Verbindungen zur Datenbank über sich ständig ändernde Workstations mit beliebigen Management-Tools nicht möglich. Er sorgt vielmehr dafür, dass die komplette Managementaktivität von vertrauenswürdigen Systemen ausgeht und mit vertrauenswürdigen Tools abgewickelt wird. Indem alle anderen Verwaltungsschnittstellen gesperrt werden, können böswillige Agenten keine sensiblen Daten von nicht vertrauenswürdigen Systemen abrufen.

Sorgen Sie außerdem dafür, dass keine Daten diesen Bereich verlassen. Die zwei wesentlichen Ziele der Datenbank- und Anwendungsserverisolation bestehen darin, eine Infiltration der Malware und eine Exfiltration sensibler Daten zu verhindern. Durch die Beschränkung aller Kommunikationswege auf vertrauenswürdige Systeme, die bekanntermaßen Teil der Anwendung sind, wird die Wahrscheinlichkeit dafür, dass ein außerhalb der Anwendung gestarteter Angriff auf die Server innerhalb der Anwendung übergreift, gesenkt. Außerdem wird die Exfiltration von Daten erschwert.

Überwachen Sie schließlich noch die gesamte Datenbankaktivität. Wir können eine bidirektionale Syslog-Integration mit SIEM nutzen, um Daten zum Zugriff auf privilegierte Datenbankkonten zu übermitteln sowie mittels CyberArk Privileged Threat Analytics vor einem mutmaßlichen Diebstahl von Datenbankanmeldedaten zu warnen. Zusätzlich können Drittanbieter-Tools Transaktionsprotokolle überwachen, DML- und DDL-Aktivität aufzeichnen und an einem SIEM melden. Diese Daten korrelieren gut mit den Protokollen von CyberArk. Durch die Implementierung der oben genannten Strategien sowie rollenbasierter DB-Konten wird die Sicherheitsposition jeder Datenbank stark verbessert.

- **Wiederherstellung**
  - **Ziel:** Gewährleisten, dass die Anmeldeinformationen in CyberArk korrekt sind, und sie automatisch ändern, wenn sie nicht synchronisiert sind.
  - Durch die Aktivierung der Kontowiederherstellung kann der CPM sicherstellen, dass alle Konten, die von ihm verwaltet werden, akkurat sind. Wenn sie extern geändert werden (versehentlich oder um Schaden anzurichten), kann der CPM automatisch ein neues Passwort erstellen und es mit dem Vault synchronisieren. Dadurch wird verhindert, dass Benutzer die Anmeldeinformationen eines Privileged Account manuell zu einem ihnen bekannten Wert ändern, um die Sicherheit zu umgehen.

Schritt 2b: Isolieren und überwachen

Dies sollte in Verbindung mit Schritt 2a erfolgen. Der Prozess für das Rotieren von Passwörtern hängt nicht vom Prozess für das Isolieren und Überwachen ab, da es sich dabei um getrennte Module handelt. Bei der Kontoverwaltung können Unternehmen Anmeldeinformation von hochwertigen Assets einbeziehen, die von **CyberArk Privileged Session Manager** und **CyberArk Privileged Threat Analytics** profitieren werden. Dadurch werden die Grenzen der Anmeldeinformationen verstärkt.

- **Sessions zu Tier-0-Assets mit CyberArk Privileged Session Manager isolieren**
  - **Ziel:** Benutzer können ausschließlich über CyberArk eine Verbindung herstellen und Anmeldeinformationen werden Endbenutzern auf ihren Rechnern nicht mehr offengelegt. Administratorzugriff auf sensible Ressourcen über mit dem Internet verbundene Workstations wird verhindert und die Verwendung von Administratorkonten wird auf Administratoraufgaben beschränkt.
  - Die Schaltflächen *Show und Copy* sind für Endbenutzer bei Tier-0-Konten nicht mehr verfügbar. Sie müssen stattdessen auf „Connect“ klicken. Die Session wird über die CyberArk Privileged Session Manager Komponente verbunden, ohne dem Endbenutzer oder dem Rechner die Anmeldeinformationen offenzulegen. Der **CyberArk Privileged Session Manager** baut über einen „Jump-Server“ sichere Brokering-Sessions zu den Zielgeräten auf. Dieser besitzt zudem Funktionen zur Session-Aufzeichnung und -Überwachung. Alle Sessions werden vom CyberArk Privileged Session Manager mithilfe von nativen Protokollen wie RDP oder SSH vermittelt. Außerdem ist dank der Universal Connector-Funktion die Integration jedes beliebigen Anwendungs-Clients möglich, der in dem Unternehmen verwendet wird.
  - Der **CyberArk Privileged Session Manager** isoliert Sessions zu Tier-0-Assets und die Workflow-Durchsetzung und zeichnet die Benutzeraktivität auf.
  - Beispiele: Domänen-Administratorkonten, Server-Administratorkonten, Workstation-Administratorkonten, SAN-Controller, ESX, kritische Geschäftsanwendungen, Sicherheits-Appliances usw.
- **Überwachung des Verhaltens auf Vault und Tier-0-Assets mit CyberArk Privileged Threat Analytics**
  - **Ziel:** Schnelle Identifizierung anormalen Verhaltens auf wichtigen Ressourcen und dem CyberArk Digital Vault Server.
  - Die virtuelle Appliance **CyberArk Privileged Threat Analytics** wird bereitgestellt und leitet Syslog-Daten vom CyberArk Digital Vault und internen SIEM-Lösungen weiter. **CyberArk Privileged Threat Analytics** beginnt dann mit der Erstellung automatisierter Baselines für die normale Benutzeraktivität auf den Endpunktressourcen (z. B. Windows-Servern, *Nix-Servern, Oracle-Datenbanken) und dem CyberArk Digital Vault selbst. Es werden dann Warnungen ausgegeben, sobald das Verhalten von dieser Norm abweicht. Dadurch wird nicht nur auf einen möglichen Angriff hingewiesen, sondern auch eine automatische Passwortänderung veranlasst. Auf diese Weise wird der laufende Angriff im Falle eines Diebstahls von Anmeldedaten (bei dem ohne vorherigen Abruf von Anmeldedaten auf ein System zugegriffen wurde) verlangsamt.
  - Beispiele: Unübliche Zeiten, übermäßiger Zugriff, ungewöhnliche IP, ungewöhnliches Ziel, vermuteter Diebstahl von Anmeldedaten, nicht verwaltete Privileged Accounts usw.
- **Tier-0-Assets mit CyberArk Endpoint Privilege Manager schützen**
  - Ermöglicht Unternehmen, Angriffe auf Endpunkte und Server zu blockieren und einzudämmen, um das Risiko eines Datendiebstahls oder einer Datenverschlüsselung mit anschließender Lösegeldforderung zu reduzieren. Durch den Schutz von Tier-0-Assets können irreversible Netzwerkübernahmeangriffe eliminiert werden.
- **Lokale Administratorrechte auf IT-Windows-Workstations mit CyberArk Endpoint Privilege Manager entfernen**
  - Die vollständige Entfernung aller Endpunktbenutzer aus einer lokalen Administratorgruppe auf IT-Windows-Workstations kann ein guter Anfang für die Verringerung der Angriffsfläche bei Pass-the-Hash-Techniken sein. Da IT-Windows-Workstations aufgrund der erweiterten Berechtigungen und lokalen Administratorrechte für Endpunktbenutzer ein höheres Risiko aufweisen, können dadurch laterale Bewegungen im Unternehmen verhindert werden.

Schritt 3: Vereinheitlichung für Produktions-Rollout

Während dieser Phase werden zusätzliche primäre Gruppen gemäß dem aktualisierten Rollout-Plan eingeführt. Managementfunktionen, Workflows und Berechtigungen sollten zusammen mit dem Lösungsdesign bestätigt werden. Zusätzlich ist basierend auf dem Plan des Unternehmens eine Analyse der Anwendungsfälle/Anforderungen für die nächste Phase notwendig. Das Architektur- und Lösungsdesign sowie die Implementierungsphasen der Unternehmen werden überprüft. Dabei erhalten sie Empfehlungen zum Beheben von Lücken, die im Zuge dessen möglicherweise entdeckt wurden.

- **Die Nutzung individuell zugewiesener Administratorkonten minimieren** (die zu einem Anwachsen der Kontozahlen führen können)
  - **Ziel:** Administratoren müssen integrierte Konten nutzen und über einen Vault auf Anmeldeinformationen zugreifen.
  - In manchen Unternehmen ist es eventuell nicht möglich, einzelnen Personen zugewiesene Administratorkonten kurzfristig zu entfernen. Eine Möglichkeit besteht darin, die Anmeldeinformationen von individuell zugewiesenen Administratorkonten mit einem Vault zu schützen und dann im Laufe der Zeit den Wechsel von individuell zugewiesenen zu integrierten Konten zu vollziehen.
  - Beispiele: Domänen-Administratorkonten, Server-Administratorkonten, Workstation-Administratorkonten.
- **Session-Isolation und -Überwachung auf Tier-1-Assets ausweiten**
  - **Ziel:** Die in Schritt 2b beschriebenen Kontrollen auf weitere Endpunktsysteme ausweiten.
  - Zusätzlich zu On-Premise-Tier-1-Assets sollten Unternehmen die vertraulichen Zugangsdaten schützen, die von Maschinenidentitäten und Benutzern in DevOps-Umgebungen (z. B. in CI/CD-Tools eingebettete Anmeldedaten) verwendet werden. Dadurch wird das Risiko einer Kompromittierung hochgradig privilegierter API-Keys gesenkt, die in Code und CI/CD-Tools eingebettet sind.
  - Beispiele: Fest programmierte Anmeldeinformationen in Anwendungen, Datenbanken, Exchange-Servern usw.
    - Wie viele AWS-Root-Accounts und API-Keys sind nicht mit einem Vault geschützt?
    - Sind Ansible-, Jenkins- und andere Tool-Anmeldedaten in Freitext eingebettet?
- **Domänenadministratorberechtigungen für Anwendungen entfernen**
  - **Ziel:** Sollten Anwendungen Domänenadministratorberechtigungen verwenden, z. B. Domänenrechte für mehrere Server, ziehen Sie diese Berechtigungen zurück.
  - Für manche Unternehmen ist es eventuell nicht machbar, alle diese Anwendungen kurzfristig zu bearbeiten. Die Rekonfiguration oder das Umschreiben der Anwendungen erfolgt dann im Laufe der Zeit.
  - Beispiele: Anwendungskonten.

Phase 5 – Programm für Privileged-Account-Sicherheit

Schritt 1: Grundlegende Kontrollen ausweiten und erweiterte Kontrollen vertiefen

Nach der anfänglichen Implementierung der **CyberArk Privileged Account Security** Lösung weiten die Unternehmen ihr Programm für Privileged-Account-Sicherheit mithilfe desselben Prozesses auf die ganze Firma aus – Umstellung auf funktionale Konten, Integration neu erstellter Konten, Schutz integrierter Konten mit einem Vault, Rotation der Anmeldeinformationen und Verwendung von **CyberArk Privileged Session Manager** und **CyberArk Privileged Threat Analytics** für Isolation und Überwachung.

- **Grundlegende Kontrollen ausweiten:**
  - Session-Isolation auf Tier-1-Assets ausweiten
  - Tier-1-Assets überwachen
  - Zusätzliche Grenzen für die Anmeldeinformationen aufbauen, um laterale Bewegungen zu verhindern.

- **Erweiterte Kontrollen vertiefen:**
  - Zusätzliche Geräte verwalten: Netzwerkgeräte, Web-Anwendungen, Out-Of-Band-Zugriff usw.
  - Wie bereits oben erwähnt, kann dies kundenspezifische CPM-Plug-ins und benutzerdefinierte CyberArk Privileged Session Manager Verbindungskomponenten umfassen.
  - Management von Servicekonten und Anwendung-IDs starten.
  - Fest programmierte Anmeldeinformationen entfernen.
  - Least Privilege und Anwendungs-Whitelisting in Betracht ziehen.
- **Phasenweisen Ansatz für neue Systeme wiederholen (Erweiterung fortführen)**
  - **Ziel:** Führen Sie die Erweiterung der Kontrollen in Schritt 1–3 noch weiter fort. Wenn Sie dabei über Windows-Konten hinausgehen, müssen Sie den Umfang aller Privileged Accounts kennen. Privileged Accounts gibt es in vielen Technologien, darunter Oracle-Datenbanken, UNIX- und Apple-Computer, NAS- und SAN-Speichergeräte, alle Geräte mit IP-Adresse, Hypervisoren und Betriebsdienste in virtuellen Umgebungen und Cloud-Services.
  - Beispiele: Netzwerkgeräte, Web-Apps, Out-of-Band-Zugriff (iLO, DRAC) usw.
- **Management von Service- und Anwendungs-IDs starten (Vertiefung fortführen)**
  - **Ziel:** Kontrollen für Privileged-Account-Sicherheit auf nicht-menschliche IDs, Kontennutzung, privilegierte Sessions oder Analysen des Benutzerverhaltens anwenden.
  - Unternehmen müssen die Kontrollen verbessern, um die Kontonutzung zu überwachen. Für die sensibelsten Konten können beispielsweise eine Videoaufzeichnung privilegierter Sessions oder Analysen des Benutzerverhaltens eingesetzt werden.
  - Wie bei von Menschen genutzten IDs müssen die Kontrollen auch auf Service-Accounts angewendet werden. „Ausnahmen“ für Service-IDs sind nicht mehr tragbar. Ein gutes Programm für Privileged-Account-Sicherheit beinhaltet auch die automatische Rotation von Service-ID-Anmeldeinformationen sowie die mögliche Entfernung fest programmierter Anmeldedaten. CyberArk empfiehlt in der Regel, eine vollständige Kontomanagement-Bereitstellung durchzuführen, nachdem einige der anfänglichen, in diesem Dokument besprochenen Anwendungsfälle abgeschlossen wurden. Dadurch wird das Vertrauen der Benutzer und des Unternehmens in die Lösung gestärkt und ein besseres Verständnis der wichtigsten CyberArk Konzepte ermöglicht, bevor ein technisch anspruchsvollerer Anwendungsfall gewählt wird.
  - Beispiele: Windows-Services, geplante Aufgaben, IIS App Pools, Registry-Keys, fest programmierte Passwörter, containerbasierte IDs in J2EE-Plattformen
- **Umgestaltung der Anwendungen fortsetzen (Vertiefung fortführen)**
  - **Ziel:** Kontrollen für Privileged-Account-Sicherheit zur Umgestaltung von Anwendungen nutzen.
  - Bei Anwendungen, besonders älteren, sind oftmals Administratorberechtigungen erforderlich und die Passwörter sind auf eine Weise eingebettet, die das Rotieren erschweren. Unternehmen müssen im Allgemeinen sicherstellen, dass allen Anwendungen die mindestens erforderlichen Berechtigungen gewährt werden und dass Passwörter sicher verwendet werden. Um diese Probleme zu beheben, müssen Anwendungen oft rekonfiguriert oder neu geschrieben werden. Das betrifft nicht nur die eigenen, sondern auch Drittanbieteranwendungen. In manchen Fällen müssen die Unternehmen mit den Anbietern zusammenarbeiten, um Änderungen vorzunehmen.
- **Least Privilege und Anwendungs-Whitelisting verbessern (Vertiefung fortführen)**
  - **Ziel:** Granular kontrollieren, auf welche Befehle und Anwendungen privilegierte Benutzer in Windows und *nix zugreifen können.
  - Zusätzlich zum einfachen Sperren von Anmeldeinformationen und zum Isolieren von Sessions ist es bei sensiblen Systemen eventuell erforderlich, die Möglichkeiten von Konten auf Endpunkten einzuschränken, sobald sie Zugriff darauf haben. Indem begrenzt wird, welche Befehle oder Anwendungen von verschiedenen Benutzer-IDs ausgeführt werden können, kann die Wirksamkeit von Schadsoftware oder ihre Verwendung überhaupt eingeschränkt werden.
  - Dadurch wird außerdem gewährleistet, dass Mitarbeiter nur die Berechtigungen erhalten, die für ihren Verantwortungsbereich erforderlich sind. Somit wird die Compliance mit Behörden unterstützt und das Risiko von Angriffen verringert.

Schritt 2: Formalisierung des Programms anhand von Erfolgsmetriken

Durch das Sperren von Anmeldeinformationen, das Isolieren und Kontrollieren von Sessions und das anschließende Überwachen des Verhaltens wird die Sicherheitsposition eines Unternehmens auf wirksame und kontrollierte Art und Weise verbessert und die Produktionsprozesse werden nur minimal beeinträchtigt.

- Der Programmerfolg kann anhand von vielen verschiedenen Faktoren nachverfolgt werden, darunter Verringerung der durchschnittlichen Anzahl von Anmeldeinformationen pro Benutzer und Team, Senkung der Anzahl von Privileged Accounts ohne Eigentümer, Reduzierung der Anzahl nicht zertifizierter Privileged Accounts, Anzahl von Passwort-Zurücksetzungen in einer bestimmten Zeitspanne und natürlich der Prozentsatz von mit einem Vault geschützten und verwalteten Konten im Vergleich zur Anzahl der noch vorhandenen Konten.
- Diese Erfolgsfaktoren basieren auf konkreten, klar definierten Metriken. Da diese Metriken von den Berichtstools der **CyberArk Privileged Account Security** Lösung (sowie anderen Mitteln wie SIEM-Berichten oder Kontoworkflow-Audits über die Ticketing-Lösung) nachverfolgt und aktualisiert werden, erhalten die Unternehmen einen guten Überblick über den Erfolg des Programms für Privileged-Account-Sicherheit mit messbaren Ergebnissen.
- Durch den Aufbau neuer Prozesse für die Aufrechterhaltung und die Unterstützung der neuen Kontrollen und das Berücksichtigen von Fragen wie „Wie lauten die Prozesse für das Hinzufügen neuer Assets zum System und das Deaktivieren der überflüssigen?“ wird sichergestellt, dass die Prozesse mit den Veränderungen im Geschäft mithalten können – und regelmäßig geprüft, dass Sicherheits- und Geschäftsziele erreicht werden.
- Diese Metriken helfen beim Messen des Erfolgs:
  - **Prozesse anhand des Cyber Hygiene Program von CyberArk messen.**
    - Einmal im Monat **CyberArk DNA** Scans durchführen, um ungeschützte Hintertüren aufzudecken.
  - **Die Wirksamkeit bei echten Angriffen prüfen und beweisen.**
    - Regelmäßige Angriffssimulationen durchführen (z. B. mit CyberArk Red Team Services), um die Wirksamkeit der Kontrollen zu bestätigen.
  - **Wissen ansammeln.**
    - Vault-Administratoren die Möglichkeit geben, sich zertifizieren zu lassen und CyberArk SMEs zu werden.
    - CyberArk Security Services nutzen, um das Programm und den Wissenstransfer zu beschleunigen.