Delinea

PAM Reifegradmodell-Matrix

REIFEGRADDIMENSIONEN

REIFEGRADE

	PHASE 0: HOHES RISIKO (0)	PHASE 1: GRUNDLAGEN (1) Schaffung von Sichtbarkeit und Reduzierung der Angriffsfläche	PHASE 2: ERWEITERT (2) Richtlinien integrieren und überprivilegierte Benutzer einschränken	PHASE 3: ANPASSUNG (3) Zunehmende Automatisierung und Kompetenz
GRC Governance, Risk and Compliance • AU - Audit & Accountability • CM - Config Management • RA, SA - Risk & Security Assessment • SI - System & Info Integrity	→ Kein PAM Vault → Kein zentralisiertes Inventar aller Assets in der Umgebung. → Keine einfache Möglichkeit, Berichte über Benutzerzugriffsberechtigungen und Privilegien zu erstellen.	→ Erstellen Sie ein genaues Inventar privilegierter Konten und Passwörter. → Klassifizieren Sie Zugangsdaten und vertrauliche Informationen.	→ Lokale Konten, Gruppen, Rollen und Sicherheitskonfigurations, die Berechtigungen für alle Assets gewähren können, erkennen, klassifizieren und verwalten. → Implementieren Sie Sitzungsüberwachung in Echtzeit und Sicherheitszugriffskontrollrichtlinien für Endpunkte. → Durchsetzung hostbasierter Sitzungs-, Datei- und Prozessüberprüfungen mit Integration in SIEM. → Integration mit ITSM für die Freigabe von Änderungen.	→ Integration mit IGA für Prüfberichte und risikobasierte Genehmigungen. → Nutzen Sie Audit-Daten, Machine-Learning-Analysen und Automatisierung, um Bedrohungen zu erkennen, zu verfolgen und zu melden (Integration mit EUBA). → Erkennung und Klassifizierung von Servicekonten. Implementieren Sie die Erfassung, Bereitstellung und Verwaltung von Servicekonten über Identitäts- und Cloud-Service-Anbieter hinweg. Sicherung von Betriebssystemen und Anwendungskomponenten.
PA Privileged Administration • Gezielte Kontrollen von • AC – Access Control • CM - Configuration Management • MA - Maintenance • SC - System & Communications Protection SP	→ Benutzer können Administratoren ihrer eigenen Workstations sein. → Die Sicherheit der Arbeitsstation ist nicht vertrauenswürdig. → Kann die Verwaltung von Windows-Servern unter Verwendung der Gruppenmitgliedschaft Domain Admin übernehmen. → Verwaltet unter Umständen lokale Konten auf jedem UNIX/Linux-System und bearbeitet möglicherweise die lokale SUDO-Datei.	→ Regelmäßige Rotation für alle Verwaltungskonten speichern und automatisieren. → Vault Active Directory und Azure privilegierte Konten und Verwaltung privilegierter Gruppen. → Lokale Administratorkonten erkennen und sichern. → Einrichtung einer sicheren Verwaltungsumgebung sowohl für lokale als auch für Remote-Sitzungen. → Aufbau erster Arbeitsabläufe für privilegierten Zugang.	→ Einrichtung grundlegender Richtlinien zur Erweiterung der Berechtigungen für alle Endpunkte (Workstations und Server). → Einführung von Just-in-time- und Just-enough-Privilegien (JIT & JEP). → Erkennen und Verwahren von Linux- und lokalen Admin-Anmeldeinformationen (Kennwörter und SSH-Schlüssel). → Erweitern Sie die Fernzugriffskontrolle auf Dienstleister und Vertragspartner ohne AD-Konten einzurichten.	→ Erstellen Sie detailliertere Richtlinien für die Erweiterung von Berechtigungen. → Automatisieren Sie das Onboarding neuer verwalteter Assets.
IAM Identity and Access Management • AC - Access Control • IA - Identity & Authentication	→ Keine zentrale Zugriffskontrolle. → Admins greifen über lokale Administratorkonten zu. → Es ist fast unmöglich festzustellen, wer Zugriff hat und welche Rechte er hat. → Das Identitätsmanagement ist möglicherweise nicht zentralisiert.	→ Erzwingen Sie MFA für den Zugriff auf Vault, einschließlich des Check-Out von Secrets und der Einrichtung von Remote-Sitzungen. → Richten Sie alternative Administratorkonten ein, um die Verwendung öffentlicher Identitäten zu verhindern. → Erzwingen Sie alternative Administratoren und MFA für den Fernzugriff.	→ Durchsetzung der Multi-Faktor-Authentifizierung an Endpunkten für direkte Anmeldung und Erweiterung der Berechtigungen. → Beseitigen Sie lokale Konten durch Identitätskonsolidierung bei UNIX- und Linux-Servern. → Entfernen Sie schwer kodierte Anmeldeinformationen und Konfigurationsdaten aus Anwendungen und Skripten. → Automatisieren Sie die Privilegiensicherheit in DevOps-Workflows und -Tools.	→ Sicherstellen, dass alle Verbindungen, die für privilegierte Aktionen erforderlich sind, mit kryptografischen Anmeldeinformationen gegenseitig authentifiziert werden müssen. → Steigerung der MFA von NIST Authenticator Assurance Level 1 (Authentifizierung mit einer ID und einem Passwort) auf NIST Authenticator Assurance Level 2 (AAL2). AAL2 bietet eine höhere Identitätssicherheit durch das Vorhandensein eines zweiten Faktors. → Beschränken Sie den privilegierten Zugriff auf registrierte und unternehmenseigene Endgeräte. → Verhindern Sie den privilegierten Zugriff durch jedes Client-System, das nicht bekannt, authentifiziert, ordnungsgemäß gesichert und vertrauenswürdig ist. → Fordern Sie eine duale Autorisierung für privilegierte Operationen auf kritischen oder sensiblen Systemen an.
Produkte und Prozesse		→ **Produkte** • PAM Vault - Secret Server • Bastion Service - Remote Access Service • Connection Manager (optional) → **Integrationen** • SIEM → **Prozessveränderungen** • PAM Vault Training • Remote Access Training	→ **Produkte** • Server PAM - Server & Cloud Suite • Workstation PAM - Privilege Manager • DevOps Secrets Vault **Integrationen** → • ITSM für Änderungskontrolle, Störungsmeldungen • SIEM **Prozessveränderungen** → • Privilege Elevation Training • Help Desk Support für den Prozesswechsel • Schulung über den Zugang von Dritten	→ **Produkte** • Privilege Behavior Analytics • Account Lifecycle Manager → **Integrations** • IGA • SIEM & EUBA → **Prozessveränderungen** • App Developer Security Training • Automatisierung von Sicherheit und Compliance

Aligning with security and privacy controls as defined in NIST 800-53 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)