County Reinsurance, Limited

Issue No. 5 ● June 2024

CRL Cyber Circular

Privileged Access Management (PAM)

The subject of this issue of the *CRL Cyber Circular* is the fourth of the Top Cybersecurity Controls, Privileged Access Management (PAM).

All information technology enterprises maintain privileged accounts – the accounts whose holders are authorized to perform supervisory and administrative actions such as changing system configurations, installing software, accessing sensitive data, and creating or modifying user accounts. These functions may apply to servers, mainframes, network infrastructure components, databases, security appliances, and applications.

Privileged account holders range from the most experienced and trusted information technology professionals to regular users who may be given administrative access to their company-issued laptops. Privileged access credentials are a primary target of cyber threat actors because they are powerful tools that can enable attackers to inflict great damage, and to cover their tracks as they do so. Not surprisingly, a large percentage of cyber attacks involve compromise of privileged accounts.

Top Cybersecurity Controls

1. Multifactor authentication for remote access and admin/privileges
2. Endpoint Detection and Response (EDR)
3. Secured, encrypted, and tested backups
4. Privileged Access Management (PAM)
5. Email filtering and web security
6. Patch management and vulnerability management
7. Cyber incident response planning and testing
8. Cybersecurity awareness training and phishing testing
9. Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
10. Logging and monitoring/network protections
11. End-of-life systems replaced or protected
12. Vendor/digital supply chain risk management

NOTE: Numbers 1 through 5 of the Top Cybersecurity Controls are viewed by cyber insurance carriers as most important in the underwriting process. Cyber insurance applicants that lack strong controls in the top five areas may be denied insurance, pay higher premiums, or have other conditions imposed on their coverage.

Description

Cybersecurity measures aimed at preventing hackers from compromising privileged access must be a top priority. These measures are often embodied in technology systems called Privileged Access Management (PAM) solutions. PAM solutions typically include automated privileged credential management, monitoring, logging, and reporting of privileged access activity; and real-time alerting of anomalous activity.

Best Practices for Privileged Access Management

1. Minimize the number of privileged accounts and assign the least privilege necessary for each.
2. Maintain a complete inventory of privileged accounts, with automated discovery of new ones.
3. Create just-in-time temporary accounts with just enough privilege for the immediate task; eliminate or reduce standing, “always on” privilege.
4. Always authenticate privileged users with Multi-factor Authentication.
5. Monitor and log all privileged sessions, with real-time analytics to detect anomalies. Maintain a tamper-proof audit trail of every privileged session.
6. Conduct regular audits of privileged account usage.
7. Establish processes for the lifecycle management of privileged accounts, from creation through decommissioning.
8. Automate Privileged Access Management with a PAM technology solution.

Application

Building an effective PAM capability can be a complex undertaking. A coordinated technical strategy should be developed that defines how the solution will be used, the needed capabilities and coverage, integration of the solution into the network infrastructure (including Security Information and Event Management (SIEM) and IT service management tools), and post-implementation operations and maintenance resource requirements.

Implementation Suggestions

The listing of vendor products below can serve as a point of departure for organizations seeking to research PAM solutions.

Vendor	Solution	Description
CYBERARK	CyberArk Privileged Access Manager	▪ Tamper-resistant repository for privileged identities – human and machine. ▪ Credential management, rotation, and session isolation. ▪ Centralized session audit trails and recordings with built-in risk-scoring; video recording of Windows sessions. ▪ Comprehensive reporting on the use and granting of admin access, access certification and automation of privileged lifecycle management. Privileged Access Management (PAM) | CyberArk
Delinea	Delinea Secret Server	▪ Discover all identities, assign appropriate access levels, detect irregularities, and respond to identity threats in real-time. ▪ Manages privilege authorizations across all types of identities in one solution with consistent policies, even as roles, permissions, and IT resources change. ▪ Cloud-native PAM-as-a-service solution. Centralized Authorization Platform | Identity Security Solutions (delinea.com)
Microsoft	Microsoft Entra	▪ Microsoft Entra is a family of multi-cloud identity and access solutions. ▪ The Entra family includes Entra ID (formerly Azure Active Directory), Entra Verified ID, Entra Internet Access, and Entra Private Access. https://www.microsoft.com/en-in/security/business/microsoft-entra
netwrix	Netwrix Privileged Access Management	▪ Identifies privileged accounts across the entire environment. ▪ Provides on-demand privileged accounts that have only the access needed for the task and are then deleted automatically. ▪ Monitors, logs, and video-records all privileged activity. ▪ Enforces Multi-factor Authentication (MFA) for each privileged session. https://www.netwrix.com/privileged_account_manager.html
BeyondTrust	Total PASM (Privileged Account and Session Management)	▪ Automatically discover and onboard accounts, store and manage all privileged credentials, log and monitor all privileged activity, and secure employee business passwords. ▪ Dynamic Just-in-Time Access that adheres to the principle of least privilege. ▪ Control and audit all privileged sessions, on-premises and remote. ▪ Extensive privilege account, credential, and session analytics to simplify compliance (HIPAA, SOC, etc.) and benchmark tracking. https://www.beyondtrust.com/products/total-pasm

Note: This table provides information on a variety of products and services relevant to Privileged Access Management; inclusion here does not represent an endorsement or recommendation of the products and services by CRL.