beyondtrust
Beyond Traditional Security

EXECUTIVE OVERVIEW
The CISO Series

Privileged Account Management for Federal Agencies

Agencies grant access privileges easily and out of necessity, but they struggle to manage these privileges as employees move throughout divisions. Revoking unnecessary access tends to be forgotten and the process of recertification of access privileges is error-prone, time consuming, or worse, forgotten. "Insider and privilege misuse" was identified by the 2014 Verizon Data Breach Investigations Report as one of the 9 basic patterns of activity in the past decade that have resulted in confirmed data breaches.

Look no further than the case with Edward Snowden and the National Security Agency (NSA). Snowden's level of access may seem excessive, but it is not uncommon within agencies and was a contributing factor in his ability to steal sensitive documents. The outcome of this incident has reverberated through practically every Federal agency. As a result, the NSA has announced it is reducing system administrator privileges by 90%. Numerous agencies and their supporting contractors have followed suit to reduce the number of people with privileged system credentials in order to prevent another catastrophe. This case illustrates that technical controls for privileged account management (PAM) are often mismanaged and the ability to understand PAM controls to mitigate abuse is underestimated.

Insider abuse and misuse of privileges isn't the only concern; external attackers seek privileged access by compromising endpoints. Nation-state sponsored attackers use techniques that exploit system vulnerabilities and plant malware to gain remote access, evade detection, and remain persistent. If the malware steals a user's credentials, attackers can then gain access and escalate privilege. Once inside, attackers will move throughout the network in search of intellectual property, defense information, personnel records, and classified information.

Administrative access in the hands of an attacker allows for easy configuration changes to install malicious software as well as the capability to alter agency security controls. Attackers will cover their tracks by modifying log files and audit trails in their attempt to access and export data. An agency with excessive privileged accounts presents a larger pool to attack through social engineering and drive-by malware vulnerabilities. These incidents are far too common in all industries and show no sign of slowing down.

Security controls must be automated

Since 2009, the SANS Institute has published a list of 20 Critical Security Controls to take work originally done by the NSA and make it available to civilian agencies and non-government organizations. Among the controls on the list are:

- Controlled use of administrative privileges
- Controlled access based on the need to know
- Account monitoring and control
- Continuous vulnerability assessment and remediation

BEYONDTRUST KEY DIFFERENTIATORS

- Asset and account discovery capabilities map to FISMA compliance requirements and indicate when an asset has changed and when new users have been created or are changed.
- The BeyondInsight platform centralizes multiple PAM and VM solutions under a single console for managing, analyzing and reporting on both internal and external IT risk.
- BeyondTrust delivers context-aware privilege management, including the ability to discover and evaluate system vulnerabilities before allowing elevated access privileges.
- The BeyondTrust suite provides PAM and VM scalability and coverage across diverse network, web, mobile, virtual and cloud environments.
- BeyondTrust products integrate with several third-party SIEM, GRC, SRM, NMS and help desk solutions.

securitycurrent

Reliably defending systems requires the use of standardized, centralized programs that position administrators to apply effective security controls that minimize risks stemming from unchecked access to critical systems and data.

Agencies must first be able to identify and profile the IT assets and accounts existing across their diverse infrastructures. It's important to identify not only legitimate assets and accounts, but also unauthorized devices on the network, unknown accounts that need to be brought under management, and backdoor or stale accounts that must be shut down.

Security administrators must remove the human element from handling privileged passwords by storing shared administrative and root passwords, obfuscating them from users, and managing the access delegation process. Agencies then need to maintain granular control over elevated operating system and task privileges, enforcing least-privilege policies among desktop end users and ensuring administrator accountability on server actions.

Session monitoring and auditing comes into play at both the password management and privilege management levels. Granular change auditing is also critical for foundational agency technologies, such as Active Directory, Exchange, file systems, and databases. The key point here is accountability.

Finally, robust reporting capabilities are necessary for both internal communications and compliance reporting with regards to FISMA, PCI, HIPAA, and other mandates affecting federal agencies.

Effective privilege and vulnerability management security measures within every Federal agency are requirements that can no longer be ignored. Though IT security directorates make their case for more resources, there is little budgetary flexibility amid meager spending increases. As such, agency leaders are tasked with doing more, with less, and must make better use of existing security systems.

BeyondTrust at a Glance

BeyondTrust's privileged account management (PAM) solutions provide comprehensive visibility and control over account privileges within complex agency environments. BeyondTrust enables IT and security teams to collectively reduce risk not only through powerful discovery and management capabilities, but also by delivering contextual risk data and analytics regarding user accounts and IT assets across a diverse infrastructure.

The BeyondTrust PowerBroker suite of privileged account management products solves a broad set of challenges related to reducing user-based risk, including:

- mitigating insider threats through granular password and privilege management
- implementing least-privilege access controls for agency end users
- ensuring accountability of privileged users through session monitoring and auditing
- complying with regulations and fulfilling reporting requirements

Take, for example, PowerBroker for Windows, a least-privilege solution that allows everyone to login as a standard user. When a user accesses an application, PowerBroker for Windows swaps the security token for the application on-the-fly using predetermined rules. The privileges for the application get elevated, but not for the end user. This not only protects against internal threats from users, but also against external attack tactics such as "pass the hash." As a result, if an attacker does gain access to a network, they cannot do anything more than a standard user can do.

The company's PAM solutions are backed by the Retina family of vulnerability management (VM) solutions. In addition to delivering a variety of standalone Retina VM solutions for identifying and prioritizing IT asset risks, BeyondTrust has tapped Retina's underlying technology to bring new capabilities and risk analytics to the PAM side of the house.

WHY PRIVELEGED ACCOUNT MANAGEMENT?

- Excessive account privileges are an open invitation to misuse for insiders and provide a larger pool for outsiders to attack
- "Insider and privilege misuse" is one of the top 9 patterns that lead to data breaches
- PAM automation makes it possible for security administrators to apply effective security controls across an organization
- Regulatory requirements demand an audit of account access privileges

For example, PowerBroker for Windows includes vulnerability-based application management (VBAM), a patent-pending technology that scans end-user applications at run-time and can execute rules based on identified vulnerabilities, such as preventing the application from launching or triggering a notification.

BeyondTrust's PAM and VM solutions share a common management console framework called BeyondInsight. BeyondInsight is a central management analytics and reporting console for both the PAM and VM product families. Furthermore, BeyondInsight offers additional capabilities such as discovery, profiling and smart groups for identifying, organizing and reporting on assets and accounts. These capabilities enrich BeyondTrust's PAM products in ways that ordinary point solutions lack.

Consider the situation of a firewall administrator attempting to make firewall configuration changes from an unpatched workstation. The workstation is vulnerable to attack, compromise, and subsequent abuse of administrator accounts to target other network assets. BeyondTrust's suite can identify the vulnerability and automatically lower the worker's privileges until the risk is remediated.

One of the major strengths of BeyondTrust's products is the reporting capabilities—more than 260 reports delivered out-of-the-box, plus a flexible ad hoc reporting capability. BeyondTrust's context-aware security intelligence presents meaningful data for informed actionable decisions. The underlying asset, user, and account privilege data centralizes the view for security teams to manage users' needs. BeyondTrust's streamlined reporting allows auditors, operations managers, and executives to have intelligent insight into agency PAM and VM data.

BeyondTrust's PAM and VM solutions are optimal when integrated together, but can also operate independently. The BeyondInsight management console is scanner-agnostic, allowing data feeds from other vulnerability scanners. Government agencies and companies are able to protect their vulnerability management investment and still gain insight into internal, user-based risk via PowerBroker privileged account management solutions.

This Executive Overview is sponsored by BeyondTrust. For more information, visit www.beyondtrust.com