Privileged Account Abuse: Who’s Doing It, Signs to Watch For & How to Reduce the Risk

Devolutions

PRIVILEGED USERS ARE ALSO PRIME TARGETS FOR HACKERS WHO WANT TO BREACH DEVICES AND NETWORKS

Users with privileged account access are given “the keys to the kingdom” — or at least the keys to valuable floors and rooms in the kingdom — so they can be more productive and efficient while carrying out their day-to-day tasks. Unfortunately, privileged users are also prime targets for hackers who want to breach devices and networks, and ultimately steal data. In fact, a survey by Centrify found that 74% of data breaches are triggered by privileged account abuse.

The Enemies Within

What's more, not all users with privileged account access are responsible and compliant. There are generally four kinds of insiders who unknowingly and knowingly cause privileged account abuse:

- The Accidental Leaker: These users don't mean to cause harm, but due to ignorance or carelessness they fall victim to phishing emails, social media posts, and texts.
- The Compromised Insider: These users have their identity and/or device compromised. As mentioned, hackers are aggressively targeting users with privileged access, such as sysadmins, network engineers, database administrators, etc.
- The Disgruntled Worker: These users — who can be employees, contractors, consultants, vendors, or anyone else with privileged access — have a grievance with the company and seek revenge by inflicting damage. They typically aren't motivated by personal financial gain.
- The Double-Agent: These users pretend to be compliant, but behind the scenes they're stealing data for profit. Left unchecked, they can carry out their illicit activities for years.

Signs of Privileged Account Abuse

All organizations need to be concerned with privileged account abuse, including small businesses, which are now considered "ground zero" for cyber crime. Here are some key signs to watch for:

- A user deviates from their normal baseline activity. This may include unusually short or long session duration, accessing/reading/changing files outside of a normal work routine, or atypical keystroke patterns (which can be detected through biometrics analytics that use machine learning to study a specific user over time).
- A user transfers files to a personal workstation, when they are only authorized to transfer files to corporate systems.
- A user account is accessed by multiple endpoints at the same time.
- Multiple users are logged in from the same endpoint.
- Dormant accounts come back to life.
- Unusual window titles.

Also keep in mind that while most hackers aren't the cyber geniuses depicted in movies, they aren't stupid either. For example, they will often run little tests to see if their presence is detected. They will also create accounts and add them to high-privileged groups, and then wait weeks or months before accessing them.

How to Reduce the Risk of Privileged Account Abuse

Here are some tips to secure the privileged account landscape and reduce the risk:

- Audit, analyze and determine which accounts should require privileged access. Generally, all of the following account types should require elevated privileges: Domain Administrator Accounts, Local Administrator Accounts, Emergency Access Accounts, Application Accounts, System Accounts, and Domain Service Accounts.
- Enforce the Principle of Least Privilege (POLP), which grants users the bare minimum privilege required to perform their jobs.
- Implement Zero-Trust Architecture, which presumes that all users are potential threats until proven otherwise; consequently, establish network micro-segmentation to move the perimeter in as close as possible to privileged apps and protected surface areas.
- Establish a formal and standardized procedure for requesting, authorizing, making and documenting account changes, as well as verifying all critical changes.
- Quickly and completely disable accounts that are no longer needed, such as when projects finish or employees leave the company.
- Automatically track and log the activity of all users — not just privileged users.
- Clearly inform employees, contractors, vendors, and all other users (again, not just privileged users) that account usage is monitored. This can be an effective deterrent for some would-be abusers.
- Get alerts on violations of security policy and deviations from normal behavior patterns.
- Enforce rigorous control over access to systems that store confidential information.
- Maintain a complete and updated key and certificate inventory.
- Provide end users with training so they do not share passwords or click on unverified or suspicious links in emails. An online cybersecurity training platform is ideal for this purpose, as it allows end users to learn on their own schedule while supervisors/managers monitor progress.

How Devolutions Helps

In addition to the above strategies and policies, Devolutions' suite of solutions can help organizations effectively and affordably reduce the risk of privileged account abuse:

- **Devolutions Password Server** features a new integrated PAM component that supports a variety of PAM functions, including account discovery, account check out approval, and an automatic password rotation. Learn more here.
- **Devolutions Password Hub** features role-based access control, a centralized password vault, a strong password generator, total access control, and more. Also, due to the coronavirus pandemic, the free trial period for DPH has been extended from 30 days to 90 days. Learn more here.
- **Remote Desktop Manager** features role-base access control, account brokering, administrative password sharing, session recording, centralized password vaulting, and more. Learn more here.
- **Wayk Now and Wayk Den** both enable secure (cloud-based or self-hosted) access to remote machines, and they feature role-based access control, session audit trails, and other security functions that are part of a robust PAM profile. Due to the coronavirus pandemic, Wayk Den (including unlimited access to Wayk Now Enterprise) is free for six months. Learn more here.

From the Desk of Our CISO Martin Lemay:

The abuse or compromise of a privileged account usually results in havoc. Hours, days, months, and years of effort and money can be invested in preventing such a situation. However, no security professional will claim 100% security and, therefore, there is always the possibility that such a scenario will happen. This is why all organizations should prepare for the worst and apply the following guidelines on top of the tips previously stated:

- Define a well-documented incident response plan and train your staff on a regular basis. Organizations need to react quickly and efficiently to recover from situations where a privileged account has been compromised. Untrained personnel will be slow, sloppy, and may allow malicious actors to perform more damage.
- Backup your data securely. Make sure you are prepared for the worst-case scenario and have a copy of your data in a different environment – and protected by different privileged accounts. Recovery procedures and the integrity of backups should be tested periodically.

These simple recommendations can greatly reduce the impact of a compromised or abused privileged account by leveraging fast containment of threats and speeding up secure recovery of operations. Combined with the tips enumerated in the “How to Reduce the Risk of Privileged Account Abuse” section, organizations will be in better shape to prevent, detect, respond to, and recover from privileged account abuse or compromise.

The Bottom Line

The bad news is that as long as there are privileged accounts, there will be the risk of privileged account abuse. There is no way to 100% eliminate this possibility, just as there is no way to 100% eliminate cyber threats like malware, viruses, ransomware, worms, and the list goes on.

But the good news is that organizations can — and frankly, must — be proactive in reducing the risk of being victimized by external hackers and internal rogue users. After all, with great privilege comes great responsibility!