7 Kinds of Privileged Accounts that Organizations Must Secure and Monitor

Devolutions

HACKERS ALSO RELY ON VULNERABLE PRIVILEGED ACCOUNTS TO BREACH NETWORKS

Organizations rely on privileged accounts to drive productivity and efficiency. Unfortunately, hackers also rely on vulnerable privileged accounts to breach networks, access critical systems, and steal confidential data — often while remaining out of sight for months, or even years. A global survey by the Ponemon Institute on behalf of IBM found that the average time to detect a breach is 197 days, plus it takes an average of 69 additional days to contain the damage.

Given this perfect storm — i.e. businesses are increasingly relying on privileged accounts, while hackers are increasingly targeting them — it's not surprising that Gartner has identified Privileged Access Management (PAM) among its top 10 security projects for 2019. Specifically, Gartner recommends that PAM projects include nonhuman and human systems accounts, while also supporting a mix of cloud, on-premises and hybrid environments, plus APIs for automation.

Despite the vital importance of PAM for ensuring security, and the reality that 74% of data breaches are triggered by privileged credential abuse, Thycotic's 2019 State of Privileged Access Management Maturity report revealed the following surprising and alarming facts:

- 55% of organizations don't know how many privileged accounts they have, or where they are located.
- Over 50% of organizations' privileged accounts never expire or get deprovisioned.
- 72% of organizations do not store all of their privileged accounts in a secure privileged access management vault, or in a password manager.

There are many factors that contribute to this widespread lack of PAM maturity (or if you wish, hacker delight), including the fact that many organizations — especially SMBs that lack in-house cybersecurity staff — don't clearly understand what kinds of accounts qualify as "privileged", and should therefore be locked down and constantly tracked.

To close this knowledge gap, here are seven types of privileged accounts that all organizations must secure and monitor in order to keep their data, customers and reputations safe:

1. Domain Administrator Accounts

Domain Administrator Accounts hold the keys to the "crown jewels", because they grant control of the entire AD domain (all controllers, workstations, and member servers). It goes without saying — but there is no harm in repeating — that access to Domain Administrator Accounts should only be given on an as-needed basis. Remember: there is a reason why compromised Domain Administrator Accounts are widely hailed as a "worst case scenario" in the information security world. Basically, imagine the most harrowing scenario possible. And then make it 10 times worse.

2. Privileged User Accounts

As the name suggests, Privileged User Accounts grant more privileges — and hence more risk — than ordinary user accounts across one or multiple systems. For example, users may be able to modify or remove software, change application configurations, and so on. In many cases, Privileged User Accounts are not

assigned to a specific user, but they are instead shared across administrators. Basically, the rule that businesses should adopt is this: any account that grants users anything more than a standard account qualifies as a privileged account, and it must be managed and monitored accordingly. In fact, many information security experts believe that Privileged User Accounts represent the riskiest and most dangerous type of privileged access, because of how common they are, how much access to sensitive data they grant, and how easily hackers can compromise them.

3. Local Administrator Accounts

Local Administrator Accounts grant administrator-level access to local machines, and are typically used by IT teams to set up new workstations and carry out maintenance tasks. Hackers often target vulnerable Local Administrator Accounts to establish a foothold inside a network. From there, they evaluate their victims' cybersecurity defense tools and systems before launching an attack.

4. Emergency Access Accounts

Many people hide a spare key to their front door at home "just in case" they get locked out. In the same vein, many businesses create Emergency Access Accounts for secure systems. These are usually disabled by default until a critical incident happens — such as a cyber attack — in which case they can be accessed by specific users to restore systems and retrieve usage logs. Emergency Access Accounts (sometimes called breakglass accounts or firecall accounts) are highly privileged, and they definitely need to be embraced by a PAM strategy and solution.

5. Application Accounts

Application Accounts are used by applications to access various functional resources, such as databases and networks. They are also used to carry out automated tasks like software updates. Usually, Application Account passwords are stored in unencrypted text files on the network, so they can be quickly and easily retrieved by users across the organization. Unfortunately, hackers target known (and unpatched) vulnerabilities to steal these passwords so they can establish remote access, change system binaries, and even elevate standard accounts to privileged accounts in order to spread throughout the network.

6. System Accounts

System Accounts are used by services and applications (instead of human users) to launch processes and

carry out scheduled tasks. The good news is that System Accounts typically do not have the ability to log onto systems. The bad news is that they often have passwords that never change, because businesses either completely forget about them, or they've never known about their existence in the first place. As a result, System Accounts are frequently targeted by hackers, who launch binaries at elevated privileges in order to carry out remote access attacks.

7. Domain Service Accounts

Domain Service Accounts enable various applications and systems to communicate and access required resources, in order to call APIs, run reports, and so on. They are typically used for updating security patches, backups, and deploying software. The problem is that changing the password on a Domain Service Account effectively kicks it out of the festive applications and system party, until it gets a new invitation (i.e. is synced across the environment). As a result, many organizations rarely — if ever — change the password, which is precisely what hackers are counting on.

The Bottom Line

SMBs need to secure and monitor ALL of their privileged accounts, because failure to do so can lead to expensive data breaches, lingering reputation damage, and in some cases outright closure: 6 out of 10 SMBs fold within six months of a cyber attack.

At Devolutions, we are on a mission to help SMBs keep their data, customers and reputations safe. We have worked closely with two well-known analyst firms, and **are on target to deliver a robust PAM specifically designed for SMBs by the end of 2019.**

This platform will "democratize" PAM by making it affordable and accessible to SMBs everywhere. It will fulfill all core requirements, while reflecting our signature commitment to performance, usability, security and support. Please stay tuned for updates, which will be released in the weeks and months ahead!