Red River

WHY PRIVILEGED ACCOUNT MANAGEMENT

SHOULD BE YOUR 2020 PRIORITY

Whether you're a startup with a handful of employees working out of a garage, a multinational enterprise that employs thousands of people and earns billions of dollars a year across the world, or something in between, one thing is certain: You probably know that you need to be putting a premium on cybersecurity.

From internal financial figures to customer information, your data is your business, and breaches of that data can be extremely costly to you, both in terms of money and time spent fixing the problem.

A 2019 study of cybercrime found that the average cost of a cybercrime breach to an organization was $13 million USD. Taken in aggregate, aggressive efforts to improve cybersecurity and reduce risk could save businesses around the world more than $5 trillion USD over the next 5 years.

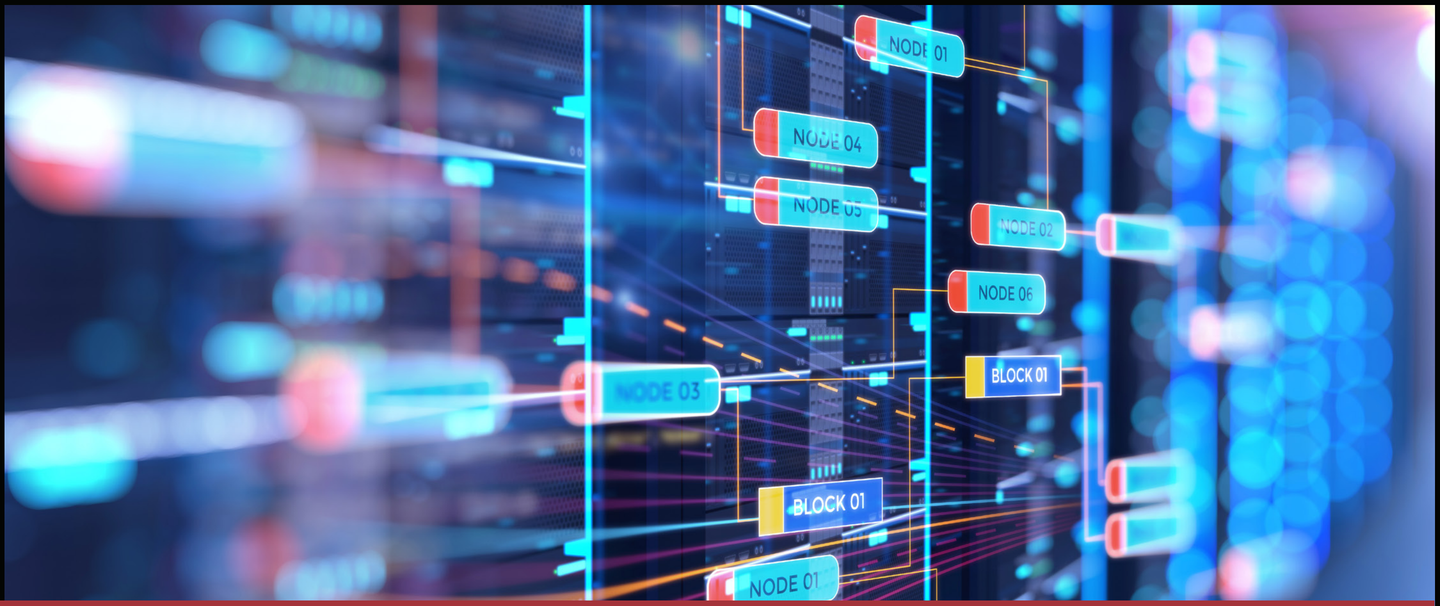
The topmost damaging types of attacks, as shown in the Accenture study, were primarily malware, web-based, and DDoS attacks, but the two with the greatest YOY growth were malicious insider attacks and ransomware attacks – types of attacks that target specific people.

How can you safeguard your business and its data against malicious actors targeting your employees? The answer is Privileged Account Management (PAM), which is why it should be one of your biggest cybersecurity privileges as we enter the new decade.

WHAT IS PAM?

Privileged Account Management, also called Privileged User Management (PUM), and its many cousins, including Privileged Identity Management (PIM) and Privileged Access Management (also PAM – yes, we know it can be confusing) all broadly fall under the larger umbrella of Identity and Access Management (IAM), which is the larger set of actions and principles that govern who, in an organization, can do what.

Broadly speaking, all of these ideas involve governing and restricting access to information and powers based on the Principle of Least Privilege.



THE PRINCIPLE OF LEAST PRIVILEGE

One of the core tenets of modern cybersecurity, the Principle of Least Privilege is a fancy name for a strikingly simple viewpoint: For greatest security, a user's account should only have the privileges to access and do the bare minimum that said user needs to do their job, and nothing more.

In other words, if an employee's job is to manage an organization's social media presence, this employee's account should probably include access to the backend for managing social media accounts, but it shouldn't let the employee install unsupervised software on their computer, or access the shared drive where the design team keeps works-in-progress. A designer, meanwhile, would have access to that drive and all the related asset libraries so that they could whip up beautiful artwork, but they wouldn't be able to access social media accounts, nor would they be able to install programs without permission.

An IT worker, on the other hand, would be able to install programs on both of these users' machines, and would likely have access to all the shared drives… but they still probably wouldn't be able to access the social media accounts.

By abiding by the Principle of Least Privilege, an organization is able to compartmentalize its risk should any one user account be compromised. Think of it like the old concept of espionage cells in spy movies – no one member knows the entirety of the organization, so if they are compromised, they can't endanger any of their fellow spies, not because they wouldn't want to give the information up, but because they simply do not have the necessary information.

When your organization follows this principle, your risk is greatly minimized.

WHO ARE PRIVILEGED USERS?

When we think of a "privileged user," our minds may understandably start thinking about users with the greatest amount of access, like IT workers or Sysadmins. However, a "privilege" just means giving a user access to any sort of system that others – no matter who – lack. Here are just some types of privileged users.

- **Employees.** Even the employees who only need access to parts of your internal, secure network have privileged access – you wouldn't extend this access to unrelated actors outside your organization like customers, would you? Employees are always considered privileged actors.

- **Third-party vendors.** Vendors may not need access to your internal systems like employees might, but it's still not uncommon to give them some form of access depending on the services or product they provide.

- **Applications.** A privileged user doesn't have to actually be a human being. If you've ever allowed a smartphone app to access your location data or images, you've made the application a privileged user on your phone. The same principle applies to companies, just on a much larger scale.

- **Security, Systems, and Web Application Admins.** It's probably not surprising that administrator-level accounts have some of the broadest privileges of them all. For the largest companies, though, where these roles may indeed be filled by multiple people rather than one administrator wearing several hats, it's important to note that even then, these administrators may not have all of the available privileges. The administrator in charge of your website and administrator in charge of your on-premise server IT have different responsibilities, after all, and so the Principle of Least Privilege means that they might not have access to the other's domain.

- **Unauthorized Users.** This group is problematic, but not necessarily malicious. It refers to users who, for some reason – typically human error – have been given access they probably shouldn't have. For instance, a former employee whose account has not been properly deactivated after leaving the organization would be in this category. Unauthorized users, who may not even know that they are unauthorized, represent a potential point of vulnerability that should be fixed, though they may not themselves be an active threat. This type of user can be very difficult to detect due to a lack of malicious behavior.

- **Hackers.** Like unauthorized users, these are people you do not want in your network, who present a very serious danger. Unlike the former category, though, hackers are actively malicious, and are the users you least want to have any sort of privilege.

  It should be noted that what many people think of as hackers – i.e., "movie hackers," who break through security systems with sheer ingenuity, using advanced software, and the like – are less common than one might think. Instead, most modern hackers are insider threats that seek to gain access to a legitimate user account through social engineering and exploiting natural human fallibility. Why bother using expensive software to break cyber defenses when you can just gain access to an account that's authorized to be in the system?

As we've previously discussed in an ebook, social engineering attacks – phishing scams, business email compromise (BEC) attacks, and the like – are some of the most increasingly common forms of cyberattacks, specifically for this exact reason. It is much easier for a hacker to try to compromise a user's account than to force access that an account should not have.

For a malicious user targeting the company where our social media manager, designer, and IT employee work, compromising either of the first two accounts would likely be beneficial, but not overwhelmingly so. They might be able to glean some information from the shared design drive or from the social media accounts, but they wouldn't be able to expand their reach into the organization. The real prize would be the IT worker's account, which could let them install software to further penetrate the network.

In a system that runs on the Principle of Least Privilege, **the accounts with the most privilege are the most prized targets for hackers**. So, how can you protect your privileged accounts?

HOW MANAGED SERVICES AND PAM KEEP YOUR ORGANIZATION SECURE

Privileged Account Management is the science and art of making sure that A) access is given to those who need it, and **only** those who need it, and B) access doesn't fall into the hands of those who shouldn't have it.

It can be extremely beneficial, when looking to implement a PAM process at your organization, to partner with a managed services provider (MSP) with the experience, know-how, and tools to make deployment simple and effective.

For instance, one of the most powerful tools on the market – and the one we ourselves use for our clients – is Thycotic Secret Server. Secret Server is a PAM solution that helps safeguard your networks through a number of features that include:

- **Active Directory integration.** Syncing with your AD deployment, Thycotic uses the same credentials to log into Secret Server, meaning your employees never need to remember more than one password.

- **Role-based Access Control (RBAC).** This controls which features Secret Server users can access within an application – can a user pull an audit, add another user to a group, or share information? – as well as which systems they can access. For example, a Tier 1 engineer cannot access SAN admin privilege.

- **Launchers.** Thycotic Secret Server helps govern the direct access and authentication into a remote machine, using Secret Server as primary interface. Launched sessions can be monitored, and passwords are masked for better security.

- **Session monitoring and auditing.** Screen capture of every session is excellent for training, auditing, and foiling malicious users.

- **User audit and forcing expires.** With a single click, you can "expire" or rotate any password that a former employee has used, making sure that nobody will ever be able to use that password to gain access that they shouldn't have.

- **Request for access control.** Sometimes, users need temporary access to privileges they wouldn't ordinarily have. For instance, let's say our social media manager needs to post art found on the design server. Lower level users can request access to systems they are not privileged to, and an admin can allow them temporary access, automatically rotating their password when the session expires and their task has been accomplished.

- **Heartbeat monitoring.** This monitoring and alerting feature checks the password in the vault to the one used by the targeted account. Failures indicate that someone has changed the password outside the Secret Server. While this could be an innocent mistake, it could also be an indication that the account has been compromised.

- **Support services.** Secret Server supports a service desk, where your IT team or the MSP can handle remediation for alerts, requests, and configuration assistance.

WHY DO YOU NEED PAM?

Other than the overall benefits of greater control over your network, PAM benefits your organization in several key ways.

Security

As previously mentioned, PAM makes your organization significantly more secure, keeping privileged accounts in the hands of those who should have them and thwarting insider threats. PAM is especially valuable when it comes to protecting Internet of Things (IoT) devices, which can be points of vulnerability into a network.

Compliance

Whether HIPPA, FISMA, GDPR, ISO, or any other "alphabet soup" regulations mandating security when handling things like personal consumer information, you want to make sure that your business is always in compliance. PAM solutions can control the use of privileged accounts and easily handle things like changing passwords after a certain time period, or removing the use of default passwords.

If you're worried about being in compliance with whatever applicable regulations your organization is subject to, consider adopting a PAM solution today.

Automation

The beauty in a PAM solution like Thycotic Secret Server is that it opens up automation for processes that can easily be missed. For instance, if an employee leaves your organization and removing their access privileges is an automated procedure, but the person assigned to do that was swamped with other work, perhaps it wouldn't get done on time – if ever.

A top-notch PAM solution will automate these processes as well as things like requests for access, requests for permanent privilege elevation, audits and reporting, monitoring and key logging, and more. The end result is greater security with much less time spent manually executing on these procedures.

If you're interested in applying a PAM solution to your organization, contact Red River today. We're experts in the field, and will be happy to use our knowledge to start protecting your business and its data.