Controlling and Managing Privileged Access

April 2021

Table of Contents

Controlling and Managing Privileged Access

According to ***Felix Gaehtgens, Research Director in Systems, Security, and Risk at Gartner,*** ***"***Privileged Access Management (PAM) is a crucial component of any security program because of the increasingly large scope of IT environments, privileged users, administrative tools, and Identity and Access Management (IAM) data such as passwords, encryption keys and certificates." [1]

While privileged access accounts are necessary to execute and control organizational operations and functions, these accounts introduce security risks and securing them is important.

Today, with the number of cybercrimes rising and threat actors focusing more on privileged accounts, controlling, and managing privileged access accounts has become increasingly challenging for CIOs and CTOs. Privileged access accounts are lucrative targets for attackers as they offer easy access to all enterprise assets and data, including files, databases, emails, systems, and applications.

Privileged accounts can be targeted by both outside hackers and insiders (such as disgruntled employees). Insider attacks are considered to be the most dangerous as they can lead to devastating losses. ***According to a global report[2] published in 2020 by the Ponemon Institute, the total average cost of insider-related incidents is 11.45 million USD.***

Definition of Insider Threat by ***Computer Emergency Response Team (CERT)[3],***

"A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

1 https://searchsecurity.techtarget.com/news/252489097/Gartner-Privileged-access-management-a-must-in-2020
2 https://www.observeit.com/cost-of-insider-threats/
3 http://ptgmedia.pearsoncmg.com/images/9780321812575/samplepages/9780321812575.pdf

A. A Few Examples of Insider Attacks

There was an insider attack on General Electric[4], where two employees stole trade secrets from the company's servers. Thousands of files were downloaded and sent to private email addresses. After investigation, the attackers were convicted, sent to prison, and penalized 1.4 million USD to recover General Electric's loss.

Another incident happened at Microsoft[5] in December 2019 when the company deployed new Azure security rules[6]. Employees misconfigured the rules, accidentally leaking a customer support database containing 250 million entries accumulated over 14 years. The incident happened because the database was not protected with a password or two-factor authentication.

Cisco[7] experienced a similar incident in September 2018.A former employee gained unauthorized access and deployed a malicious code to the company's cloud infrastructure, deleting 456 virtual machines and preventing over 16,000 users from working for two weeks.

B. Why Insider Attacks Happen

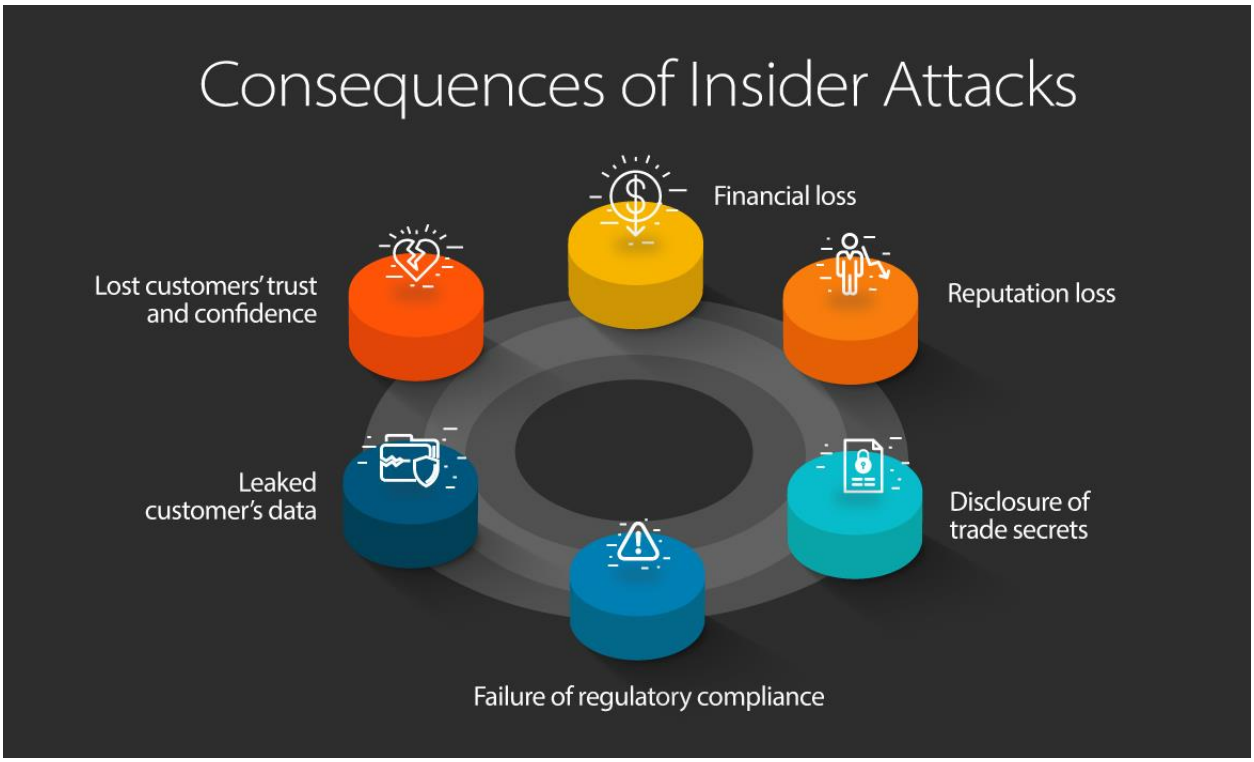
The most common motivator behind insider attacks is money. According to the Verizon 2019 Data Breach Investigations report[8], 34% of data breaches in 2019 involved internal actors. While 71% of breaches were financially motivated, 25% were motivated by the gain of strategic advantages or espionage. 29% of breaches involved use of stolen credentials.

However, sometimes data breaches may happen simply due to employees' negligence and mistakes. The IBM 2019 Cost of a Data Breach survey[9] found that 24% of data breaches were caused by negligent employees and contractors (human error).

4 https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920
5 https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=7e9bf0624d1b
6 https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview
7 https://www.bankinfosecurity.com/ex-cisco-engineer-pleads-guilty-in-insider-threat-case-a-14917
8 https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
9 https://www.ibm.com/downloads/cas/RDEQK07R

Reasons Behind Insider Attacks

Consequences of Insider Attacks



As discussed above, the possible consequences of insider attacks may harm organizations in different ways. And that is why managing and controlling privileged access accounts is crucial for CIOs and decision makers in organizations of any kind. In this paper, we will talk about Privileged Access Management (PAM), how hackers obtain access to privileged accounts, and how can CIOs control and manage privileged accounts better.

C. Privilege Access Management (PAM)

Companies often provide elevated or privileged access to some employees so that they can access enterprise network systems or sensitive data whenever needed. However, the number of privileged users varies based on the size of the enterprise. For example, small businesses often have just one privileged account that is allotted to the most trusted person in the organization, whereas medium or large businesses can have multiple privileged users who use the same privileged access credentials.

Providing elevated access can create problems if trusted employees become disgruntled and plan to cheat the organization. That's precisely why businesses need some kind of mechanism in place to prevent users from abusing elevated accounts.

Additionally, many organizations work with third-party vendors to get their job done, and for that, these third parties need to access privileged accounts and credentials. Technically, when third parties finish their jobs, the shared credentials and account access should be revoked. If this is not done, they may misuse access rights in the future. Thus, businesses must have a system in place to revoke access either manually or automatically once the task is done.

Also, businesses need to be compliant with certain regulations such as GDPR[10], HIPAA, and PCI DSS. Non- compliance may cause serious consequences.

Privileged Access Management (PAM) can help businesses deal with all the problems mentioned above. Privileged access management consists of policies, processes, and mechanisms that help ensure that all privileged users are using credentials in the right way only doing what their jobs demand. Timely audits are also a part of privileged access management, to ensure that authorities can quickly act to resolve any discrepancies.

10 https://www.42gears.com/blog/42gears-commitment-to-general-data-protection-regulation-gdpr/

D. Types of Privileged Users Accounts

Let's see how many types of privileged accounts exist:

Privileged User Account: When businesses grant privileged access to any user account beyond that afforded to a standard account, it is considered a privileged account. Privileged access accounts are considered the most dangerous type of privilege access, as they are difficult to shut down if commandeered by someone with malicious intentions.

Domain Administrator Account: These accounts are granted many privileges, including access to all servers, controllers, and workstations. That is why these accounts so frequently become a gateway for multiple security threats.

Local Administrator Accounts: IT administrators grant privileged access to local machines to carry out maintenance tasks. Sometimes these accounts are available by default at the OS level (such as in Windows[11], where it was available by default until Windows 7). Hackers may leverage these accounts to look for cybersecurity loopholes to abuse the network and system.

System or Service Accounts: System accounts can be privileged local or domain accounts. Applications and services generally use these accounts to interact with the OS, with the accounts providing privileges based on what the applications and services need. These accounts are risky because, more often than not, business executives are unaware that such accounts exist. As a result, the passwords remain unchanged for years, making such accounts vulnerable.

Application Accounts: Applications use these accounts to access organizational networks and data. Generally, application account passwords are saved in an unencrypted form, or in text files, so that they can be accessed by users whenever needed. This can be a security vulnerability, as attackers may abuse known passwords for malicious purposes.

How Hackers Obtain Privileged Access Credentials

In a CyberArk webinar[12], Kevin Naglich emphasized common techniques such as keystroke logging, password cracking, memory scraping, password spreadsheets and social engineering that are used to steal privileged credentials. Let's take a closer look at all these separate points and check some other techniques as well.[13]

11 https://www.varonis.com/blog/working-with-windows-local-administrator-accounts-part-i/
12 https://cyberark.wistia.com/medias/2ttz5d4p6w
13 https://www.cyberark.com/resources/blog/six-ways-attackers-try-to-steal-privileged-credentials

Keystroke Logging

According to Tom Bain, former VP of security strategy at Morphisec, "Keyloggers are software programs that leverage algorithms that monitor keyboard strokes through pattern recognition and other techniques.". They capture all the keystrokes of user types, including privileged passwords, and send them to a third party.

Password Cracking

Network, database, and system admins are generally people who know the entire system and infrastructure very well. For that reason, it's easy for them to crack or guess the credentials.

Memory Scraping

Memory scraping was declared one of the most dangerous attack techniques by SANS Institute, in 2011[14]. It is malware that looks into the memory of desktops to find personal data, credentials, or other sensitive data that otherwise couldn't be obtained.

Password Spreadsheets

People sometimes maintain a list of passwords in spreadsheets, but it could be devastating for a business if those spreadsheets fall into the wrong hands. Hackers generally look for spreadsheets that contain all passwords so that they can get multiple passwords at once.

Social Engineering

Hackers sometimes try to get credentials by using social engineering. Here, attackers send an email or some other kind of communication with a malicious link, with an accompanying urgent message. This results in victims promptly clicking malicious links or files. Social engineering attacks are hard to fully protect against, as they prey upon emotions.

Obtaining Application Credentials

Even when companies do a good job of protecting passwords, this is all for naught if they don't frequently change those passwords. If companies never change passwords, disgruntled former administrators can use them to access sensitive resources years after their departure.

14 https://www.cybertraining365.com/cybertraining/Topics/Memory-scraping_malware

Other vulnerabilities

- Passwords may be saved in ways that are impossible to track, such as files, spreadsheets, hard copies or print outs. As another example, admins may have circulated multiple copies of password-containing documents amongst themselves. These things make passwords vulnerable to exposure and increase the likelihood of someone abusing them for malicious purposes.
- Tracing the person responsible for password abuse is difficult in a shared environment where passwords remain impersonal.
- Failing to remove temporary passwords provided for third-party contractors.

How Privileged Accounts Should be Monitored

Decisions makers may not always be aware of the ways privileged accounts can be misused, as such accounts attract little attention. That's one of the reasons the number of insider attacks has increased significantly in recent years.

Insider attacks cannot be prevented or avoided completely; however, devising strong and effective policies and strategies to monitor privileged accounts can help minimize the frequency of attempted insider attacks.

Here are few ways in which businesses can monitor the privileged accounts:

Identifying Privileged Accounts

The first step is to identify the different privileged accounts that exist in an organization, and where they are, so they can be monitored and controlled. This can help thwart potential attacks. Administrators can implement a system to send automatic alerts to required personnel if these accounts display any suspicious activity.

There are a few tools available that can identify privileged accounts[15] in your network, and check if all privileged passwords are being changed regularly, either manually or automatically.

Monitoring Keystroke Logging

To prevent keystroke logging attacks, businesses need to continuously monitor desktop activities. In addition to this, IT managers should be able to monitor what is happening on a screen and

15 https://www.ibm.com/account/reg/us-en/signup?formid=urx-40578&_ga=2.25086009.2064868923.1615268949-785315238.1615268949

record those activities for future reference. Furthermore, managers must be able to monitor keystroke logging and revoke access at any time (if needed).

Centralized Passwords Repository

All administrative passwords should be encrypted and saved in a centralized repository to avoid storing passwords in random places. and make password cracking as difficult as possible.

Limited Access to Passwords

An employee should only be able to access passwords that they are authorized to use. This can not only minimize the occurrence of attacks but also help identify the miscreant in the event of an attack.

Automatic Password Change

All administrative passwords should automatically change (to strong, unique passwords) at fixed intervals. This will make it hard for former insiders to crack passwords.

Password Policies for Temporary Users

Temporary users should be allotted passwords that are valid only for a certain period, and only on request. Also, the moment the temporary user's job is done, access permissions should be revoked.

Regular Password Audits

All allotted passwords should be audited on a regular basis to check for irregularities and ensure that privileged account holders aren’t misusing their access rights.

Password management for employees leaving

If an employee is leaving the organization, the allotted passwords should be either transferred to some other employee or reset automatically. This helps to avoid password misuse by disgruntled employees.

Principle of Least Privilege

Organizations need to adopt the principle of least privilege, which keeps privileged knowledge as safe as possible. Passwords should be allotted as per the needs of each employee and granted

only when they are needed. This approach can help organizations avoid privileged password abuse.

E. Summary

Providing privileged access to privileged or administrator accounts isn't a problem. However, allowing these accounts uncontrolled access with no monitoring and control may have devastating consequences for any organization. With technologies evolving and organizations adopting more technology, we can't afford to become complacent. Cybercrime and insider threats will always come along with such advancements.

The good news is that we have solutions like PAM, which is a subset of IAM (Identity and Access Management). IAM has a broader coverage and includes all users while PAM is used for some privileged accounts only. But, there is a twist in this - the PAM tools available in the market have limited capability to secure IT infrastructure.

Organizations use multiple tools and applications such as CRM, EMM/UEM, Marketing, HRM tools, but PAM tools can only provide limited features that do not extend to the application level. If threat actors somehow get the passwords, they can access the tools such as CRM and EMM via these passwords. And that is why we need some kind of PAM support for these tools and apps as well. 42Gears' UEM (unified endpoint management) solution has features like role-based access (principle of least privilege), audit trails, SIEM (Security Information and Event Management) integration and MFA (multi factor authentication), which aligns with Privileged Access Management.

Try 42Gears' UEM solution[16], also known as SureMDM[17], to secure your privileged accounts.

16 https://www.42gears.com/solutions/unified-endpoint-management-uem-solution/
17 https://www.42gears.com/products/mobile-device-management/