Securden

What are Insider Threats:

How to Mitigate the Risk Posed by Trusted Insiders?

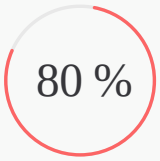
Index

Insider attacks: A brief introduction

While the instances of attacks carried out by external threat factors are well documented, the much worse counterpart is often overlooked. Insider threats, while smaller in numbers, cause bigger problems to organizations at the time of breach. Attacks perpetrated by insiders often take longer to be discovered and the damage is almost always more extensive because of the permissions/privileges the insiders already carry.

The average cost of a breach attributed to an **insider threat** costed around **$15.5** million in 2023.

Attacks perpetrated by insiders take **200 days** on average to be discovered.



More than **80%** of internal cyberattacks stemmed from privilege misuse.

Who are considered insiders?

“Insiders” is a term used to describe trusted people, often present and past employees of the organization who are trusted with access to assets by the organization. Along with employees, business partners, contractors and temporary resources are also considered insiders.

How do trusted people become insider threats?

To protect the organization from insider threats, we must first know how a trusted person becomes a threat that needs to be dealt with. Based on how they become a threat, insiders could be classified as **Malicious Insiders, Negligent Insiders, Exploited Insiders,** and **Third-party Insiders.**

- **Malicious Insiders:** These users are often disgruntled employees and ex-employees who intentionally want to damage the organization. Damage caused by intentional insider threats are often on the expensive side. In some instances, insiders have also received financial incentives to act with malice.
- **Negligent Insiders:** Negligent users habitually overstep security measures and are poorly educated on cybersecurity. They intend well but nevertheless contribute to the risk and are considered a threat. Acts of negligence can include taking home an unencrypted USB stick with customer data, noting down credentials to sensitive machines in a sticky note etc.
- **Exploited Insiders:** Exploited insiders are high ranking employees of the organization who have access to sensitive assets. They are of high value to attackers and are repeatedly targeted using advanced techniques such as social engineering and sophisticated phishing methods. The external attackers use these targets to gain a strong foothold inside the organization.
- **Third-party Insiders:** Some insiders may not be even a part of the organization. The number of contractors and vendors organizations are dealing with is at an all-time high. These third parties are often granted access to internal assets to allow them to perform their tasks. They contribute to the accumulated risk and are considered an insider threat even though they are not technically part of the organization.

Assessing vulnerability towards insider threats

Evaluating the level of exposure to insider threats is one of the very first steps an organization can take to prevent a future mishap. Before taking steps to protect against internal threats, it is imperative to identify all the ways a potential malicious insider can exploit the IT infrastructure and cause damage.

Here are a few key parameters to be assessed:

1. How many users are trusted with access to sensitive information?
2. Who has permission to export bulk data from the database?
3. How quickly is access revoked once an employee leaves the organization?
4. What is the security policy for remote workforce?
5. How frequently are the passwords rotated?
6. Is access to privileged systems monitored and tracked?
7. How is vendor access to internal IT systems regulated?

Each of the parameters discussed above needs to be addressed to ensure the organization is safe from insider threats. While some of the questions are justified implicitly, others need to be explained.

How does remote access to internal assets play a role in increasing the insider threat?

The percentage of full-time employees working from home or through a hybrid-model has shot up to 40% as of 2023. Users accessing internal IT assets from outside the corporate network is at an all-time high. While many organizations are resorting to traditional VPNs to facilitate such work models.

However, VPNs are more of an all-or-nothing security measure. The employees either get complete access to all the assets or are not allowed to access anything. The lack of granular access control in VPNs increases the risk of allowing remote employees to access corporate assets. Allowing employees to access all internal assets implies that huge trust is placed on them to not abuse their access permissions.

Your most trustworthy vendor still shouldn't be trusted

Users who are not part of the organization will often access internal assets. Instances include a vendor trying to deploy a new solution, contractors who need access to perform maintenance tasks and so on.

Access to internal assets should not be granted permanently in such cases. Permanent/standing access to assets when granted to third parties can be abused by the third-party. Additionally, when such vendors or contractors are subjected to cyberattacks, the intruders will be able to leverage the existing permissions to gain a foothold inside the corporate network.

Ex-employees pose a significant risk to corporate data

It is not possible to ensure that all ex-employees left the organization on good terms. Disgruntled ex-employees might be inclined to cause damage to the company. Not revoking access from users who are leaving the organization is extremely risky.

Ex-employees who still have access to internal IT assets can misuse their permissions and cause data leaks, service disruptions at the very least. If the passwords of sensitive assets the ex-employee had access to remain unchanged, then there is a possibility of them remembering and using the password to access internal IT resources.

Privilege escalation and lateral movement

Once threats gain foothold inside the corporate network, they will start jumping from one device to another leveraging the permissions available. Given the opportunity, attempts to escalate the user privileges will be made and access to sensitive assets is gained by the attackers.

Along with these three major scenarios, many more common practices lead to an increase in the risk faced by organizations due to insider threats. Some of these are:

1. Granting IT administrators complete access to critical systems.
2. Not tracking activities related to privileged access.
3. Storing sensitive information in plain text using spreadsheets, sticky notes, etc.
4. Granting users unfettered access to sensitive resources such as allowing them to copy files onto USB sticks.
5. Not training your employees in cybersecurity best-practices to become phishing resistant.
6. Allowing admin account passwords to stay stale for prolonged periods.
7. Allowing password reuse across corporate devices and assets.
8. Allowing employees to use corporate devices for personal work and vice versa.
9. Allowing helpdesk technicians to log in using domain admin credentials to end-user machines for maintenance work.
10. Granting developers and administrators complete access to database servers.

Avoiding these common practices can help reduce the threat faced by the organization from insiders.

For external threat vectors, gaining a foothold is a huge hurdle. However, for internal users, the foothold exists by means of the trust bestowed by the organization. Insiders are often granted access to sensitive assets to help them complete tasks. Strict access controls and activity tracking should be implemented to maintain a stringent security posture.

The principle of least privilege and zero-trust

To tackle the risk introduced by the privileged access granted to users in the organization, security principles such as Zero-Trust and the Principle of Least Privilege were developed.

The principle of least privilege mandates that users should only be granted the minimum level of permissions/privileges that helps them complete their tasks.

The **Zero-trust** security model mandates that no trust is placed upon users both inside and outside the corporate network.

The principle of least privilege and zero-trust go hand-in-hand to protect internal IT assets from external and internal threats by minimizing the blast radius of cyberattacks.

Steps to protect yourself from insider threats

There is no method that can prevent cyberattacks 100% of the time. However, breaches resulting from lax security measures and access controls can be prevented.

The most important step to prevent insiders from causing harm to the organization, intentionally or otherwise, is to limit their potential to cause harm in the first place. To achieve this, you can follow the eight steps explained below.

Step 1: Consolidate Passwords, Keys, Certs, and other Credentials into an Encrypted, Centralized Vault

Credentials belonging to privileged assets should be centrally managed for optimal control and enhanced oversight.

1. Users tend to store passwords in plaintext using spreadsheets and sticky notes. Such practices should be avoided altogether as plaintext credentials are extremely risky.
2. Local admin accounts and service accounts with stale passwords are at risk and can render the whole IT network vulnerable.
3. Credentials of sensitive assets can easily get orphaned if the device is no longer in use. However, the permissions held by the account are still powerful.

All these credentials / accounts should be discovered and consolidated inside an encrypted vault for centralized management. Using a central vault makes sharing access to IT assets easy while upholding high standards of safety.

Step 2: Enforce Password Security Best Practices and Multi-factor Authentication

Enforcing password security best practices are usually associated with preventing external credential-based attacks. However, they have a positive impact in preventing insider threats from causing damage too.

1. Periodic password resets: Automating periodic remote password resets ensures that passwords noted down on sticky notes or memorized credentials are of no use. Ex- employees or vendors will not be able to gain unauthorized access to IT assets.

2. Enforcing password complexity rules: Complex passwords are tougher to remember. Insiders who try to memorize the passwords are more likely to fail if the passwords are long and complex in nature.

3. Rotating passwords for domain accounts: Domain accounts often have dependent services and rotating their passwords could potentially stop these services from running. For this reason, domain account passwords remain stale in most organizations. These accounts are very sensitive and can be easily misused. It is important to rotate these passwords periodically. A privileged access

management tool can be used to fetch the dependencies of domain account for centralized management. Once the password is changed, the change can be propagated to the services instantly.

4. Enforcing Multi-factor Authentication: Insiders who fall prey to phishing attacks can protect themselves by using MFA. However, it is important to train all employees to be aware of phishing methods and MFA fatigue.

Step 3: Enforce Principle of Least Privilege using Granular Access Controls

Users having permanent access to sensitive assets/information have the potential to leak the data intentionally or due to negligence. It is important to limit the permissions granted to each user.

The best practice dictated by the concept of zero-trust is to never trust any user and always verify their identity before granting access. Access to sensitive information should be granted only when required, that too after multiple steps of verifying their identity.

On top of this, you can limit how much access a user gets through granular access controls and role-based access controls. This is prescribed by the principle of least privilege.

Example:

For a developer to perform their routine task, they might need to access the database management server. Instead of letting them view the password of the server, you can simply let them launch a remote connection to the asset and inject the credentials programmatically. This ensures that the user cannot view, note-down, or memorize the password of the database server.

Alternatively, a database admin might have to perform routine server administration tasks and require permissions that allow them to share access to the database server with other users. These users should be granted higher privileges than other users to let them complete their tasks.

Step 4: Enforce Strict Onboarding and Offboarding Protocols

When onboarding new employees to the organization, a set of protocol should be designed and enforced strictly.

If Azure AD (Entra) or Active Directory is used, the user profile should be created within the required user group. This is encouraged to ensure the new user gets access to the required resources/assets seamlessly.

Similarly, when an employee leaves the organization or switches their job role, their permissions should be rescinded/revised accordingly. If a new employee is tasked with the leaving user's responsibilities, the access permissions should be transferred immediately. Once transferred, the credentials accessed by the outgoing users should be rotated.

The goal is to continuously ensure that only the right users have the permissions to access sensitive information.

Step 5: Move away from VPN and Adopt Contextual Remote Access

VPNs have little to no provisions that can control and monitor who has access to which asset. It is a blanket entity which grants access to all IT assets once a user is inside. Unfortunately, all insider threats are granted access to the corporate network. Context based security provides oversight over "who" needs access to "what" and "why".

Context based security controls make it easier to adopt the principle of least privilege and limit how much access a remote user can get to a corporate asset.

Monitoring and recording remote sessions to sensitive assets can increase visibility over privileged access and improve accountability to actions. If a user is behaving suspiciously, then the remote session can be terminated, and necessary remedial actions can be taken.

Step 6: Streamline and Secure Vendor Access to Internal Assets

Granting vendors, contractors, and other third-parties access to internal assets is inherently risky. They should only be allowed to launch remote connections to the required asset temporarily. Once their access is over, the password of the remote asset should be reset immediately.

Thus, access to the remote asset is truly temporary.

Step 7: Eliminate Local Admin Rights from Endpoints and Enforce Application Control

Granting local admin rights to everyone gives rise to a wide variety of vulnerabilities across the organization. If an insider is exploited to grant an intruder access to his system, the inherent privileges held by local admins can be leveraged to gain access to sensitive information. Moreover, the intruder can then move laterally to other systems and escalate their privileges at their will.

To fulfill their job-responsibilities, most employees don't need admin rights at all. They might need to run specific apps as admin. To facilitate this a practice of on-demand privilege elevation can be adopted to grant standard users the ability to elevate specific apps and perform their duties.

Step 8: Track All Privileged Access and Activities Through Audit Trails

Maintaining a comprehensive record of 'who' had access to 'what' and 'when' is important to effectively enforce the principle of least privilege. Any change made to access permissions should be reviewed periodically to remove excess privileges.

Eliminating privilege creep can be done by periodically reviewing the list of access permissions granted to each user. Maintaining complete access history records ensures a culture of accountability in the organization.

Enforcing these steps manually can seem like a far-fetched dream. **Securden Unified PAM** is a full-fledged privileged access management solution that can help enforce password management best practices, enforce strict access controls and track privileged access effectively.

The solution consists of four different modules, all integrated into a single bundle.

1. Privileged Password Management: This module can be used to discover and consolidate privileged accounts and enforce password management best practices centrally.

2. Privileged Access Management: This module helps you enforce access controls, adopt JIT access, and control and monitor remote access to IT assets.

3. Endpoint Privilege Management: This module helps remove admin rights from endpoints and adopt JIT based privilege elevation to allow standard users to perform their tasks seamlessly.

4. Auditing and Reporting: This module tracks and records all privileged activities as audit trails which helps maintain a tamper proof record of 'who' had access to 'what' and 'when'.