PARABLU

Insider Threat: Why Insider Threats are scarier than ever

In most organizations, there is strong emphasis on perimeter security, usually targeted to eliminate, or at least minimize the possibility of data leaks and breaches by external actors. It is however important to recognize that not all threats originate outside the organization.

Statistics indicate that 34% of businesses around the globe get impacted by insider threats each year and there has been a 47% increase in the number of insider incidents over the last two years. Clearly this is a threat vector that enterprises should not take lightly.

Yet, there is little focus on insider threats and means to control them. In a recent Mimecast study, 45% of the IT professionals who were polled, identified malicious insider attacks as one of the risks that they are least prepared for.

The Pandemic and its effect on Insider Threat

But, one may ask, if insider threat has always been a problem for organizations, what has changed recently that makes them a graver concern now?

PARABLU

Many organizations entrust their knowledge workers with terabytes of sensitive company data. In return for this trust, most employees assume the huge responsibility of safeguarding this data. But given the level of access employees have, it is very likely that they themselves could turn into a threat to such data. Armed with detailed knowledge of physical and network layouts, with privileged access to critical functions, and with a deep understanding of internal business practices, malicious insiders are always in a position to cause a tremendous amount of damage.

This problem has been exacerbated during the pandemic. It has pushed a lot of enterprises to adopt third-party technologies and solutions for convenience, perhaps too quickly. This has had the undesirable result of creating an increased attack surface. Also, when working from home, in an unsupervised setup, employees are able to do things which wouldn't have normally been allowed on a corporate network. In a casual home setup, employees can also unwittingly become victims of social engineering attacks.

Whether it is a malicious insider motivated by financial gain, a disgruntled employee with an emotional motivation to destroy, or a careless worker, who disregards recommended best practices, the pandemic and the WFH arrangement has made it easier for each of these to become a more dangerous threat than ever before.

Work from Home and Insider Threat

Also, for InfoSec teams, the WFH setting has made monitoring and tracking behavioral anomalies on employee devices much more complex and difficult. Here are a few of common reasons why insider attacks are on the rise with work from home setup:

1. Mixing of personal and business habits

One of the common causes of an insider threat is when employees mix personal and business habits especially while operating on less than secure home networks. Attackers commonly categorized under Negligent and Oblivious Insiders who are not always malicious in nature can put business data at risk with a simple click on a phishing email, by demonstrating a cavalier attitude towards following password protection policies, or by sharing login credentials with a colleague.

2. Exceptional experiences that lead to unexpected behaviours

It is understood that exceptional experiences can provoke irrational responses in people. When employees work and operate in trying times, at considerable variance from their normal business setup, it can test employee resilience. Overextended employees show increased anxiety, impulsiveness, and poor judgment – all of which can be fertile ground for potential insider threat events.

3. Employee separations triggers

Unsurprisingly, a large percentage of insider attack occurred in conjunction with voluntary or involuntary employee separation events. This threat is especially heightened now, with a lot of organizations having to terminate or let go of employees remotely which may be viewed from the impacted employee's perspective as cold and impersonal. Also, because of the financial impact, the pandemic has had on organizations, their otherwise streamlined process to revoke network, application, and device access rights for terminated employees may be broken due to the new and hastily put together WFH arrangements.

There have been multiple incidents where former employees, after being terminated, maliciously deleted or edited business data, resulting in significant data losses for the businesses and worse, impacted their credibility.

4. Lowered barriers and personal gains

When working in a formal operational environment, like an office, company endpoints are protected by perimeter security measures such as firewalls, reverse proxies, and intrusion prevention systems. Now, with business starting to get conducted outside the office, coupled with limited monitoring, these barriers are gone, or at least significantly lowered – increasing the possibility of misuse of company's resources.

Malicious Deletion – and backups

Malicious employee actions, especially resulting from a job termination are not usually premeditated or driven by financial gain. They are more an emotional reaction driven by vengeance or spite. The goal of actions taken in such a state of mind are usually more biased towards destruction rather than theft. It is therefore not surprising that malicious deletion forms a significant percentage of insider threats.

The remedy for malicious deletion is ridiculously simply. Just backup all employee data. Period. The pandemic has of course made this more complex as employees and their devices are operating from homes without access to the company servers or network.

A cloud-hosted data backup, offered as a BaaS (Backup As A Service) is possibly one of the best defenses in this scenario.

How to protect against an insider attack: Best practices

The COVID-19 pandemic has impacted the data protection strategy for nearly every organization. Protecting business data from breaches and thefts while being sensitive to employee productivity has made it difficult for businesses to find the right balance. But here are few things to consider:

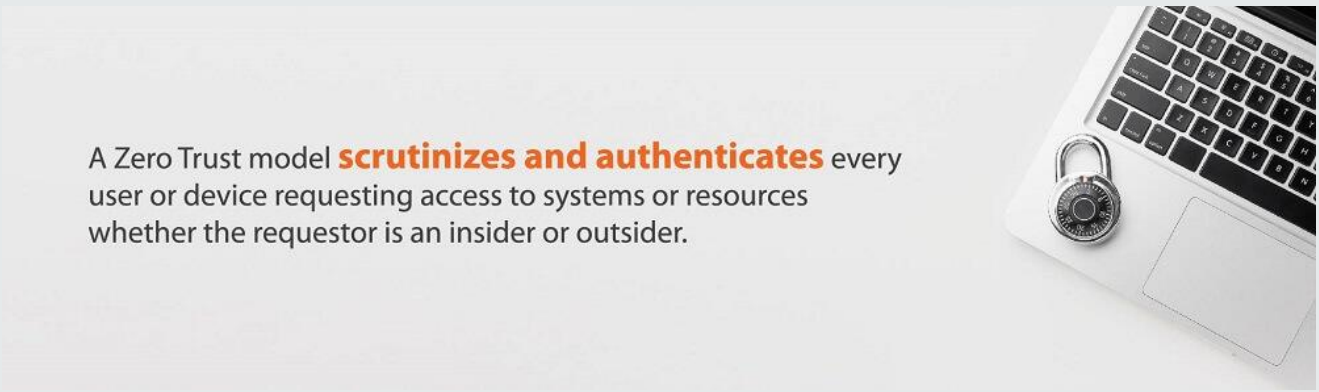
1. Communication and awareness about data security

Organizations must communicate and spread awareness about data security. Educating employees to recognize suspicious activities that could be potential threats to business data, and making employees aware of behavior that could potentially compromise the company's privacy and security stance, are important steps all InfoSec teams should take. It is also important to join forces with HR to regulate employee knowledge, investigate incidents, and ensure monitoring of access when employees change roles or leave the organization.

2. Zero Trust Model

With employees working from home and workloads shifting out of traditional data centers into SaaS clouds, organizations have increasingly started turning to a Zero Trust security model. A mechanism of continuous verification, validation, and approvals for all access, Zero Trust isn't a new paradigm, but has gained increasing relevance during the pandemic.

A Zero Trust model scrutinizes and authenticates every user or device requesting access to systems or resources whether the requestor is an insider or outsider. It is based on principles of explicit verification through a single centralized source of truth for authentication. Secondly, it enforced the Principle of Least Privilege for all accesses – which promotes granting 'just enough access and no more' than required to do the job. Zero Trust also enforces authentication/validation of access through a layered access authorization model like Two-Factor or Multi-Factor authentication. It helps the IT team to identify and block all unauthorized insider activities including high-risk activities performed by potential malicious insiders.



3. Enterprise-grade Backup Strategy

Apart from these layered defenses, implementing a secure backup and recovery process can help organizations prepare against the risk of malicious deletion. When looking for a backup solution, here are a few important things to consider:

Industrial grade encryption that enforces strict segregation of duties to guarantee data privacy.
Immutable backups which are insulated from changes made on the endpoint, so as to protect against accidental deletion, and more importantly intentional malicious insider attacks.
Centralized monitoring, reporting and audit logging.
Look for a solution like Parablu's BluVault which can ensure an encrypted, tamper-proof, versioned, backup copy of all endpoint and SaaS data – to a secure storage target. A periodic, secure copy of all data – that is backed up based on a schedule – which can be restored on demand, can go a long way towards avoiding the hassle and disruption malicious deletion can cause.

PARABLU

4. Access policies and account management

Some insiders could be armed with ready knowledge of the company's internal security processes and mechanisms. It is therefore quite important to revisit access and privilege policies periodically. Defined separation of duties and implementation of least privilege can help businesses ensure that the right set of people are authorized for the minimally necessary set of resources they need to do their jobs. This narrows the attack surface significantly.

5. Monitoring suspicious behavior

In addition to other measures, businesses can closely monitor suspicious or anomalous employee behavior, especially when they interact with critical and sensitive data. It could be custom alerts to notify IT teams when business files are moved outside of enterprise systems or employees engaging in suspicious downloads/uploads, or accessing data outside their job responsibility's purview. Such alerts can help InfoSec teams identify potential insider threats and take proactive measures.

6. Handling employee termination

Organizations should ensure that there is a streamlined post-termination procedure in place to protect data that is resident on employee endpoints or in shared drives. This procedure should involve disabling employee access to office networks, business systems/apps, and data.

At Parablu, we provide industry leading solutions for backup, archiving, content collaboration and secure file sharing. We have helped several customers achieve regulatory compliance, combat ransomware and defend against malicious insider deletion.

Want to know more about how Parablu can help you against insider attacks and see our solutions in action? Reach out to us at info@parablu.com or contact our experts here.