TACKLING THE INSIDER THREAT

THE PATH TO MITIGATION

It is becoming common for organizations of any nature to be violated by data breaches. Breaches occur when an organization's security infrastructure is penetrated and sensitive data is accessed. The malicious path individuals take to penetrate an organization's data varies. Because of this variation, organizations must be open minded to different, evolving threats and be prepared for them.

> 43% of data breaches that occur are caused by individuals with inside access into a company.[1]

These negligent or malicious individuals are given the name Insider Threats. An insider is any individual - contractor, employee, manager or CEO - that has access to sensitive company data, and they have the administrative rights to inflect changes on that data. An insider threat can steal, destroy or transfer data from an organization. They can take many different forms; which we will further explore in this paper.

Data breaches due to insider threats are boundless. The threat is ever evolving, and the industry must keep up. However, there is a silver lining. Organizations can actively prepare with forward-thinking preventional methods to defeat insider data loss. Take action - threats are zoning in on organizational vulnerabilities and adapting to current defenses.

WHAT IS THE INSIDER THREAT?

Insider Threats: Insider, in security jargon, refers to anyone who has privileged access to sensitive data inside your organization.

FOUR TYPES OF INSIDER THREATS

Let’s look further at the insider threats organizations must look for. There are four types of insider threats that are anticipated to make their rounds in the cyber security world.

The **oblivious insider** is any individual who has access to valuable company data. This insider likely assumes it is business as usual and has no knowledge that something is amiss within the organization. This insider is entirely unaware that the company is vulnerable and in a breached state, as the organization is probably monitored from the outside.

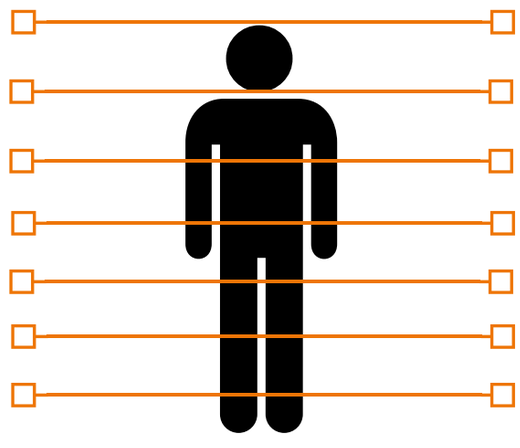
The **negligent insider** is next. This insider may be uneducated or they may simply workaround cyber security measures. This insider is vulnerable to click or open an infected link or webpage. The negligent insider’s entire lack of caution has put the organization at risk.

> RSA was hit by a phishing attack carried out by two hacking groups as well a foreign government in 2011. Unknowing employees clicked on a malicious link that allowed the hackers inside where they compromised SecurID authorization tokens and accessed 40 million employee records.[2]

The **malicious insider** is an individual who is purposefully seeking to cause harm to an organization. A malicious insider comes in many forms. This insider has the purpose of malicious intent. They may go through several hoops to reach their goal of destroying or stealing data. They may be a disgruntled employee destroying data as they leave or an employee who is secretly transferring sensitive data files offsite to make a profit on the darknet.

> In April 2017, Anthem Medicare Insurance discovered they had been struck by a data exfiltration attack via a malicious insider. It was discovered that the disgruntled insider had been emailing data to their personal email address since July 2016. 18,000 insurance members had personal health information (PHI) stolen.[3]

Finally, we have the **professional insider**. This insider may be acting under the facade of a real employee while secretly compromising the organization. A professional insider may seek out an organization with vulnerabilities to target or simply search for vulnerabilities where they are employed. Once a malicious insider has obtained the data, they sell the data on the darknet for profit.



> In 2016 a UK accounting firm, Sage, had salary and bank information breached. This occurred when an employee purposefully accessed internal log-in data they did not have authorization to.[4]

INSIDER ATTACKS: WHERE'S THE ENEMY?

The Netwrix 2018 Cloud Security Report stated that 58% of attacks in 2017 were caused by employees. [5]

That's over half of the attacks on sensitive data. These threats go undetected for months, because they can be perceived as everyday activity. For example, an employee might send data to a personal email or delete files once a week.

"Over a quarter (28%) of attacks involved insiders. The insider threat can be particularly difficult to guard against, it's hard to spot the signs if someone is using their legitimate access to your data for nefarious purposes." [6]

Furthermore, it may be difficult to prove an employee or vendor is guilty of suspicious activity without having concrete forensic evidence.

62% of employees involved in an insider attack were seeking to establish a second income from their employer's data. 29% of employees stole data to take with them to future jobs and 9% were looking to sabotage their company; the remaining employees were attributed to being negligent.[7]

The latter percentage of employees are acting destructive in nature, both with a purpose and/or carelessness. Data is being manipulated, stolen or breached either way.

45% of IT leaders disclosed that an insider attack is the type of attack they are the least prepared for. [8]

This indicates that a large amount of organizations are not asking the fundamental question. It's not a matter of 'if', but it's a circumstance of 'when.' It's not '*If* an insider attack hit us?' but '*When* will an insider attack hit us?' The message here is simple, prepare for insider threats, because they are inevitable. How do organizations prepare?

FORWARD PROGRESSION: INSIDER THREAT MITIGATION

The first step in insider threat mitigation is becoming aware of all four types of threats and preparing mitigation methods for each. There are standard preventional tactics that organizations can use to combat the insider threat. Firewalls, antivirus software and backing up your data are not enough. They are simply the beginning framework.

Coupled with traditional security tools as mentioned, other forms of data loss prevention tactics are not enough for the insider threat. Standard prevention tactics like performing employee background checks, implementing least privilege access for unnecessary areas and training employees on cyber threats are important.

However, the effectiveness of all of these tactics fluctuate. An employee with a clean background check can evolve into a criminal. Least privilege access policies can become ineffective; if an employee uses someone else's computer or accesses another's credentials. There is no guarantee that employees will abide by the policies, techniques and tools explained in any training sessions. Further, changes in workflow or structure can lead to a disgruntled employee that can potentially become an insider.

Modern day technology advancements have led us to a much more comprehensive and effective way to mitigate the insider threat. Now, organizations can identify threats to their sensitive data by using monitoring detection and behavioral analytics software.

Monitoring software operates through machine learning and behavioral analytics, once the software is deployed it will identify organizational trends. From here, a profile of normal behavior is established. Any trend variation or unusual activity will be noted.

This technology is a progressive and proactive approach to insider threat mitigation. It allows automated detection and alerts to be delivered in real-time to the admin. Threats are detected quicker and forensic evidence of the breach can be provided.

FORWARD PROGRESSION: INSIDER THREAT MITIGATION

Did you know? 87% of [data breach] compromises took minutes to execute?[9]

Data can be used for training methods, or an employee can be stopped in mid-action from performing a bad data hygiene practice. The training benefits of monitoring software are not to be understated. Using interactive, real examples of what to do vs what not to do is the content that needs to appear in training sessions rather than a slideshow.

The findings from monitoring software are impactful for privileged access training as well; those users have extensive access to sensitive data. It is pertinent to keep privileged access users current in training to stay on top of threat trends and risk mitigation.

Employers can monitor file transfers, emails and behavioral trends to determine if an insider is stealing sensitive data. Through an anomaly detection feature, when an employee performs an undesirable action - categorized by the administrator - notification is swift and detailed. Some changes recorded are: a shift in working hours (working at times when nobody else is), a decrease in productivity, missing deadlines or meetings or completing tasks outside of their regular duties.[10]

A comprehensive dashboard compiles all activity monitored within the organization, whether employee or third party vendor related.

FORWARD PROGRESSION: INSIDER THREAT MITIGATION

Let’s refer back to our four insiders with examples of how user analytics and monitoring can prevent each of these scenarios.

The **oblivious insider** has opened a seemingly typical vendor email detailing that the employee must update credentials. Through email monitoring, the employer can identify the dangerous email and halt the interaction.

The **negligent insider** who carelessly breezes past security measures has clicked on an infected link. Monitoring software will alert to the link as well as allow the employer to locate the source of the link and perform any necessary damage control.

The **malicious insider** was just fired and is searching for data to destroy. Monitoring software will alert you to any files that are being tampered with allowing you to intervene.

The **professional insider** is attempting to exploit a company vulnerability to steal data for profit. Advanced DLP coupled with monitoring software provides data visibility, allowing you to view and halt any data transfers.

Teramind software offers organizations the threat detection, monitoring and security measures necessary to arm themselves against the influx of insider threats coming our way.

TERAMIND

TACKLING THE INSIDER THREAT: THE PATH TO MITIGATION

TRY TERAMIND

TERAMIND.CO | HELLO@TERAMIND.CO

Works Cited

1. Seal, Tara. (2018). Infosecurity Magazine. Insider Threats Responsible for 43% of Data Breaches. Retrieved from https://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/.

2. Leyden, John. (April 4, 2011). Edgify. RSA Explains How Attackers Breached Its Systems. Retrieved from https://www.theregister.co.uk/2011/04/04/rsa_hack_howdunnit/.

3. ObserveIT. (March 22, 2018). ObserveIT. 5 Examples of Insider Threat-Caused Breaches that Illustrate the Scope of the Problem. Retrieved from https://www.observeit.com/blog/5-examples-of-insider-threat-caused-breaches/.

4. Ashford, Warwick. (August 15, 2016). Computer Weekly. Sage Data Breach Underlines Insider Threat. Retrieved from https://www.computerweekly.com/news/450302518/Sage-data-breach-underlines-insider-threat.

5. Melnick, Jeff. (January 23, 2018). Netwrix. Cloud Security Risks and Concerns in 2018. Retrieved from https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/.

6. Verizon. 2018 Data Breach Investigations Security Report. 2018. Verizon Enterprise. Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

7. Kohen, Isaac. (March 13, 2018). B2C. Insider Threat: A New Threat to Cybersecurity. Retrieved from https://www.business2community.com/cybersecurity/insider-threats-new-threat-cyber-security-02027677.

8. Thudium, Megan. (September 4, 2017). IT Security Central. 4 Different Types of Insider Attacks. Retrieved from https://itsecuritycentral.teramind.co/2017/09/04/4-different-types-of-insider-attacks-infographic/.

9. Verizon. 2018 Data Breach Investigations Security Report. 2018. Verizon Enterprise. Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

10. Thudium, Megan. (October 4, 2017). IT Security Central. Observable Behaviors of a Malicious Insider Threat. Retrieved from https://itsecuritycentral.teramind.co/2017/10/04/observable-behaviors-of-a-malicious-insider-threat-infographic/.