CYBERLINX
People | Process | Technology

INSIDER THREATS UNPACKED

Insider threats are not new and have been with us for a long time, however the focus on these threats have definitely been lacking in the industry. The primary reason for this is that over the last 10 to 15 years cyber security has been extremely focused on protecting us from outside attackers, such as the hackers who want to infiltrate organisations using malware. The result is that we've seen countless cyber security companies established to specifically detect and prevent malware and hack attacks. This is great for all organisations, but unfortunately it has left the insider as the soft target for attackers. Below we will discuss what exactly insider threats are, the types of insider threats, and provide recommendations to reduce the risk of these threats.

WHAT IS AN INSIDER THREAT?

Insider threats are threats that originate from within the organisation. This typically includes employees, consultants, partners, and contractors. Put simply, anyone who has legitimate access to an organisation's corporate network is considered an insider threat. Since these individuals have legitimate user accounts, they already have the access required to disclose, modify, and delete sensitive company information without the need to bypass the company's perimeter defences.

TYPES OF INSIDER THREATS WITH EXAMPLES

When we discuss the types of insider threats, we usually refer to malicious insiders who intentionally allow sensitive information to leave the company motivated by financial gain or revenge. However, insider threats are also about the unintentional mistakes that we as human beings naturally make almost every day. Knowing and gaining an understanding of how and when these mistakes happen and treating them as educational opportunities is crucial to address unintentional instances of insider data breaches. Let's look at a couple simple examples of both unintentional and intentional insider threats below.

Unintentional

A user receives a phishing email from a hacker containing a link that looks legitimate. The user clicks on the link by mistake without any intent to do harm to the company, resulting in malware being injected onto the user's machine. This could lead to a compromised user account giving the hacker legitimate access to the corporate network. The hacker utilises the compromised account to escalate privileges and steal sensitive information from the target organisation.

Instead of using malicious links or attachments to inject malware onto the target user's machine, the hacker impersonates a trusted source such as the CEO, a fellow colleague, or a third-party supplier. This is called an impersonation attack and typically involves the user receiving an email from a seemingly trusted source asking them to send by example banking information or login credentials. The user, unaware that he/she is engaging with an imposter, unintentionally sends the hacker the requested information resulting in a data breach.

Another common example is where a user takes sensitive company information off the corporate network. Typically, the user will upload sensitive information to their personal cloud storage provider such as Google-drive or email sensitive information to their personal email account to work from home over the weekend. This is exactly what happened to an employee working at the aviation company, Boeing. In this case, the employee took a company spreadsheet home with him to work on over the weekend which unfortunately resulted in personal information on 36 000 employees being exposed.

Intentional

A disgruntled employee who has legitimate access to sensitive company information abuses this access and intentionally discloses the company's intellectual property or trade secrets resulting in a data breach. This is especially dangerous when the employee has elevated levels of privilege, such as network administrators or database admins. This is what happened to a company called General Electric (GE). In this case, an employee with legitimate access to trade secrets and proprietary data, successfully exfiltrated over 8 000 sensitive documents from GE's systems. The employee's intention was to start a competing company utilising the stolen information to gain a professional advantage.

Another interesting real-world example of a malicious insider comes from a former employee of Coca-Cola and Eastman Chemical Company. The employee had access to trade secrets and intellectual property at both employers as part of her role. Due to this access, the employee had no need to perform a sophisticated attack and instead used Google-drive to upload and steal the sensitive information. The employee was working with a co-conspirator with the aim of disclosing the information to a Chinese company. Court proceedings for this employee is currently underway.

RECOMMENDATIONS TO REDUCE THE RISK AGAINST INSIDER THREATS

Before we dive into the recommendations it is important to understand that insider threats are not a technology problem but rather a human problem. It is in this context that we need to address the threats posed by insiders. At Cyberlinx Security, we believe that any effective cyber security strategy is dependent on three key areas: People, Process, and Technology. Let's apply these areas to build a holistic Insider Threats Management (ITM) programme.

People

1. A cyber awareness training programme is essential in stopping incidents of unintentional insider threats. Educating internal staff on the tactics, techniques and procedures used by malicious actors such as phishing, ransomware, and scams. This allows your users to become resistant against making costly mistakes.

2. Understanding that insider threat prevention and detection is a collective effort within any organisation, it requires commitment and teamwork from all the stakeholders and departments involved, including the security team, HR, Legal and Compliance.

3. For intentional or malicious insider threats, make sure you are aware of the typical behavioural indicators that malicious insiders and compromised insiders display. For example, if an employee's account has been compromised or when a malicious insider is attempting to exfiltrate sensitive data, they will almost always leave a trail of clues behind. Typically, this will involve the malicious insider or compromised insider performing system level activities that fall outside of the normal user interactions with data.

4. Differentiate between instances of malicious insiders and unintentional insiders with the aim of tailoring your incident response according to the harm done and motivations involved.

Process

1. A thorough company risk assessment to identify the company's unique risks pertaining to insider threats. This will provide you with the understanding and clarity required to start mitigating and reducing the risks associated with insider threats.

2. Make sure to create consistent, repeatable processes that are fair to all employees within the organisation. Utilise technology to enable and support these processes.

3. Implement the Principle of Least Privilege throughout the organisation. The Principle of Least Privilege refers to an information security concept in which a user is given the minimum levels of access – or permissions – needed to perform his/her job functions.

Technology

1. Implementing a modern Data Loss Prevention (DLP) solution. A modern DLP is a toolset that allows you to monitor how data is used and moved. It provides the ability to monitor and/or block unwanted usage and sharing of data. Make sure the DLP solution implemented has the following capabilities:
   - Data Visibility: You can't protect what you can't see. Data Visibility is understanding how you collect, store, use, process and share data in your organisation.
   - Data Discovery: The process of discovering all data and file types that are stored in Databases, Fileservers, Servers, and Endpoints. This data is then matched to the defined classification criteria in order to promote data visibility and protection.
   - Classification: Data classification employs a repeatable and consistent process to evaluate digital data and assign a classification tag – either visibly, in the document metadata, or both. That tag is then used to establish the relative sensitivity of the document to the business.
   - Data Taxonomy: Data taxonomy is the classification of data into categories and severity levels depending on the data's purpose and sensitivity. Data needs to be organised into common terminologies so that it promotes usability across multiple platforms and assists the classification process.

2. Implementing an Endpoint Detection and Response (EDR) technology to successfully combat malicious activity within the organisation. EDR software monitors endpoint processes to detect malicious actions such as malware, trojans, ransomware and any attack that involves abnormal processes on endpoint devices. This software can successfully detect insider compromised accounts as these accounts will typically generate abnormal processes such as the escalation of privileges to access sensitive information. An EDR solution will detect these endpoint processes and trigger an alert for investigation by the security team.

3. Implementing a Privileged Access Management (PAM) solution. PAM solutions are designed to prevent breaches and limit ongoing damage linked to attacks in which privileges are used as the penetration tactic. Credentials, such as those given to administrators, are highly desirable to malicious actors who can leverage them throughout an organization. PAM security strategies and technologies monitor and control the activities of users with higher-level credentials than regular users. These tools can discover privileged accounts, manage passwords, monitor and track privileged access activities and block unauthorised access.

4. Implementing user-centric technologies such a User Activity Monitoring (UAM) and User Behaviour Analytics (UBA). A UAM software monitors what users are doing on endpoints such as how users are interacting with files, what application privileges the user has, and whether users have access to information they shouldn't. In addition, the UAM software will provide the security team with the context they need to investigate and respond to an incident through visual capture and session recordings. A UBA software utilises machine learning to create a behavioural profile for all users within the organisation. This allows security teams to discern between normal user behaviour and abnormal user behaviour, with any abnormal and risky behaviour being flagged, triggering an alert for the security team. In summary, both UBA and UAM are software created to correctly detect user behaviour that deviates from the company's security policies.

5. Bringing it all together with a modern/next-gen dedicated Insider Threat Management (ITM) software. With companies becoming increasingly aware and concerned by the threats posed by insiders, the industry has responded by developing more advanced ITM technologies to augment the existing security tools and software detailed above. These technologies are still in its infancy with very few players in the market, but the future looks extremely promising as companies continue to invest in ITM technologies. What makes these advanced ITM technologies so appealing in addressing the insider threat problem is that it combines both the data-centric and user-centric approaches in a unified stand-alone technology. This provides you with a holistic risk profile, providing the security team with actionable insights and relevant context to address potential insider threats in near real-time. When evaluating an advanced ITM technology or solution look for the following capabilities:
   - Provide alerts on anomalous user behaviour and policy violations to identify changes in a user's risk profile without constant calibration of privileged access controls.
   - Provide the ability to correlate file, user, and data activity. It should facilitate real-time data exfiltration alerts for quick action and resolution.
   - Combine and correlate both user and data in context, to create a clear picture of events before, during, and after an incident.
   - Make sure the solution has a negligible impact on the end users as it should never hinder productivity as this could lead to users exploring workarounds.