Cyberwatch Finland

WEEKLY REVIEW

WEEK 1/2024

”CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS”

Cyberwatch Finland

KEY TAKEAWAYS

1. The concept of insider threat is broad and includes both intentional and unintentional actions.

2. There are plenty of examples of various insider threats that have realised. When examining cases, intentional damage appears to be more common than intentional damage.

3. The insider threat cannot be completely eliminated, but there are ways to reduce the risk.

Cyberwatch Finland

INSIDER THREATS

Insider threat is a common and troublesome cyber threat. Some kind of insider component is involved in most cyberattacks, either as an enabling component or as a direct trigger. Indeed, insider threats are often at the top of the list of cyber threats in all organizations, regardless of industry and size. An insider threat can both lead to situations where data is wiped or an organization is exposed to external attack and materialize into actions where employees act deliberately against their own employer. In this review, these difficult to detect and often serious forms of threat are discussed from different perspectives. First, the aim is to describe what is meant by insider threat and how the threat from within can be materialize. This is followed by a few examples of the types of incidents that have resulted when an insider threat has realized. The aim is to produce an understanding of how extensive the threat field is. Finally, the challenges of preparing for threats and how organisations can seek to detect and prevent insider threats to themselves are discussed.

DEFINITION OF THE THREAT

Insider threat is a very commonly used term, but at the same time quite diverse by definition. It can refer to risks of very different causes and severity. In order to avoid conceptual ambiguity, it is important to understand the different ways in which an insider threat can materialise. Naturally, insider threats are discussed in much more than just the context of cybersecurity, but it is in cyber events that insiders play a particularly important role. In practice, an insider can refer to any person who has authorised access to an organisation's data or premises and who has been granted these rights, whether it is a current or former employee, subcontractor or service provider. Although the definition is usually associated with the concept of permissibility, it is typical that when an insider threat materialises, the perpetrator of the threat has gained access to material to which he or she has no legitimate access or which he or she should not have handled. Indeed, authorisation relates to general access to an organisation's premises, data or systems, and aims to distinguish internal actors from external ones, as prevention measures are very different. There is a significant difference between trying to access sensitive material from outside or from within the organization, where the actor has already bypassed many controls through their position or role.

Since the insider threat is relevant and applies to every organization, it has also been analyzed and studied extensively. The different forms of threat have been divided according to, for example, causes, objectives or intentionality. Although it does not really matter from the point of view of an organization seeking protection how the threat can be approached in all different ways, it is essential to understand different factors forming insider threats.

The most common form of approaching the phenomenon is the division of insiders into those who act intentionally and unintentionally. Of these, the former often receive more attention. This is simply due to the greater media attention they receive and the fact that intentional acts are more serious. However, it can rightly be argued that the number of insider threats arising from unintentional actions is significantly higher, and the damage they cause is also significant. Unintentional action can mean damage caused by a simple accident, but also an error due to inadequate training or understanding that compromises the organization's cyber security. This may be, for example, a lack of understanding of how the systems work or what is required to operate them safely. At worst, this type of activity can be repetitive or even routine, and it won't be noticed or to intervened until the worst has happened. In addition to action, threatening behaviour can also be a lack of action if, for example, safety protocols are neglected due to haste, laziness or indifference.

The actions of an intentional insider may include, for example, leaking information, infecting an organization's networks with malware, enabling an external attack, or revealing details related to the firewall of systems or the operation of protections. In addition, there are not always traces of operations, and especially in the case of long-term insiders, it is typical that they know how to cover their own tracks effectively. At worst, it is possible that, on retrospect, insider help in cyber events is not even detected, or at least cannot be ascertained with certainty. The concept of intentional insider can be further divided into those who act alone and those that receive external support. However, it is essential to try to understand why an insider acts consciously and willingly against their own organization. Typically, it is the sum of more than one factor, but common motives are dissatisfaction with the employer, financial gain, feeling marginalized or mistreated, or bitterness stemming from other factors. An employee may end up doing harm to their employer completely on their own, for example by actively acquiring and selling encrypted material they have access to, without being requested to so by anyone outside the company. It is also possible that a member of the organisation is individually recruited or pressured to become an internal informant and mediator. This is less common, and the threat most often concerns high-profile companies or operators in sectors critical to society.

It is important to understand that the motive for betraying one's own organization can arise unexpectedly, and for example financial difficulties, that are behind the actions of many deliberate insiders are often something that the organisation cannot detect or know affecting their employees. In the end, the actual action can also be quick and seem minimal. Simply selling a password, inserting a flash drive into a work computer, or changing a certain firewall setting can be enough, and especially for externally motivated insiders, the seriousness of the act and the risk of getting caught are downplayed to the insider. In some cases, an insider may also believe that they can later correct their actions. Examples can also be found in cases where employees have ended up causing harm to their employer without any external motivation. Often this is just selling secrets, but there are also cases where an embittered employee has, for example, destroyed valuable data after dismissal or termination of employment.

The rarest form of intentional insider threat is the so-called "mole", i.e. a person who specifically infiltrates a specific target organisation, whose goal is to try to cause harm to the organization from the very beginning while avoiding being caught. When it comes to cybersecurity, however, the use of moles has been rare, at least so far. It is more likely that the mole will be recruited already from among the employees of the organization.

All in all, insider threat as a concept encompasses a considerable number of different threat scenarios. It is impossible to respond to all of them with the same measures, which is why it is essential to understand the diversity of the concept when preparing for risks. Every organization's risk profile is unique, but the threat posed by an unintentional insider in particular applies to everyone. It should not be forgotten that just as every organization is an attractive target from a cyberattacker's point of view, and there is valuable blackmail in companies, libraries and government organizations alike, an individual employee can also understand how valuable information they are working with and end up on dark web forums looking for buyers interested in their access rights.

Cyberwatch Finland

CASE EXAMPLES

Insider threats often become reality and have been a major factor behind several recent cyber security incidents. Unintentional insider threats are significantly more common than intentional ones. Recently, Finland's largest bank reported that customers' personal data had been leaked after an individual employee's Office 365 credentials were leaked to a threat actor as a result of phishing. As a result, the attacker gained access to the employee's email folder, which included company's internal emails and critical information about customers. The leaked information included customers' names and social security numbers, which could lead to an increased risk of becoming a victim of identity theft. Another example of an unintentional insider threat can be found in August 2023, when the Police Service of Northern Ireland accidentally published information online about the employment status of its employees and other personal data online, posing a security threat to employees. One of the police officers stated that he had protected his privacy for several years by giving up hobbies and using social media, among other things, but all the effort was wasted because of one wrong click. Another example comes from U.S. military biometrics devices that ended up being resold in 2022. Research on devices revealed fingerprints, photos and other personal information of more than 2600 people. The cleaning of the equipment had been done inadequately or not at all. In all of the above cases, data was leaked due to unintentional human error, and it's no wonder that human activity remains the weakest link in the cybersecurity chain.

Intentional insiders pose a less common, but often more serious, threat than careless or poorly trained employees. A deliberate actor knows what he is doing and often also knows how to avoid being caught. An example of a deliberate insider threat is the so-called Vulkan Files case, which arose when a dissatisfied employee stole and handed over information to a German newspaper about a Russian company called NTC Vulkan. The employee's decision was based on the war started by Russia in Ukraine, which the individual opposed. The leaked information allowed the company to be linked to Russian security services and APT groups carrying out cyberattacks. One example of abuse of the authorised right of access can be found from Finland, where in the Finnish HUS hospital district, an employee is suspected of having inappropriately visited the health records of public figures, such as one of that times ministers of government. In the case of HUS, more than 1,000 patients have been affected and caused at least moderate reputational damage due to the excessive curiosity of one employee. A deliberate insider threat can also be motivated by financial reasons. In 2019, Trend Micro, a major cybersecurity firm, reported that an employee sold data from the company's customer database, leading to customized phishing calls to customers. Personal revenge can also be a motive. This was the case in 2021, when a former hospital employee in Georgia, USA, downloaded patient data to a USB stick. The incident was detected with the help of an up-to-date alarm system, and patient data was not known to be exploited. This, as well as the other examples mentioned above, shows that insider threats can materialise in several different ways. It may be mere unintentional negligence, employee curiosity, financial or political motives, or personal retaliation.

Cyberwatch Finland

HOW TO PREPARE FOR INSIDER THREATS?

Insider threats are difficult to avoid if the organization's supervision culture is not at an adequate level. In the case of deliberate conduct, insiders are usually well aware of how supervision is carried out and how to avoid it. On the other hand, unintentional activity that remains under control is detected and corrected. The challenge is how to detect harmful behaviour or planning of intentional misconduct in advance. However, it is possible to develop supervision when it is known what needs attention. For example, controlling and restricting access helps to prevent both accidental and intentional threats.

In addition to detecting a threat, it is also essential to try to prevent it as effectively as possible. Not all threats can be detected in advance. A good general guideline to avoid unintentional insider threats is to maintain a healthy cybersecurity culture. Investing in safety and safe behaviour must be made possible alongside other duties. Hurry should not be a reason for bad security behaviour. Cyber-secure operations should not only be a "theoretical" or "optimal" guideline that is not suitable for practical working life, but it should be a feasible strategy that does not create additional burden.

In all threat preparedness, one must remember that no organization will ever be able to fully protect itself from all threats. Accidents are inevitable and no amount of training or monitoring systems completely eliminate this risk. It is essential to prepare for and practice actions in the event of a risk realizing and try to limit how badly an accident can affect. Digital means alone are not enough to reduce the insider threat. Well-functioning HR processes, such as background checks, orientation and training, as well as effective access rights management, play a key role. More attention should also be paid to data classification and the tools used to process secret and confidential data. A well-functioning cyber security culture must be part of the overall security culture of the company and organization.

INSIDER THREAT PREVENTION MEASURES

Unintended threats

- Managing access rights
- Training staff and requiring the right action
- Maintaining a good information security culture, leading by example
- Operational control

Deliberate threats

- Managing access rights
    - Do employees have unnecessary access rights to systems that they do not need to perform their duties?
    - Do employees have access to more than just their own credentials? For example, sharing passwords among colleagues, or accounts of employees that have already left that are still active.
- Maintaining the physical security of IT assets and monitoring access to equipment
- Staying aware of one's own risk profile
    - Identifying valuable IT assets
    - Mapping access rights and limiting them to only what is necessary
    - Assessment of the amount of interest from the outside

INSIDER THREAT DETECTION METHODS

Unintended threats

- Monitoring and mapping security practices and culture
- Automated monitoring to detect abnormalities
- Introduction and accessibility of an internal reporting channel

Deliberate threats

- Employee monitoring, detection of suspicious behavior
  - Activities outside working hours, such as logging in to work systems in the evenings without a clear task or need
  - Significant change in employee behavior
  - "accidental" innocent security breaches, the purpose of which is actually to determine the level and scope of surveillance
  - Surprising/increased activity or applying for positions of responsibility
- Technical solutions, monitoring, tracking logins
  - Simultaneous use of multiple systems
  - Increasing visibility with the goal of making undetectable activity as difficult as possible

REFERENCES

https://cisomag.com/4-types-of-insiders-you-need-to-know/

https://jyx.jyu.fi/handle/123456789/86845?locale-attribute=fi

https://sports.yahoo.com/ex-hospital-worker-arrested-sgmc-001600795.html? guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAND4DpT83Jy7–S31z2BE-QfAPXaPrT4TIFrylelrU3jsNI5yN8UuB48D8iim3hw5eG-64NOvxSc12MZ0Qm7d1NqHbOUYvGX9dJxOkumTOx9fiY6oWyc8CtxdraPV-VoZy7KSiL3BsGil8rLfEvF-acxzBXp5DgDEDyGeDyKaBmWUb

https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches

https://www.hs.fi/politiikka/art-2000009563344.html

https://www.imperva.com/learn/application-security/insider-threats/

https://www.nytimes.com/2022/12/27/technology/for-sale-on-ebay-a-military-database-of-fingerprints-and-iris-scans.html

https://www.opentext.com/what-is/insider-threat

https://www.politico.eu/article/police-service-of-northern-ireland-mistakenly-releases-own-officers-personal-data/

https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236

https://www.zdnet.com/article/trend-micro-reveals-insider-threat-exposing-customer-data/

Pictures: Pixabay