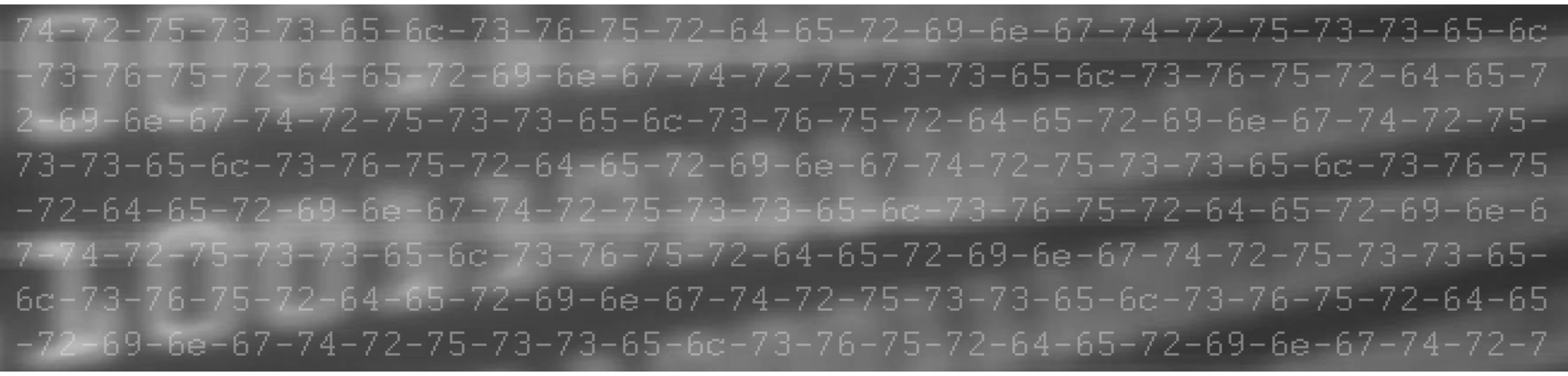
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat from intentional and unintentional insiders


74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c
-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-7
2-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-
73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75
-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-6
7-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-
6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65
-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-7

Threat Assessment Branch under the Centre for Cyber Security

February 2019

CENTRE FOR
CYBER SECURITY

Centre for Cyber Security
30 Kastellet
DK-2100 Copenhagen

Phone: +45 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. Ed.
19.02.2019

Threat assessment: The cyber threat from intentional and unintentional insiders

The purpose of this threat assessment is to inform public authorities and private companies of the threat from insiders with access to business critical IT systems. Careless, negligent or malicious employees may cause harmful compromises of data security in these organizations.

Key assessment

- No enterprise is immune to the unintentional insider threat, increasing their vulnerability to cyber threats.
- The Centre for Cyber Security (CFCS) and the Danish Security and Intelligence Service (PET) assess that unintentional insiders are responsible for approx. 50 per cent of security-related incidents in an organization.
- State-sponsored actors and cyber criminals exploit unintentional insiders in connection with cyber attacks against Danish organizations.
- Intentional insiders may exist in all organizations.
- The majority of malicious insider incidents are triggered by a dispute with the employer.
- Without the use of effective access management and logging mechanisms, it may prove impossible to identify an intentional insider.

Introduction

This assessment has been prepared in cooperation with PET and describes the insider threat. The main emphasis of this assessment is on insider incidents involving data and IT system breaches in public authorities and private companies, hereinafter called organizations. This assessment uses PET's definition of an insider as an individual with authorized access to an organization's network, who intentionally or unintentionally affects the operations by compromising, harming or changing information and processes that are fundamental to the existence of the organization.

The insider threat is particularly harmful to organizations that are vital to the functioning of society or to services that handle sensitive data or store valuable intellectual property.

There are two types of insiders: intentional and unintentional insiders. Unintentional insiders are employees who may inadvertently cause harm to the organization. Intentional insiders are employees who deliberately violate security policies for personal gain or with the intent to harm the organization.

The unintentional insider

All organizations are vulnerable to cyber attacks involving employees who may inadvertently violate information security. Just like vulnerabilities in, for instance, software, unintentional insiders may pose a threat to organizations. Consequently, organizations need to address the unintentional insider threat.

Museum victim of CEO fraud

In 2017, criminals defrauded the National Gallery of Denmark by luring employees into transferring a total of DKK 805,000 to overseas accounts by impersonating the museum's CEO.

Based on the ENISA Threat Landscape Report 2016 among other, the CFCS and PET assess it likely that unintentional insiders may be responsible for approx. 50 per cent of all registered security-related incidents in an organization.

The group of unintentional insiders includes employees who unwittingly violate the organization's security policies due to lax or insufficient security policy or training. For example, the unintentional insider may insert an unknown and thus potentially corrupted USB memory stick into their work computer or be tricked into sharing login information or other sensitive information by telephone or email to criminals posing as, for instance, an IT employee in the organization.

Cyber attacks via emails, so-called phishing or spear phishing, are a widely used technique to compromise an organization as it is relatively easy and effective. An unintentional insider may be tricked into clicking on a link to a fake website or opening a malware-infected attachment.

Phishing and spear phishing attacks

Phishing and spear phishing are social engineering techniques that involve fake emails sent to recipients in an attempt to lure them into conducting actions that may prove harmful to the recipient or the organization. Phishing includes fake emails sent to a large number of recipients, while spear phishing involves fake emails targeting carefully selected recipients. Spear phishing emails are fake emails that have been carefully tailored to individual recipients.

The CFCS and PET assess that both state-sponsored actors and cyber criminals often use phishing and spear phishing emails in connection with cyber attacks against Danish public authorities and private companies. The actors try to exploit service-minded and loyal employees by, for instance, posing as a client or an executive manager, thereby making the employee more likely to ignore warning signs or bypass security procedures. CEO fraud is a phishing technique where criminals will try to trick employees in an organization into transferring funds to the criminals' accounts by sending fraudulent emails and making fake phone calls. This type of scam may be very profitable and does not require sophisticated hacker skills.

Spear phishing attempt against Tryg thwarted

In March 2018, four key individuals employed by Danish insurance company Tryg received malware-infected spear phishing emails. It is likely that the aim was to gain access to financial statements before publication. Due to the vigilance of the employees, the fake emails were detected and the attack was thwarted just in time to prevent a potential compromise.

Social engineering

Social engineering is the art of psychological manipulation used by criminals to exploit an individual's habitual behaviour, trust in authority, curiosity, or helpfulness to disregard warning signs in emails, phone calls etc., and potentially tricking individuals into revealing confidential information or performing harmful activities. Spear phishing emails often appear to come from a person, organization, or authority that the recipient trusts or are designed to include links to projects, products, conferences, or documents that may be of interest to the end target.

LinkedIn is exploited for social engineering

In June 2017, the German Intelligence Service BfV warned about fake Chinese LinkedIn profiles disguised as researchers, think tank members, and consultants. These fake profiles targeted more than 10,000 German officials.

Social engineering requires that the criminal has a certain amount of information on the victim such as employer, colleagues, field of work, daily life, hobbies, or social network. This information may be found online, but may also be obtained by employing more aggressive tools such as trying to build a trusting relationship with the victim by pretending to have common personal and professional interests. Contact to the victim may be established at meetings and conferences or via social media such as LinkedIn and Facebook. A fraudster may find it appealing to target spear phishing emails at employees with decision making authority or IT system administrator rights. This type of information is often available on an organization's website or LinkedIn profile.

Negligent employees

Negligent employees, who fail to follow existing security procedures because they seem complicated or unnecessary, make up a particular group of unintentional insiders. The lack of or insufficient security procedures may be another reason for employee negligence. For instance, employees may share their password with colleagues, neglect to follow the organization's rules for designing safe passwords or transfer sensitive data via private email accounts or unsafe media, for instance, in order to work from home.

The lack of suitable in-house IT tools may force employees to use unsafe and unauthorized solutions such as downloading unapproved software or sharing in-house documents via Internet-based file sharing solutions outside the control of the organization. Employee negligence may also entail that IT systems are not installed and operated according to company security policies or best practice.

Employees struggling with a heavy workload may ignore security procedures that may delay their work further.

Physician mistakenly sent sensitive patient data to criminals

In 2016, a physician employed by the Danish Patient Safety Authority sent files containing patient data to his private email after having problems opening a number of files in a closed network. However, the physician typed in the wrong email address, sending the files to a mail server likely controlled by criminals.

Urgent and vital operating errors may force an employee to deliberately disregard existing security policies that would otherwise delay error recovery. For instance, an employee may borrow a colleague's password to access an operating system to correct an error. This may not necessarily be a serious breach, but may over time result in a poor security culture. Consequently, organizations need to consider whether security procedures should take this type of unforeseen circumstances into account.

The intentional insider

An intentional insider may cause substantial damage to an organization. Unlike outside hackers, who are often blocked by security measures such as firewalls, email scans and anti-virus filters, intentional insiders will often succeed in their efforts as the security mechanisms are not designed to prevent intrusions from insiders who do not necessarily use malware, but rather legitimate access privileges to carry out their plan.

Insider convicted of source code theft

In 2017, a former employee with IBM in China was convicted of copying IBM source codes. According to US authorities, the employee wanted to use the code to produce and sell software to customers.

The exact extent and number of security-related incidents caused by intentional insiders is uncertain, and the number of incidents is probably underreported. However, foreign security company reports indicate that many organizations are familiar with intentional insider incidents. A survey showed that almost 50 per cent of the surveyed organizations had had at least one incident in 2017. Based on public reports and incidents and compared to data from cooperation partners, the CFCS and PET assess that intentional insiders are a potential threat to any organization.

Employee sabotages Citibank routers

In 2016, a former US Citibank IT administrator was convicted of sabotaging the bank's routers. The incident was motivated by a conflict between the employee and the company executives.

It is impossible to prepare a general profile of an intentional insider. However, a survey by Carnegie Mellon University in the United States shows that 80 per cent of the intentional insider incidents are triggered by work-related issues such as staff cuts, transfers or disciplinary proceedings between the employee and the employer. A conflict may prompt the employee to harm the organization in order to achieve a measure of vindication. Other motives include financial gain, idealism or strong loyalty to nations, groups, or individuals outside the organization.

In connection with the use of subcontractors and outsourcing, an organization often has limited knowledge of or influence on a supplier's internal affairs. Thus, organizations should be aware that conflicts may erupt between subcontractors and their employees without the organization's knowledge, increasing the threat from intentional insiders in the supply chain with no or short notice.

State-sponsored actors recruit insiders

Certain states are actively seeking to recruit spies in Denmark, in part to support the country's economy by stealing intellectual property, in part to collect information of national strategic importance.

Also, in certain states the link between the intelligence service and the civil population is close and citizens and private companies may even be obligated under national law to support the country's intelligence service.

It may prove difficult to identify an intentional insider

A 2015 US survey showed that airtight identification of perpetrators was impossible in over 50 per cent of the registered insider incidents due to lack of or insufficient access management and logging mechanisms.

Effective access management limits the number of employees with access to sensitive systems and data, and logging mechanisms can reveal the identity of the person who has accessed business-critical systems and data at a specific time, as well as outline the employee's behaviour.

Malicious insiders are often involved in data theft. Insiders, who aim to compromise their current employer or secure leverage for themselves or a future employer, may steal sensitive information such as intellectual property, client documentation, or other corporate secrets and carry it with them to a new employer. Without effective logging mechanisms, it is difficult to detect unauthorized copying of data.

Insiders seeking financial gain or committing data theft under duress may copy sensitive data that could be sold or exploited for the purposes of financial crime. Insiders may also try to trick the employer into believing that the data has been stolen by cyber criminals and that it will not be released unless ransom is paid. Without network monitoring, access management, and logging systems, it is difficult to prove whether compromised data is illegally copied by an employee or stolen by external hackers.

Intentional insiders will often perform their activities using their inside knowledge of the organization and their IT access privileges. An IT administrator, who seeks revenge over his employer, may be particularly malicious. The insider may obtain access to sensitive data as well as change or disrupt business-critical IT systems, consequently jeopardizing the organization’s financial position and reputation. If logging systems are not protected, the insider will also be able to cover all traces of his activities.

System administrator convicted of hacking against former employer

Following his 2010 dismissal from the then US-owned Internet supplier PA Online, this former staff member tried to access the company’s network in an attempt to steal software that he believed he owned. His attempt resulted in system breakdown, disrupting the supplier’s clients Internet access for a week.

If employees have remote access to an organization’s IT systems, it may be impossible to control who is actually accessing the system or who is looking over the shoulder of the employee. Even the use of access management and logging mechanisms may make it impossible to detect the possibility of an employee allowing a third party to use his remote access to the organization’s IT systems.

Recommendations

The CFCS and PET recommend all public authorities and private companies address the insider threat and include this threat in their continuous risk assessments.

Even though unintentional insiders may exist in all organizations, it is important to recognize employees as a significant defence guard against the cyber threat that will only work, however, if the organization constantly motivates its employees to follow well-defined and comprehensible security procedures. The organization should also keep its employees updated about the methods used by threat actors as well as train them in spotting warning signs in, for instance, unexpected contacts, phone calls, emails, etc. Instead of blaming the employee that have fallen victim to phishing and social engineering, corporate executives should encourage transparency and openness about such incidents, allowing threat information sharing and improving employee security awareness and capability to detect the threat.

It would be profitable for organizations to examine the extent of damage a potential intentional insider in the organization may cause just by exploiting available processes and legitimate access to business-critical IT systems and data. The results of the investigation may prompt the organization to introduce or review security policies, processes, technical security mechanisms or employees' access to and roles in critical IT systems.

The number of employees with access to business-critical systems and data should be limited. The number of employees with administrative privileges, in particular, should be reduced to a minimum, which will also contribute to the protection against external hackers. In connection with termination of employment or transition to a new function, it is vital that unnecessary IT accesses are quickly cancelled and that possible joint administrative and root logins known by the employee are changed.

Some employees may take the view that anything that is not prohibited is permitted. Thus, it is important to establish clear rules stipulating what the employee is allowed to do, should do and what is forbidden. The rules must be recognized and enforced. Ultimately, insiders may be deterred by the realisation that their actions are against internal rules and procedures and may have ramifications.

The risk of exposure may deter intentional insiders from carrying out their schemes. Consequently, organizations that aim to mitigate the insider threat should ensure an effective access management and logging mechanism of business-critical IT systems – measures that also contribute to the protection of external cyber threats. Precautionary measures will only have an effect if the employees are made aware that their activities are registered and monitored. The constant awareness can be ensured by general information and by contacting employees personally even in case of minor incidents such as failed login or login outside regular office hours, incidents that may also indicate an external cyber attack.

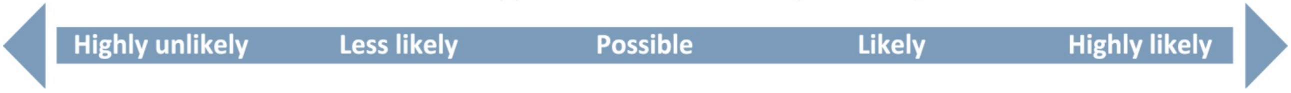
Also, it is important to be aware of potential in-house conflicts with employees and ensure they are addressed and handled appropriately, as well as remain attentive to issues that may potentially spark a conflict.

The CFCS has prepared a number of guidelines that are also relevant to the insider threat:

- Effective cyber defence measures
- Spear phishing – a growing problem
- Logging – part of an effective cyber defence

Furthermore, PET offers courses on the insider threat. Course information is available on PET's website at www.pet.dk.

The DDIS applies the below scale of probability


Highly unlikely
Less likely
Possible
Likely
Highly likely