Article

Cybersecurity—The present situation and future challenges

A crisis creates unexpected challenges. In this article, we will examine the present situation and the pandemic's effect on cybersecurity in Sweden and internationally. We will also look ahead and try to outline future challenges in protecting critical systems and sensitive information.

The challenges of the pandemic have been different for different types of operations, authorities and other organizations. Some have had to pivot in order to survive, while others have gotten more work than they can handle. The report Cybersecurity in Sweden—in the shadow of a pandemic (Cybersäkerhet i Sverige – i skuggan av en pandemi), published by the Swedish Civil Contingencies Agency (MSB), describes how operations in Sweden have managed this transition from a cybersecurity perspective. In the same way that many operations have been forced to change their actions and methods in the wake of the pandemic, attackers have likewise adapted their methods of attack to respond to the new situation in society. According to Sectra Communications Cybersecurity Expert Leif Nixon, cybersecurity must be a part of the entire organization as well as a continual and proactive effort.

"Since each individual employee is a potential path for attackers to enter an operation's network, cybersecurity efforts must be integrated into the entire organization. This applies to everything from securing technology to training employees and giving them the right tools so that they can work securely. The important thing is for everyone to be on board and that a continual and proactive effort takes place across all functions of the operation," says Leif Nixon, Cybersecurity Expert at Sectra Communications.

Hostile actors

Cyberattacks designed to carry out industrial espionage against Sweden are now something that happens constantly. According to the MSB report Cybersecurity in Sweden 2020—threats, methods, shortcomings and dependencies (Cybersäkerhet i Sverige 2020 – hot, metoder, brister och beroenden), there are multiple types of hostile actors with different agendas carrying out cyberattacks against Sweden. The majority of the attacks come from state actors and criminal groups, but groups with ideological incentives are also responsible for attacks. The state actors are ordinarily intelligence services that carry out attacks in their own country's interests. Criminals attack in order to make money, which often causes them to direct their attacks against operations with critical assets. Ideologically motivated actors consist of groups that act according to their own views of right and wrong, which are usually linked to factors such as politics, religious beliefs and human rights. The ideologically motivated groups have varying capabilities in terms of possessing the knowledge, means and assets to carry out advanced cyberattacks.

Conversion and methods of attack

Sweden and several other European countries are now high-tech countries that quickly adopted new information technology for citizen services to make them more convenient and accessible. This adoption comes with many benefits, but it also creates a dependence on having digital communications technology function without interruption.

This conversion has allowed the workplace to be moved from the office to the home for many people, including people who handle sensitive information, and the effect of this move has also shaped the attackers' approach. The growing use of remote login services has led to an increase in "password spraying attacks" with the objective of breaking into closed systems. This is a method of attack that has been known for a long time but continues to be used since it still works.

As a result of the rapid conversion to remote work, security efforts have been assigned a lower priority within some operations in order to get day-to-day communication working. In its report, the MSB provides examples of how many operations early on began using a small number of popular services

Password Spraying

Password spraying is based on testing simple and common passwords on numerous login accounts. This type of attack is often conducted over a longer period to avoid drawing the attention of the administrators monitoring the systems. The risks can largely be reduced through use of multi-factor authentication.

that claimed to have appropriate security features, claims that it turned out they couldn't live up to.

It's easier for an operation to control security when employees are at the office rather than when they connect to the office network from home. At the office there are tools such as network logs and more secure connections that minimizes the risk of infiltration of internal systems. Even business equipment can be exposed to attacks, especially if it is also used for private purposes. Damaging effects can either occur immediately or when they are later brought back to the regular workplace.

In recent years, there has been a global increase in attacks on critical infrastructure operations, both regarding private companies and authorities. The amount of attacks has increased and the average ransom requested for ransomware attacks has more than quadrupled in the last two years. In 2021, Colonial Pipeline, which owns the largest oil pipeline in the US, was subject to a ransomware cyberattack that cut off their deliveries for six days even though the company paid the requested ransom.

Ransomware

Ransomware, extortion software, is a method that is increasingly being used by attackers today. The method is based on encrypting data and essential information that an operation depends on to operate normally. The attackers then offer to restore access in exchange for a ransom and threaten to leak sensitive information to the public if the ransom is not paid. Today, ransomware is a multibillion-dollar industry around the world and is viewed in many countries as a matter of national security. Unfortunately, many parties that suffer an attack and agree to pay the ransom are usually attacked again sometime in the future.

Future challenges

The present situation has primarily been shaped by digitalization and technological advances, which have accelerated in recent years—accompanied by demands from an increasingly technically demanding environment. Today, the society depends on having digital solutions for applications such as production, information and communication function without interruption. It will become even more important for countries and government authorities to develop clear legal requirements and regulations that help operations protect sensitive information and infrastructure. As the number of hostile actors increases and the attacks get more advanced, it is vital for these operations to make it a priority to conduct methodical and continuous security risk management. In a changing world where both workplaces and communication technologies are evolving, security must be integrated with accessibility.

Cybersecurity is based on different capabilities—namely, detection and protection—that must be balanced to provide the most complete protection possible. It is not enough to focus on the protection capabilities and forget to integrate detection capabilities into the security work. According to the MSB report Cybersecurity in Sweden 2020—recommended security measures (Cybersäkerhet i Sverige 2020 – rekommenderade säkerhetsåtgärder), organizations within government authorities, municipalities and regions ought to introduce some type of function to detect cyberattacks. One recommended measure stated in the report is for organizations to implement a Security Operations Center (SOC). An SOC uses both automated and manual methods to analyze log data and monitor networks in order to detect anomalies in the system. If such a detection capability is not established, for example with an SOC, attackers may be able to hide their existence in critical systems, and undesirable activities may be able to take place without detection. In many cases, cyberattacks are not discovered until they have a tangible impact on day-to-day operations.

"It's actually not possible to completely predict what types of attacks we can expect in the future. On the other hand, we can guarantee that the number of cyberattacks will increase and operations must work according to the theory that it's a matter of when, not if, they will be hit by a cyberattack," says Leif Nixon, Cybersecurity Expert at Sectra Communications.

One of the major threats to future-proofing confidentiality for sensitive and classified information is quantum computers, advanced supercomputers that can perform certain types of calculations much more efficiently than today's computers and may therefore pose a threat to the encryption methods used today. In some organizations, current security solutions must be able to protect information for the next 30 to 40 years, which means that it's important for new security solutions to be built on quantum secure principles.

"It's very likely that hostile actors store encrypted information in the hope of being able to decrypt it in the future. The problem is that it's not always possible to determine what type of information the hostile actor might have successfully stored and it's therefore difficult to know what the consequences could be. The first thoughts go instinctively to information that must be kept confidential over a long period of time – but it could also be a potential goldmine for someone who's looking to carry out influence operations," says Niklas Johansson, Research Manager at Sectra Communications.

Five tips for working from home securely

Leif Nixon has five short and specific tips for operations to reduce security risks when people work from home:

1. Provide employees with secure connection via a secure and reliable virtual private network (VPN).
2. A secure collaboration tool should be used for daily communication. For both legal and security reasons, it's important to know not only in which physical location the information is saved and where the service infrastructure and hardware is located, but also where the service provider and its parent company is domiciled for legal purposes—which means that many cloud services cannot be considered secure as a result.
3. Operations can employ policies that limits which applications the user is allowed to download.
4. Train personnel on cybersecurity and provide clear information on the security risks that come with working remotely and what they should do to protect sensitive information.
5. Check and revise users' authorizations in the system and reduce the number of system administrator accounts. It's important to have some type of detection capability, for example an SOC that monitors and reacts to deviations in traffic.

References

Cybersäkerhet i Sverige 2021 – i skuggan av en pandemi

Cybersäkerhet i Sverige 2020 – hot,metoder, brister och beroenden

Cybersäkerhet i Sverige 2020 – rekommenderade säkerhetsåtgärder

This is a marketing material and may be changed at any time without prior notice.
Sectra will not be held liable for any errors or misconceptions herein.

Knowledge and passion