Monthly Review

Cybersecurity news from around the world

GENERAL CYBERSECURITY NEWS 2

ARTICLES

Legislation struggles to address ransomware 4

Enhancing security awareness with Mitre ATT&CK 8

KEY TAKEAWAYS 10

ARTICLE

Enhancing security awareness with Mitre ATT&CK

Read article →

SECTRA

General cybersecurity news

1 Cybersecurity of mobile payments

Payment methods have evolved over the years, with cash being replaced by credit cards, contactless payments, and now mobile payment options like MobilePay, Apple Pay, and Google Wallet. While some users may have concerns about the cybersecurity of mobile payments, they are actually more secure than traditional physical credit cards or contactless payments.

When paying with a smartphone, the transaction uses NFC technology, which is integrated with physical bank cards for contactless payments. NFC technology uses radio waves and doesn't require an internet connection from the smartphone. The network connection is only needed from the payment terminal to obtain approval from the credit card issuer. Mobile wallets like Apple Pay and Google Wallet don't store full card details on the device or their servers. Only a few numbers from the bank card are displayed in the mobile wallet app, reducing the risk if the device is lost. The card number, CVS, or PIN code used in mobile payments are never visible during the transaction, reducing the risk of someone snooping on the details. The security features on the phone, such as PIN codes or biometric identifiers, provide an extra layer of security compared to physical cards. Even if a criminal gets hold of a user's account information, they would still need additional card details and confirmation from the bank to make payments on a different device. Mobile payments are generally safer than physical cards, but it's important to take precautions to protect payment-related information and IDs stored on smartphones.

2 Industry collaboration urged following recent IT failure

Last month, an IT disaster caused by a faulty update of Crowdstrike's Falcon virus protection app affected 8.5 million Windows devices worldwide. The incident showed the widespread impact of global information security giants and raised questions about their responsibility. It highlighted the need for a backup plan in case of extensive downtime and the operating principles of Endpoint detection and response software. The incident may lead to improvements and collaboration in the industry, as well as the development of alternative solutions. Preparedness for future outages is crucial for organizations of all sizes.

3 Researchers discover HDMI cable exploit

Researchers from Uruguay have developed a method that allows hackers to spy on targets by exploiting electromagnetic leakage from HDMI cables. This leakage can be captured with an antenna several meters away, and using artificial intelligence, the researchers can reconstruct the signal into usable data. With a specialized antenna and deep learning AI, they were able to capture up to 70% of the original image quality on their own screen. This type of attack could potentially capture sensitive information like usernames, passwords, and business secrets. While this method has not been widely known or publicly used, researchers believe it may have been utilized by state-sponsored threat actors. Implementing this attack requires specialized equipment, knowledge, and relatively close access to the target device. Protecting against this threat involves combining physical and technical security measures, such as limiting access to target hardware and monitoring outside the organization's walls. It is also important to be aware that there are various forms of digital eavesdropping, highlighting the need for constant monitoring and active defense against emerging threats.

ARTICLE

Legislation struggles to address ransomware

Australia announced in early August that it is preparing a bill that would change organizations' reporting obligations after ransomware attacks. The proposal, which is still yet to be approved by Parliament, would add to the law an obligation to notify if an organization has decided to pay a ransom to the perpetrator of a ransomware attack.

Failure to comply with this obligation could result in a fine of AUD 15,000. The idea is not to prevent or prohibit the payment of the ransom, which is almost a U-turn from the plan to make it illegal just a year ago. Australia, which has long sought a solution to the ransomware problem plaguing the country, was long at the forefront of drafting laws to prohibit cooperation with extortionists. At the end of 2023, the idea, which faced significant opposition, was finally abandoned. The problem with making ransom payments illegal is that, instead of actually affecting the amount of ransom received by criminals, it increases the likelihood that the person who paid the ransom will make every effort to conceal what happened. This, in turn, directly benefits criminals – the less that attacks are talked about and knowledge about operations is known, the better the conditions for extortionists to operate. →

Australia's new approach is better in that it aims to raise awareness of the problem by encouraging organizations (albeit under penalty of a fine) to communicate openly about what has happened, even if the ransom is paid. Ransomware is a major problem in Australia, and according to research conducted by McGrathNicol Advisory, a consultancy that has been monitoring the situation for years, up to 56% of Australian companies have been hit by ransomware in the last five years. In successful attacks, about 73% of companies have ended up paying ransoms. The figures are alarmingly high. Of course, it is good to note that this is data collected by only one consulting firm, and that it is based on data collected from the companies themselves. When the interest may be to hide what happened at all costs, the reality may be something different or even worse. The figures are at most indicative. Surely one of the main reasons behind the current bill is to gain more visibility into the phenomenon by getting more information directly to the authorities from victim organizations.

"Up to 56% of Australian companies have been hit by ransomware in the last five years."

The new solution however, is not without any issues. It has already provoked opposition from Australian companies. The main concern regarding the reform is that reporting a successful attack would lead to scrutiny by the authorities. If reporting leads the authorities to conclude that the attack was made possible by a lack of data protection, the threat of a fine for non-reporting may be preferable to reputational damage and possible prosecution for data protection breaches. Australian authorities have also handed out a large number of fines for failing to comply with data security obligations, so the new law could put companies in a situation where they have to choose between two different threats of fines. An attempt has been made to respond to this with a statutory provision according to which the content of paid ransom reports is not shared between authorities or publicly. →

This would allow reports to be made safe from concern of reputational damage or prosecution. However, according to business representatives, this is no guarantee that there will be no difficulties, and immunity from prosecution for security breaches has been flashed for companies that report crimes. However, this idea was very quickly shot down, as it would directly encourage disregard for data protection when it would be possible to obtain protection against possible infringements by reporting that an attack had occurred.

Another concern relates to the size of companies that would be affected by the future law. Criticism has been levelled at the AUD 3,000,000 minimum annual turnover required by the reporting obligation. Representatives of the business world believe that this is too strict and imposes unnecessary obligations on small businesses. According to the lawmakers, the cap is appropriate and therefore the regulation applies to precisely those companies that are on the target list of attackers.

Legislation makes it very difficult to find a mutually satisfactory and workable solution to the ransomware problem. One problem is often that the politicians who make the laws are not experts in the field. In addition, the slow legislative process may change several times during the drafting phases, making it difficult for companies to prepare, especially if the process drags on over government terms. →

However, Australia has made it a critical goal to root out ransomware from companies in the country. The current idea of increasing visibility and better mapping the threat picture is a step in the right direction, although implementation may still have some complications. Open corporate communication is the only way to increase social understanding and thus protection against ransomware, and since the carrot for this seems to be impossible to find, Australia is now trying the stick.

Still, open and honest communication about cyberattacks that have occurred or ransoms paid should not be just an activity under threat of a fine. Companies should understand that, at best, transparency can mitigate the adverse effects of a successful attack, and silence only supports criminals' activities and increases the risk of further attacks. Open communication makes it possible to control the situation and gives an image of an honest and responsible actor. Covering it up by paying a ransom and discovering it later is an even more damaging blow to your reputation. Of course, open communication requires that data protection has been taken care of appropriately and that the company has up-to-date information on what was in each database that criminals have gotten hold of. On the other hand, there should be other motivators for their realization than facilitating communication.

Whether the rest of the world follows Australia's example will depend a lot on how well the bill is implemented and whether it affects companies' eagerness to announce ransom payments. Although it is still possible that the proposal would be blocked in Australia, this does not seem likely. If the new model works well, it is possible that it will also lead the way for legislation in Europe. ■

ARTICLE

Enhancing security awareness with Mitre ATT&CK

One way to gain understanding about cyberattacks can be done using so-called kill chains or attack models. Attack models refer to the process and its steps in which threat actors carry out cyberattacks.

Attack model thinking offers a structured and systematic way to examine, understand and prepare for cyber operations afterwards. Several models have been developed over the years and although there are similarities between the different models, there are also differences.

"The model developed by Mitre is possibly the most extensive and technically deepest attack model known."

Perhaps the most popular and currently well-known attack model is the Mitre ATT&CK attack model, developed by the non-profit US company MITRE Corporation. In Mitre's model, a cyberattack is divided into 14 parts, which include reconnaissance and the threat actor's final impact on the target system. In addition to the phases of attacks, the model breaks down the phases into parts according to technical functionalities. It shows what kind of technical measures could potentially be taken by the threat actor at each stage of the attack. The model developed by Mitre is possibly the most extensive and technically deepest attack model known. It is used, for example, in audits of IT systems and products, due to the comprehensive and detailed classification provided by the model. →

There are differences in the use of attack models, but their main purpose is to illustrate the flow and ontology of cyberattacks. Detailed and technical solutions such as the Mitre ATT&CK model is an excellent tool for technical experts who can get practical solutions and perspectives for developing information security of an organization. It also serves as a tool for information security audits. Due to its complexity, the model has only limited usefulness outside of technical experts.

As a counter-balance to Mitre, simpler models serve as good illustrations and discussion starters as part of the organization's strategy work or, for example, as training material for personnel. In any case, it is worthwhile to familiarize oneself with attack models, whether it is technical security personnel or other personnel. By knowing the attack models, the organization at least gains awareness of the typical practical ways of implementing cyber threats. At its best, knowledge of the models provides tools for developing cyber security at strategic, operational and tactical levels. ■

Key takeaways

1. Mobile payments are considered secure due to several factors, like NFC technology, limited card details storage and additional verification for payments on different devices.

2. The worldwide security disaster caused by a failed update of Crowdstrike's Falcon product raised global concerns.

3. Digital eavesdropping via HDMI cables is a new threat that has not previously been anticipated.

4. Australia proposes mandatory reporting of ransom payments after ransomware attacks for increased transparency.

5. Cyberattack models are used to illustrate the stages of cyberattacks. Understanding the models helps organizations prepare for potential threats.

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden, and operates through offices in Sweden, the Netherlands and Finland.

SECTRA