6 May 2025 | National Cyber Security Centre NCSC

Semi-Annual Report 2024/II (July – December)

Cybersecurity

Situation in Switzerland and internationally

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Defence,
Civil Protection and Sport DDPS
National Cyber Security Centre NCSC

Management summary

In its semi-annual report, the National Cyber Security Centre (NCSC) outlines the key incidents and developments in the context of cyberthreats targeted against Switzerland and internationally. The NCSC received 28,165 reports of cyberincidents in the second half of 2024. This is slightly lower than in the first half of 2024, but the figure rose by 13,574 to a total of 62,954 reports over 2024 as a whole. The fluctuations are mainly due to the large ripple effect of the phenomenon of fake threatening calls from authorities. The ratio between the number of reports received from private individuals and companies remains constant at 90% and 10% respectively. The categories of fraud, phishing and spam stay the most reported phenomena.

General public group most affected by fraud attempts

Fraud is consistently the most frequently reported phenomenon and accounts for two thirds of all reports in the second half of 2024 with 18,270 reports received. There were no spikes in reports of fake threatening calls from authorities in the second half of the year. This phenomenon was covered in detail in the first 2024 semi-annual report.[1] In contrast, the NCSC observed a tripling of reports received in the current reporting period for fraudulent lotteries. The subscription scams take advantage of legal grey areas, which fraudsters are increasingly exploiting deliberately due to a lack of effective countermeasures. On the corporate side, there was a sharp increase in reports of CEO fraud, with many victims being found in communes and churches in particular.

Overloads lead to disruptions, faulty updates result in outages

On 19 July 2024, the most far-reaching IT outage in history occurred. It was not a cyberattack, but a faulty software update from the cybersecurity provider CrowdStrike that rendered over 8.5 million Windows systems unusable – primarily those of large companies. In addition to the impact on organisations such as hospitals and businesses, the aviation sector in Switzerland and worldwide in particular was severely restricted for several hours.
Overload attacks on the websites of cantons and communes, but also on web services for financial services, restricted their availability for a period of time. Distributed denial of service[2] attacks (DDoS) are executed using distributed attack infrastructure – usually in the form of a botnet such as 'Gorilla'.[3]

Creative ways of distributing malware – ransomware puts companies at risk

Players and attack methods in the field of ransomware extortion are continually adapting to circumstances and remain the most relevant threat to companies. For example, cybercriminals in the 'Black Basta' group flood email accounts with spam messages and then offer help in resolving the problem via digital communication platforms, compromising the victims in the process.

---

1 See Semi-Annual Report 2024/1; ch. 5.

2 Attack on availability (DDoS) (ncsc.admin.ch)

3 See Brief technical analysis of the "Gorilla" botnet (ncsc.admin.ch)

The names of well-known Swiss companies such as health insurers and debt collection agencies have been misused to distribute malware to recipients of malicious emails in their name. On fake or compromised websites, visitors are tricked with fake CAPTCHAs into manually executing malware scripts thereby infecting their devices. Using QR codes on letters, cybercriminals attempted to trick recipients into installing an infected “Alertswiss” app on their Android mobile phones.

Phishers are looking for new bait and channels

Obtaining access data or financial information through phishing remains the second most frequently reported category. In addition to the familiar phishing emails, cybercriminals are increasingly trying to spread their fake requests via other channels. For example, alleged bank employees contact victims by telephone, or mobile messages are sent via the SMS successor Rich Communication Services (RCS)[4]. Classified ad portals offer scammers an easy opportunity to contact people and in the real world, QR codes are pasted over parking meters to divert payments from motorists.
Furthermore, the general public and organisations in Switzerland submitted 497,096 reports of suspicious websites via the ‘antiphishing.ch’ reporting platform in the second half of the year.[5] The NCSC was able to identify 9,311 clear phishing sites from these and initiate appropriate countermeasures.

Other phenomena

The amount of time that organisations have to fix vulnerabilities before they are exploited by attackers is becoming worryingly short. The exploitation of such vulnerabilities repeatedly leads to data leaks but is also used by state actors for espionage and, in rare cases, even for sabotage against industrial control systems. These global trends must be adequately addressed to protect against cyberthreats in Switzerland.

---

4 Rich Communication Services (wikipedia.org)

5 See also Anti-Phishing Report 2024 (ncsc.admin.ch)

Contents

Editorial

In 2024, the NCSC received a total of 62,954 reports, an increase of over 13,500 reports compared to the previous year. Even if not every report received corresponds to a successful cyberattack, the figure still impressively shows how much the threat situation in the digital world has increased. But it is not just cyberattacks that posed a threat to our IT infrastructure. Unsuccessful manipulation of our own IT infrastructure or the installation of faulty updates can also lead to massive problems, sometimes with global repercussions. An example of the far-reaching effects of such a mistake was impressively demonstrated on 19 July 2024, when a faulty security update of the Falcon protection module from the company CrowdStrike led to computer failures worldwide. According to estimates, around 8.5 million systems worldwide were no longer available on that day. The damage caused is estimated at several billion US dollars.

These events once again highlight what has long been recognised in specialist circles: technical measures alone are not enough. Although they are unavoidable, their effects are felt in the real world and must be accompanied by organisational measures. Only the combination of technical and organisational measures allows us to increase the resilience of our systems to the maximum and to be able to react quickly in an emergency.
Effective patch management is central to IT security. It ensures not only the secure operation of applications, but also their stability. A phased approach to patch management based on the criticality and exposure of systems is well worth considering. The trick is to find a balance between the necessary testing and the timely installation of updates.
Regular training of IT staff in responding to IT outages is equally important. Regular exercises help staff to act quickly and effectively in the event of an emergency because in the event of an incident every second counts.

This semi-annual report provides a comprehensive insight into the cybersecurity challenges facing Switzerland in the second half of 2024. In addition to the incidents mentioned above, it also covers topics such as DDoS attacks, cyberespionage and vulnerability management.
I hope that this semi-annual report provides you with many valuable insights and approaches to further improve the security of your IT infrastructure and enhance its resilience to attacks and outages.

Florian Schütz, Director of the National Cyber Security Centre

1 Cyberthreats in Switzerland – an overview

Knowledge of the threats in cyberspace is of central importance for securing communication and information technology in Switzerland and internationally. A significant proportion of threats originate from actors with different motives and capabilities. However, the incident of the faulty software update by the cybersecurity company CrowdStrike in July 2024 made it impressively clear that such processes must also be the focus of attention to ensure the proper functioning of critical infrastructures. Nevertheless, the classic threat phenomena are still central when assessing the cybersecurity situation, as threat actors are continuously optimising their methods and tactics. Current developments in this area include, for example, the targeted inclusion of local characteristics such as the Swiss German language, the increased exploitation of legal grey areas (see ch. 5) and publicly published information on the business hierarchy. As a result, cyberspace is a dynamic environment for both attackers and defenders. Cyberactors who are keen to experiment set new trends and create imitators if an approach proves to be effective.

The number of reports received in the second half of 2024 (28,165 reports) fell slightly compared to the first half of the year (34,789 reports) (see fig. 1). Despite this, a general annual increase of 13,574 reports to a total of 62,954[6] reports in 2024 can be noted. The increase is due in particular to the phenomenon of fake calls from authorities[7] (see fig. 2). Compared to the previous year with 7,193 reports, there was a significant increase to 21,903 reports in 2024. In contrast, there has been a significant decline in threats sent by email[8] in which the criminals accuse the victims of having committed a criminal offence in a similar way to the phone calls. In 2023, 10,120 reports of this phenomenon were registered with the NCSC, compared to just 3,825 in 2024. This illustrates the trend which has been observed for around four years that criminals are once again increasingly using the telephone as a distribution channel. Although the individual effort for the fraudsters is higher when making phone calls, they can respond better to the needs of the victims and immediately counteract any doubts that arise.
The NCSC observed a significant increase in reports of fraudulent lotteries[9] (3,509 reports), with the number tripling in 2024 compared to the previous year. In the second reporting period in particular, the number of reports rose from 744 in 2023 to 2,398 in 2024. In many cases, the names of well-known food or retail companies, electrical retailers or transport companies in Switzerland were misused.

The ratio of reports from the general public (90%) to those from companies, associations and authorities (10%) remains stable. In terms of the fraud offences most frequently reported by

---

6 The NCSC records all reports received in its statistics. These include general questions, information and reports that cannot be categorised. In 2024, there were 1,622 reports that could not be classified to a specific phenomenon or incident.

7 To examine the phenomenon of fake calls made on behalf of authorities in more depth, the NCSC has compiled a report which was published with the Semi-Annual Report 2024/1. Among other things, the report highlights developments relating to this phenomenon, various approaches and technologies used, and the national and international legal situation.

8 Fake threatening emails from authorities (ncsc.admin.ch)

9 Fraudulent lotteries (ncsc.admin.ch)

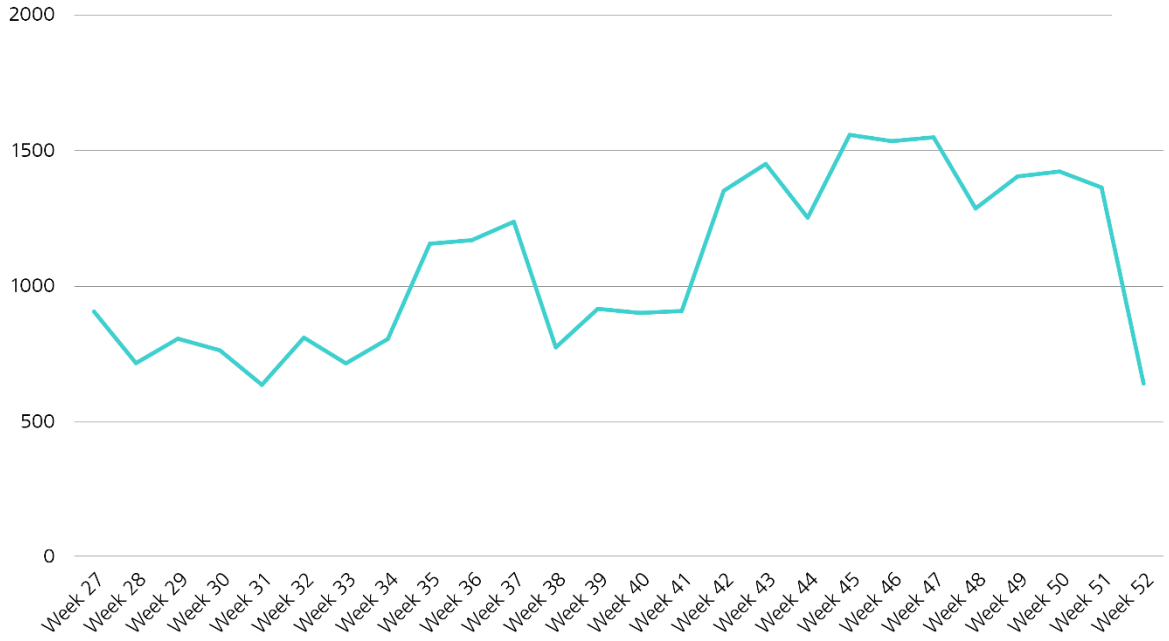

Fig. 1: Number of reports per week to the NCSC in the second half of 2024, cf. current figures (ncsc.admin.ch)

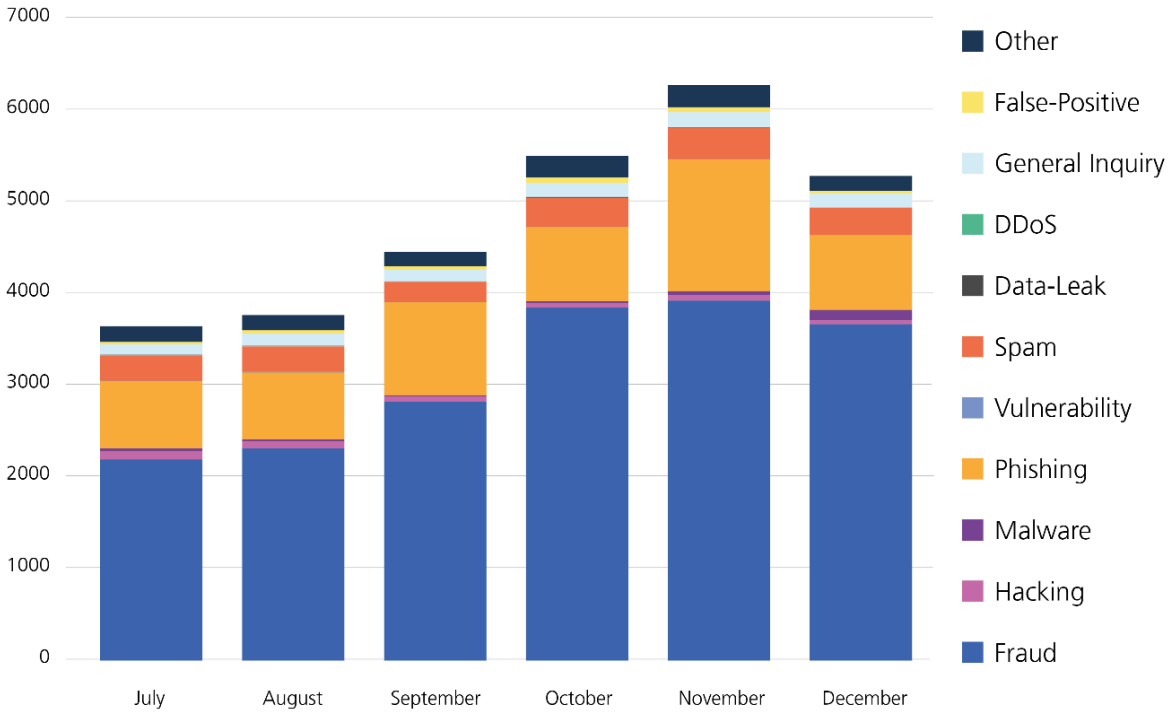

Fig. 2: Reports to the NCSC in the second half of 2024 by category, cf. current figures (ncsc.admin.ch)

companies, there was a significant increase in the phenomenon of CEO fraud[10] with 487 to 719 reports. In 2024, communes and churches were excessively affected by this phenomenon (see ch. 5.3). The slight downward trend in ransomware came to a halt. While 20 fewer incidents were reported in the first half of the year, the number of reports received in the second half of the year rose slightly by three to 48 incidents compared to the same period in the previous year. The NCSC received 92 reports of ransomware throughout the year. In general, however, the number of reported cases does not provide any indication of the extent of the damage. Ransomware groups are increasingly concentrating on lucrative targets, which means that the expected damage per incident is likely to increase in the future. In addition, ransomware attacks are now almost always accompanied by data leaks. This not only increases the damage for the affected companies but also augments the risk of knock-on effects for third parties whose information is found in the leaked data records.

The statistics underline that cybersecurity and the task of protecting Switzerland against cyber risks is a perpetual challenge for the businesses, the state and society. Accordingly, the semi-annual report presents the core phenomena that characterise the threat landscape in cyberspace for Switzerland and internationally. These include phishing[11], malware[12], vulnerabilities[13], fraud and social engineering[14], attacks on the availability of websites and other internet services (DDoS)[15] and disruptions to infrastructure, data leaks and cyberespionage and sabotage. The thematic chapters provide an overview of current features, interesting incidents and developments. The report derives recommendations for the public on how these challenges can be met in the spirit of personal responsibility for a more secure digital Switzerland.

2 Phishing

After fraud, phishing attempts are the second most frequently reported cyberincidents to the NCSC. These enable threat actors to collect access data, financial information and other confidential data from users without being noticed. Typically, users are manipulated (social engineering) without the use of malware.[16] While phishing for a large group of recipients via email is still the most common method, other approaches use voice (voice phishing or vishing) or SMS (smishing) to obtain sensitive information.

In 2024, 12,038 incidents were reported to the NCSC, which corresponds to an increase of 2,623 incidents compared to the previous year. Nevertheless, it can be seen that the number of reports received has stabilised at a level of 5,395 since the second half of the year. The phishing statistics show a different picture when viewed from the perspective of the phishing

10 CEO fraud (ncsc.admin.ch)

11 Phishing, vishing, smishing (ncsc.admin.ch)

12 Malware (ncsc.admin.ch)

13 Vulnerability (ncsc.admin.ch)

14 Social engineering (ncsc.admin.ch)

15 DDoS attack - What next? (ncsc.admin.ch)

16 There is no single international definition of phishing, thus other definitions often include the distribution of malware, see Phishing (attack.mitre.org). However, the NCSC explicitly excludes this dimension in its applied definition.

URLs checked and confirmed[17] by the NCSC. A steady increase can be observed here, both annually[18] and every six months. In the second half of 2023, 5,242 unique phishing URLs were registered. In the same period in 2024, this number doubled to 9,355. The detailed weekly development is shown in figure 3. In order to make the phishing pages as trustworthy as possible, criminals use the names of well-known brands and companies to lure their victims to the phishing pages. In the reporting period, the financial sector was the most frequently misused for phishing, namely in 23% of cases. This was followed by postal services with 22%, public transport with 22%, the IT sector with 11% and the telecommunications sector with 8%. This ratio has remained relatively constant from month to month (see fig. 4).

In addition to the classic phishing attempts against financial service providers, phishing attempts continue to focus on fake parcel notifications and refund emails in the name of suppliers, SBB and SwissPass respectively, as well as various tax administrations. In this reporting period, phishers increasingly tailored their attacks to Switzerland, for example by sending phishing emails in the name of the AHV compensation fund.[19] Phishing attempts against Microsoft 365 accounts also continue to be observed. The currently widespread approach here involves a snowball-like distribution of phishing emails, known as chain phishing, in which phishing messages are immediately sent to all contacts in the entire address book once the email inbox has been compromised.

In addition to emails, phishing messages are also increasingly being sent via text message. In the second half of 2024, the NCSC also observed the use of the RCS system and iMessage by fraudsters. This is probably due to the fact that mobile phone operators Swisscom, Salt and Sunrise have been using an SMS filter since 2022 and can therefore stop fraudulent text messages more efficiently. By using RCS and iMessage, fraudsters can bypass these filters and continue to reach potential victims. As in many areas of cybersecurity, the back and forth between fraudsters and security service providers is also evident here.

While the sending of phishing emails and text messages is a mass business and only a small proportion of these attacks are successful, there have also been repeated attempts to target specific groups this year. These include telephone calls from people purporting to be from a bank's fraud department, phishing attempts against sellers on classified ad platforms or the pasting of QR codes on parking meters. These three methods are explained in more detail in the following chapters.

---

17 The NCSC receives reports of phishing not only through direct reports, but also through the antiphishing.ch platform, which provides additional sources of data. As a result, the figures presented here may differ from the number of direct phishing reports.

18 A detailed annual analysis of phishing in Switzerland is provided in the Anti-Phishing Report 2024.

19 Caution: Phishing emails in the name of the OASI (ncsc.admin.ch)

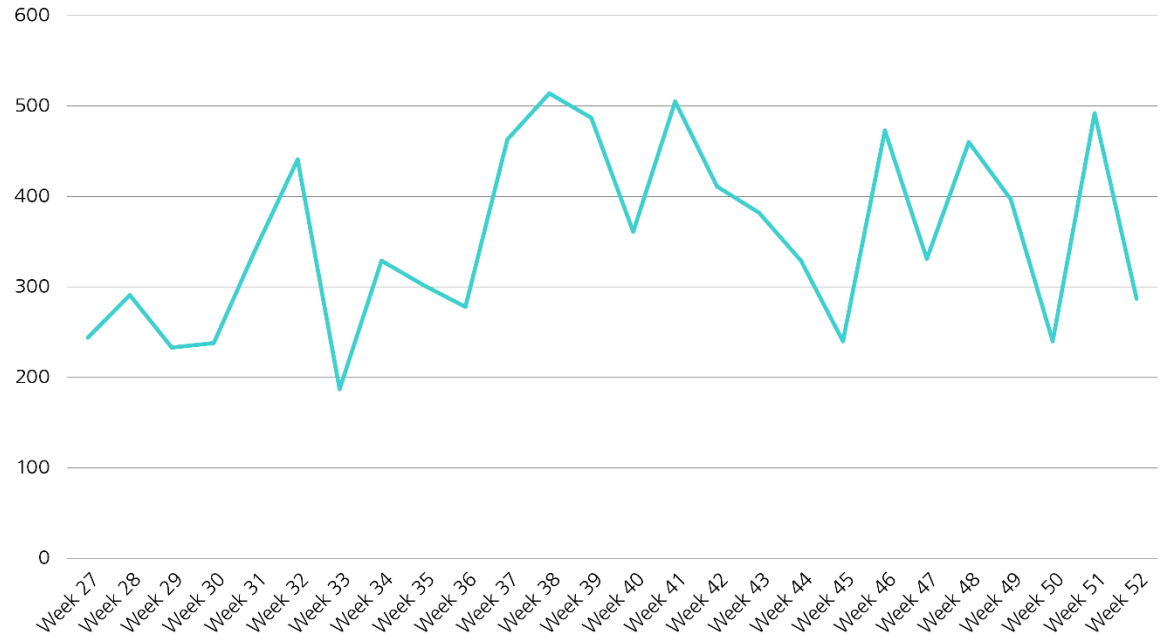

Fig. 3: Number of phishing URLs checked and confirmed by the NCSC per week in the second half of 2024

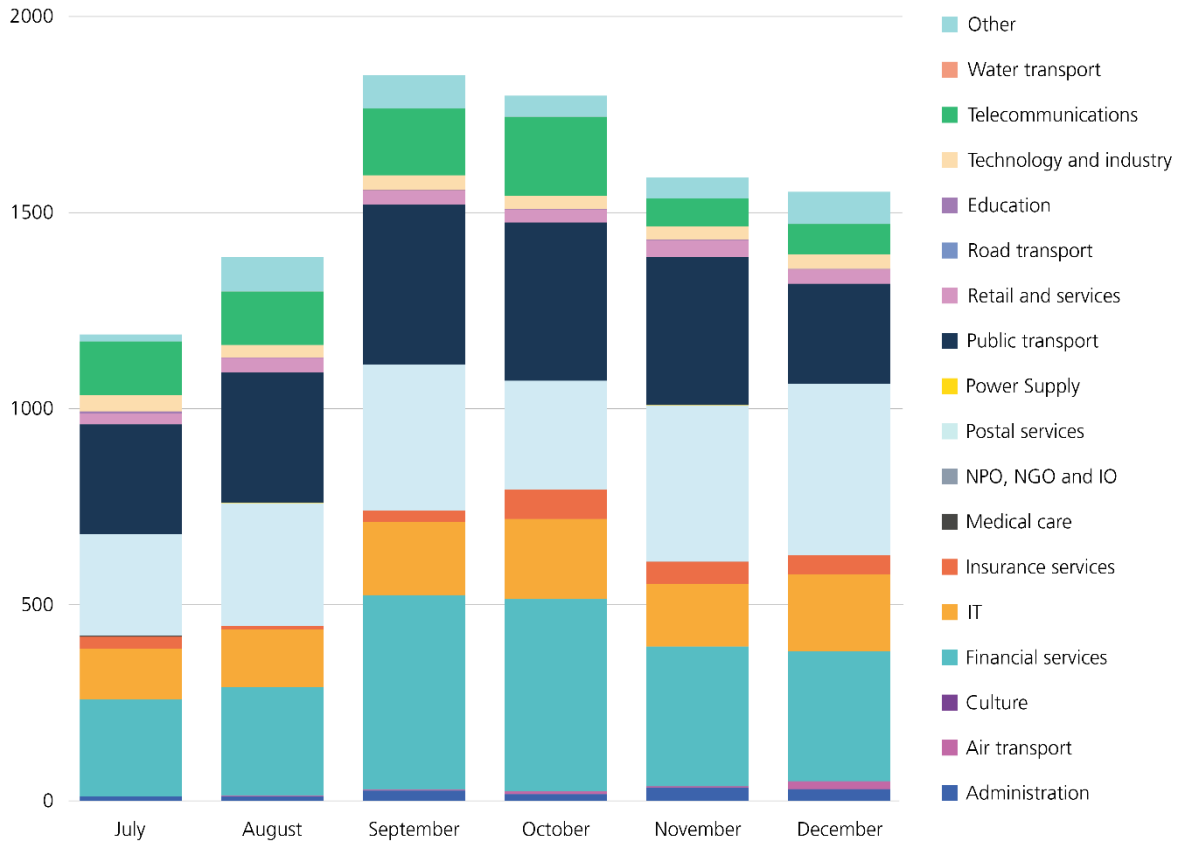

Fig. 4: Number of phishing URLs checked and confirmed by NCSC in the second half of 2024 by sector of misused brands

Recommendations

Report suspected phishing attempts to the NCSC via reports@antiphishing.ch or directly on the antiphishing website (antiphishing.ch). If you would like feedback, you can also report the phishing incident using the report form or by contacting our specialists at incidents@ncsc.ch. With your help, the NCSC can issue targeted warnings and take action to ensure that the websites are taken down.

2.1 Calls from alleged bank employees

Several phishing campaigns against customers of various Swiss banks were identified during the reporting period. The institutions in question included both regional banks and major banks. This campaign was characterised by a combination of different methods designed to appear credible to the victims. In addition to technical means, the criminals relied on social engineering, for example by pretending to be employees of payment portals such as PayPal, bank employees or police officers from the respective fraud departments.

Calls from alleged bank employees are nothing new. The Reporting and Analysis Centre for Information Assurance (MELANI) warned of such phishing attacks back in the 2010s. At the time, the callers pretended to have to carry out an e-banking update, which was then to be tested. The aim was to convince the victim to install remote access software in order to carry out an alleged e-banking update. The functionality of the system was then to be checked with a test payment. The victims later discovered that several thousand francs had been debited to the account of one of the fraudster's accomplices.[20] However, the NCSC has also repeatedly registered such calls in the recent past. Although the basic approach remained the same, the fraudsters have since adapted the pretext. In the current incidents, for example, the fraudsters pretend to be a 'Mr Fischer', who works in the bank's security department. The callers claim to want to stop a fraudulent payment. The telephone number displayed corresponds to the official number of the bank that the fraudsters claim to represent. However, the number is falsified by the fraudsters, also known as 'spoofing'[21]. While in some cases it is still claimed that there is a debit for a flat screen in an electronics store, the more recent cases usually involve an alleged fraudulent debit of CHF 800. The fraudsters advise the victims to call the fraud department of the cantonal police immediately. The number is provided by the attackers. To stop the fraudulent payment, the victim should also install remote access software on the computer and authorise access to both the computer and the bank account. Instead of stopping the payment, fraudulent payments are also triggered in this instance.

In other variants, in addition to the call, the victim received a text message with a four-digit code to be given to the alleged fraud department for verification. Here too, an alleged bank employee then called the victim to help with alleged problems with the e-banking portal. In addition to technical measures such as the use of spoofing, the accent-free Swiss German spoken by certain fraudsters increased the perceived credibility. As a result, victims, assuming they were talking to a bank employee on the phone, also divulged security tokens such as their

20 Social Engineering: Neue Angriffsmethode richtet sich gegen Firmen

21 Spoofing (ncsc.admin.ch)

two-factor authentication. With this element, the fraudsters gained access to the victims' e-banking.

The perpetrators use such methods to obtain the necessary access data in real time before it becomes invalid. If an application uses multi-factor authentication (MFA), this is necessary because the perpetrators can only log in at the exact moment when the victim discloses their own data. It is not possible to use the tapped data at a later time. This distinguishes such vishing attacks from classic phishing attacks, such as SwissPass phishing or, in some cases, credit card phishing, where the data can also be used at a later date. In these cases, a simple static phishing page is sufficient.

Recommendations

Enable multi-factor authentication (MFA) as additional security for your accounts wherever possible. Although MFA greatly reduces the risk of being compromised, it can be undermined by social engineering[22] techniques. So be wary of fake requests, especially via email and SMS if you are asked to confirm access or forward your security token to someone else. No Swiss bank will ask for such a security token over the phone to verify its customers. Also bear in mind that email sender IDs and phone numbers can easily be spoofed.

2.2 Phishing for classified ads

Classified ads offer fraudsters a multitude of opportunities for attack. The classic variants include the sale of non-existent goods or the non-payment of purchased goods that have already been dispatched. In addition, phishing variants targeting sellers have now become established. The fraudsters feign interest in a product and urge the victim to make the delivery and transfer the money via a parcel delivery service defined by the alleged buyer. If the victim agrees to this, the alleged parcel delivery service demands fictitious fees, which the victim is then asked to pay by credit card. In these cases, the attackers are primarily after credit card details. However, in some cases reported to the NCSC, attempts were also made to create a Twint account with the victim's phone number. The victims were first asked for their phone number and account number. A Twint account was then registered using this information. The victim was then asked to submit the Twint security code via a website to confirm that the phone number actually belonged to the person who wanted to open the account.

In contrast to the unspecific phishing emails sent out in large numbers, where the senders hope that the generic text will catch on with the victims, in the current cases the phishers go to great lengths and communicate directly and individually with the victim, adapting their scenario to the respective circumstances. In connection with these phishing attempts, attempts are also repeatedly being made in Swiss German.

22 Social engineering (ncsc.admin.ch)

Recommendations

Be careful with demands from buyers. Insist that shipping and transaction fees are paid by the buyer. Write this explicitly in the advertisement.

2.3 Parking fee phishing with fake QR codes

Online payment options for parking are becoming increasingly popular. Modern payment solutions enable drivers to pay their parking fees quickly and efficiently via various platforms such as apps on mobile devices, websites or special parking meters. Most of them use QR codes for a user-friendly payment process.

However, this simplification also harbours risks. In various Swiss cities during the reporting period, fraudsters repeatedly covered the real QR codes in car parks with manipulated codes, which then directed the victims to a false but deceptively real-looking payment website. The victim could choose between paying by Twint or a credit card.

Fig. 5: Fake QR code sticker on a parking meter

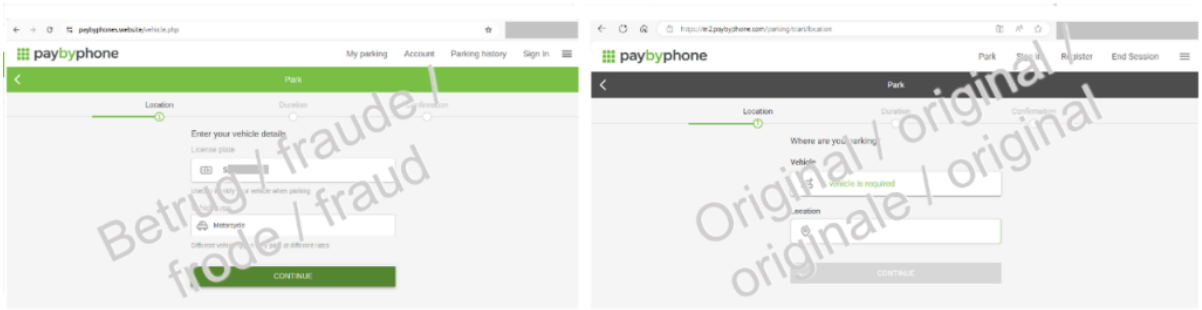

Fig. 6: Deceptively genuine scam website (left). Only the web address reveals that this is not the real site.

As victims are usually in a rush when parking, payment details, such as the amount debited or the recipient, are rarely checked. The payment is authorised and several hundred francs are quickly transferred to a fraudulent account.

In contrast to classic phishing methods, the fraudster or their accomplice must be on site to apply the stickers. In doing so, they run the risk of being caught. It is astonishing that multiple attempts were carried out. After the fraud attempts were noticed and the stickers removed, in some cases the fraudsters wasted no time in applying new stickers.

Recommendations

Look at or touch a physical, public QR code before scanning it to make sure it is not a false sticker. Make sure that the web address (URL) called up corresponds to the expected address. Take a close look. The differences can be very small. Be sure to cancel the payment process if you notice anything out of the ordinary.

3 Malware

Malicious software or malware continues to be a main tool used by cybercriminals to gain access on a device or a network. The following subchapter deals with the use of malware to initially infect systems. Attempts to distribute malware in the name of Swiss health insurers and debt collection companies were conspicuous. The NCSC also observed new methods that use fake CAPTCHAs[23] to trick potential targets into infecting themselves by executing malicious program code. For the majority of companies, ransomware remains the biggest threat at present. The second subchapter highlights incidents in Switzerland and relevant developments relating to this phenomenon. Finally, the third subchapter describes a campaign that uses QR codes in written correspondence in an attempt to persuade recipients to install an Android app infected with malware.

3.1 Initial access with malware

Cybercriminals often use malware as a gateway to compromise computer systems. In many cases, these attacks are accompanied by social engineering methods. This approach is intended to entice users to perform certain actions, such as executing the malware mentioned above. The most important trends regarding initial access with malware and the accompanying social engineering methods for the second half of 2024 are highlighted below, with a focus on developments in Switzerland.

During the reporting period, there were numerous attempts to infect systems with malware such as 'Agent Tesla', 'SnakeKeyLogger', 'Formbook', 'Lumma Stealer', 'Vidar Stealer', 'Strela Stealer' and the mobile malware 'Coper/Octo2'. It was found that the majority of these distribution campaigns lacked specific characteristics for Switzerland. The approach adopted was consistent with the international norm. This suggests an opportunistic approach on the part of the criminals, who want to infect systems without specifically selecting them beforehand. However, two campaigns that took place in November 2024 were specific to Switzerland. Firstly, there was a distribution of the mobile malware Coper/Octo2 by physical mail with a link to the malware, whereby the corporate identity of MeteoSwiss was misused (see ch. 3.3). Secondly, there was an email campaign in which the corporate identity of various Swiss companies was misused to spread Lumma Stealer.

[23] CATPCHAs are a prompt on internet forms where users have to confirm that they are human and not a machine. This includes, for example, an arithmetic problem or the task to select all pictures where animals, cars, bridges etc. are depicted.

The NCSC received numerous reports of suspicious emails allegedly sent by a Swiss debt collection agency or a Swiss health insurance company. These messages refer to a fictitious credit note or payment reminder and ask the recipient to click on a link to view the invoice. Clicking on the link downloads a malicious shortcut file which, when executed on a Windows system, triggers a script. This script launches an initial loader, which is referred to by various IT security companies as 'Emmenhtal'[24] or 'PEAKLIGHT'[25]. Subsequently, an information theft Trojan (infostealer) of the type Lumma Stealer is installed. The program collects and sends sensitive information such as login data, browser cookies or even wallets for cryptocurrencies.[26]

In addition, other Lumma Stealer distribution campaigns were observed in Switzerland, but these were carried out using the usual international methods. One of these methods, known as 'ClickFix', has been increasingly observed recently. Users are fooled by a fake CAPTCHA, which is actually used to differentiate between real and automated users. By clicking the 'I am not a robot' button, the malicious code is copied to the clipboard and the website prompts victims to press the key combinations 'Windows + R', 'Ctrl + V' and 'Enter' to complete the verification process.[27] In reality, however, this action leads to the execution of a malicious script and the installation of the malware. This method of users unwittingly executing malicious code appears to be very effective, as many variations have been observed distributing different types of malware. For example, YouTube channels have either been compromised or created specifically to publish fraudulent instructions to trick users into executing malicious code. The claim that this code is the solution to a specific issue, such as cryptocurrencies, software licensing or computer problems, is used as a pretext.[28]

Another notable case in Switzerland concerned a developer who was contacted via LinkedIn. Under the pretext of a job offer, he was tricked into downloading and running software that was actually malware. Here the aim was to steal data relating to cryptocurrencies. Internationally, several security service providers have reported similar campaigns. This case may be part of an international campaign called 'Contagious Interview', which specifically targeted IT developers via LinkedIn and aimed to trick them into running malware during the application process.[29] This was done by hiding the malicious code in a program that was to be debugged or in an installer for video conferencing software that was needed for the interview. In addition, in a related campaign, attackers managed to distribute infected copies of legitimate software packages on the NPM (node package manager) platform. NPM is a platform that allows programmers to share libraries or packages that are then used to develop programs. The attackers exploit the trust in such platforms by publishing deceptively genuine copies with similar-sounding names.[30] In one particularly sophisticated case at the end of the year, the attackers

---

24 Emmenhtal: A little-known loader distributing commodity infostealers worldwide (orangecyberdefense.com)

25 PEAKLIGHT: Decoding the Stealthy Memory-Only Malware (google.com)

26 Caution: Emails with malware in the name of debt collection agencies and health insurance companies (ncsc.admin.ch)

27 How attackers try to distribute malware with fraudulent CAPTCHAs (ncsc.admin.ch)

28 Your Data Is Under New Lummanagement: The Rise of LummaStealer (cybereason.com)

29 Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers (paloaltonetworks.com)

30 Tenacious Pungsan: A DPRK threat actor linked to Contagious Interview (datadoghq.com)

even managed to inject malicious code into updates of two original packages, infecting systems that had installed the compromised version of these packages with the crypto-mining software 'XMRig'.[31]

These cases are just a small selection of the diverse malware programs and attack methods used by cybercriminals. To be profitable, these criminals need to generate a return, which in simple terms consists of two variables: the required investment and the expected profit. So far, the development of artificial intelligence (AI) has not had a disruptive impact on the development of these threats. However, criminals are increasingly integrating AI to optimise specific tasks and compensate for existing deficits, which can reduce the required effort.[32] The increasing spread of cryptocurrencies and their storage on private devices increases the profitability of such attacks. It can therefore be assumed that such threats will remain an effective means of attack in the future.

Recommendations

Do not open attachments or click on links in suspicious emails and do not scan any QR codes. If in doubt, contact the purported sender via another channel to verify that the email is really from them.

When looking for software on the internet, make sure you are on the manufacturer's website or another trusted website (such as a well-known computer magazine) before downloading. Especially when using search engines, be aware of whether or not the website you are viewing is declared as paid advertising. If it is paid advertising, caution is advised, as attackers often use this method to be placed at the top of the search results.

Always be careful when a download window opens.

If possible, always let programs update themselves automatically. Otherwise, use the built-in update function or download the latest version directly from the manufacturer.

Do not connect any unknown or found USB devices to your computer.

3.2 Ransomware

This subchapter presents the current situation regarding ransomware. In this type of attack, cybercriminals use malware to encrypt data on the victim's IT systems, rendering it unusable for the victim.[33] The criminals usually exfiltrate the data at the same time. They then demand that the victim pays a ransom for a decryption tool and for not distributing the stolen data. The following examines the situation in Switzerland, then the incidents and trends at international level.

3.2.1 Ransomware activities in Switzerland

Following the targeted smashing of large ransomware groups such as 'LockBit' and 'ALPHV' in the first half-year of 2024, some developers and affiliates of ransomware groups had to look

[31] Supply Chain Attack on Rspack npm Packages Injects Cryptojacking Malware (socket.dev)

[32] See Semi-Annual Report 2024/1; ch. 5.1.

[33] Ransomware (ncsc.admin.ch)

for new alliances. This led to increased competition as other ransomware groups – such as 'RansomHub'[34], 'Akira', 'BlackCat' and 'Play'[35] – tried to entice these experienced operators to work with them by offering more attractive working conditions. As the following section on incidents in Switzerland shows, some well-known ransomware names such as Akira, LockBit and 'INC Ransom' are also at the top of the list of Swiss incidents.

The slight downward trend in ransomware of recent years has ended statistically. While 20 fewer incidents were reported in the first half of the year, the number of reports received in the second half of the year increased slightly by three cases compared to the same period in the previous year (48). Accordingly, the number of reports in 2024 as a whole fell by 17 reports compared to the previous year, from 109 to 92 incidents. The trend of ransomware primarily being targeted at companies is generally stable.[36] Ransomware incidents against private individuals, especially against their NAS devices, have fallen significantly in the second half of the year. Only eight incidents affected private individuals.

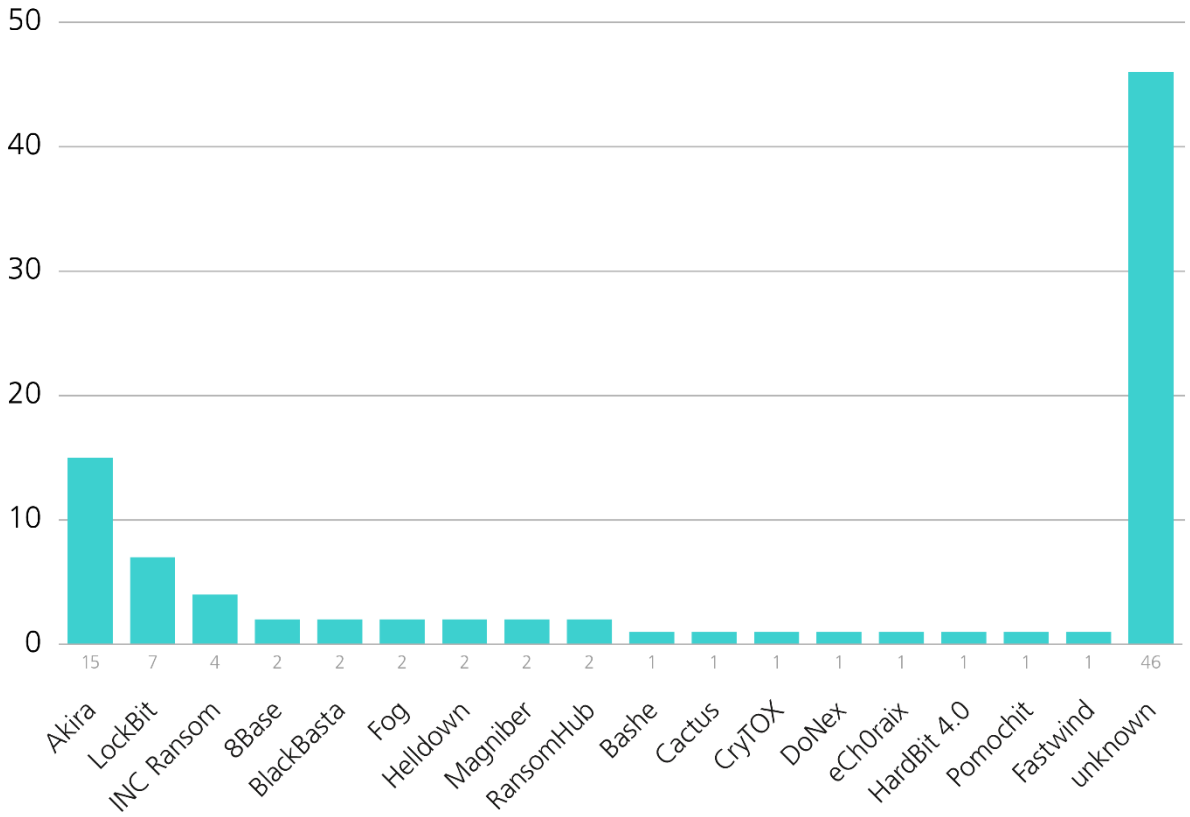

Fig. 7: Number of ransomware incidents reported to the NCSC in the second half of 2024

Looking at the most frequently reported ransomware groups (see fig. 7), Akira stands out in particular, with 15 cases, more than twice as many as the second most frequent ransomware variant LockBit. Akira is characterised by an opportunistic attack behaviour which was already

[34] RansomHub Overtakes LockBit as Most Prolific Ransomware Group (infosecurity-magazine.com)

[35] Play & LockBit Ransomware Join Hands to Launch Cyber Attacks (gbhackers.com)

[36] See Semi-Annual Report 2024/1; conclusion in ch. 3.2.1.

observable in the first half of 2024. This resulted in a relatively high number of victims that includes different sectors and company sizes. In contrast, LockBit was slowed down by the 'Cronos' police operation in February 2024 but still belongs to the most frequently reported ransomware variants in Switzerland. During the police operation, law enforcement agencies seized and destroyed LockBit's infrastructure, fragmented the network of those involved, and made decryption tools available to victims free of charge. Nevertheless, the ransomware activity remains at a stable level, as underscored by the LockBit group with an announcement of a new version – 'LockBit 4.0' – scheduled for February 2025 in December 2024.[37]
Ransomware INC Ransom follows in third place with four reported cases. The rest of the field is spread across 14 different ransomware families. In addition to a few large ones, the threat activity is spread across many different groups. Thus, many ransomware operations have evolved into a more modular and decentralised approach. Large ransomware groups have given way to many small groups in which ransomware attackers work alternately or simultaneously for several different operations.[38]

New ransomware variant

The new ransomware families observed by the NCSC in Switzerland include: 'RansomHub', 'INC Ransom', 'Fog', 'Helldown', 'Pomochit' and 'Cicada'.[39] Although these ransomware variants are considered new, they often show similarities to already existing malware, as it is the case with Cicada.[40] In the case of Helldown that emerged by the end of the summer, the group with the same name attacked a Swiss IT service provider and accessed 67 GB of data.[41] Helldown is still little known and mostly exploited vulnerabilities to infiltrate victims' networks and install the ransomware, which is partly derived from the code of 'LockBit 3.0'. The group first became known after the widespread exploitation of a vulnerability in Zyxel products.[42]
RansomHub is a ransomware-as-a-service (RaaS) released in February 2024, recruiting former users of ALPHV and LockBit. Since February 2024, RansomHub has already claimed over 210 victims, including at least three victims from Switzerland: an interior design company from French-speaking Switzerland, an industrial company from the canton of Zurich and a software company from the canton of Bern[43]. The ransomware targets poorly configured cloud storage locations and backups. According to an analysis by CISA (US Cybersecurity and Infrastructure Security Agency), critical infrastructures are also among RansomHub's target groups.[44]
The INC Ransom[45] malware, which has been active since July 2023, has already affected the healthcare and financial sectors as well as at least one association and several SMEs. Initial access can vary with this software since the observed methods include spear phishing via email and exploitation of vulnerabilities.

---

37 LockBit Admins Tease a New Ransomware Version (infosecurity-magazine.com)
38 See Semi-Annual Report 2024/1; conclusion in ch. 3.2.
39 Neue Ransomware-Banden zielen auch auf Schweizer Firmen (inside-it.ch)
40 Cicada 3301 - Ransomware-as-a-Service - Technical Analysis (truesec.com)
41 Ransomware-Angriff auf Schweizer IT-Dienstleister (inside-it.ch)
42 Helldown Ransomware: an overview of this emerging threat (sekoia.io)
43 Aufstrebende Ransomware-Bande attackiert Schweizer Software-Firma (inside-it.ch)
44 #StopRansomware: RansomHub Ransomware (cisa.gov)
45 Ransomware Spotlight: INC (trendmicro.com)

Activities of known ransomware variants

In the six months under review, there were also attacks with known ransomware such as Akira or Play, which affected the industrial, real estate, education, service and retail, financial and SME sectors. In the case of Play, the victim was a Swiss asset manager. A quarter of the clients mentioned in the leaked data were high-risk or politically exposed clients from different countries.[46] This case demonstrates that the publication of sensitive personal data not only poses risks for the company itself but can also endanger individuals mentioned in the data.

Recommendations

On the NCSC website, one can find a list of preventive measures to protect against ransomware as well as instructions for action in the event of an incident.

3.2.2 Ransomware as a global challenge

Wide range of techniques being used in attempted attacks

The changing dynamics in the ransomware ecosystem have forced certain groups to become flexible and evolve in terms of technology and tactics. The ransomware group 'Black Basta' which was already discussed in the first half of 2024, exemplifies this.[47] The group, known for its high-profile targeting, used new and/or versatile methods of infection.[48] This included amongst others:

- Email bombing: Attackers flood victims' email accounts with thousands of spam messages in order to overload recipients' email accounts or hide other unauthorised activities.
- Fake support: Using compromised Microsoft 365 accounts, the attackers send messages or make calls via the Teams collaboration platform and pretend to be the organisation's technical support. They trick victims into downloading remote monitoring and management software or send them malicious QR codes to gain access to the desired IT environment.
  One variant of fake support consists of requesting remote access to the victim's device instead of getting the victim to download malicious content themselves. Using the existing functionalities of Microsoft Quick Assist or control sharing in MS Teams, the attackers take control of the victim's device and ultimately install ransomware if they can obtain administrator rights.

Black Basta's latest distribution technique using a QR code via MS Teams was also used against Swiss companies.[49] The disruption of the 'Qakbot' botnet, which necessitated new

46 Boreal Capital: Hackers steal data from asset manager (tagesanzeiger.ch)

47 See Semi-Annual Report 2024/1; ch. 3.2.1.

48 Sophos tracks two ransomware campaigns using "email bombing," Microsoft Teams "vishing" (sophos.com), ReliaQuest Uncovers New Black Basta Social Engineering Technique (reliaquest.com)

49 WWeek 44: "Black Basta" - A clever way to defraud businesses: using spam to trick people into installing ransomware (ncsc.admin.ch)

partnerships with retailers for initial access and new personalised tools, may have been a factor in the switch to this new attack method.[50]

This adaptability and willingness to diversify and optimise their own operations is also evident in other groups such as Akira.[51] The group's focus is now primarily on stealing data. Prior to this action, the attackers carry out a pre-selection and sorting of the collected data.[52] They conduct reconnnaissance to extract valuable sensitive information, financial data, staff and patient files, classified documents, data on information technologies and networks used along with other particularly sensitive data.

Trends among victims and threat actors

According to a study conducted by Semperis in 2024, more victims than expected paid a ransom.[53] The main reasons given were the need to resume business activities as quickly as possible, the protection of patient, customer or company data or the risk of reputational damage. Another argument was cyber insurance, which covered the costs.

Recommendations

In general, the NCSC and its international partners[54] advise victims of ransomware not to pay a ransom. There is no guarantee that cybercriminals keep their word. Above all, paying a ransom supports cybercriminals financially to further expand their structures and carry out further attacks.

Another international trend observed in the six months under review was the use of ransomware by threat actors whose motives are not exclusively financial. According to Microsoft, cyberespionage actors closely linked to a state use ransomware as the final step in their operations to achieve financial gain, disruption, distraction, false attribution or deletion of evidence.[55] This is supposedly the case with the Chinese group 'ChamelGang[56] and with North Korean, Iranian or Russian[57] groups. In relation to North Korea, a research report thematizes how the state cooperated with members of the Play group.[58]

50 UNC4393 Goes Gently into the SILENTNIGHT (cloud.google.com)
51 Akira ransomware continues to evolve (talosintelligence.com)
52 Ransomware-driven data exfiltration: techniques and implications (sekoia.io)
53 Ransomware Risk Report (semperis.com)
54 Guidance for organisations considering payment in ransomware incidents (ncsc.gov.uk)
55 Microsoft Digital Defense Report 2024 (microsoft.com)
56 ChamelGang | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware (sentinalone.com)
57 Escalating Cyber Threats Demand Stronger Global Defense and Cooperation (microsoft.com)
58 Jumpy Pisces Engages in Play Ransomware (unit42.paloaltonetworks.com)

Hacktivist groups, such as ‘CyberVolk’ with suspected links to India, are now also using ransomware against state and public institutions in countries that pursue other interests.[59] In contrast, certain financially motivated groups such as ‘FunkSec’[60] also engage in hacktivism on the side.

Exploitation of vulnerabilities in ransomware attacks

The exploitation of vulnerabilities in authentication and remote access systems is popular as the initial access point for ransomware attacks (see ch. 4).[61] The exploited vulnerabilities are also often still unknown zero-day vulnerabilities. In this case, the victims are rarely specifically chosen by the cybercriminals. Instead, they scan the internet for vulnerable virtual private networks (VPNs) and firewalls whose management interfaces are accessible on the public internet. As such solutions serve as an access point to internal networks, they often become the gateway for ransomware attacks. The perpetrators therefore act opportunistically without targeting a specific sector. However, once they have identified a potential victim, they focus their efforts on it. The first half of the reporting period demonstrated that ransomware actors exploited various vulnerabilities for their activities. This included established and newer ransomware variants such as Akira, Black Basta, Fog, Helldown and LockBit.[62]

In addition to the exploitation of vulnerabilities, companies are particularly at risk in their supply chain environment. The risk often arises from the impact that the company is exposed to following an incident at an external partner or subcontractor. Supply chains are often complex, which makes it difficult to implement cybersecurity measures consistently. For example, the manufacturing industry[63] is considered particularly exposed due to the complexity of the systems and installations that are connected to the internet.

As at the end of the second half of 2024, there are more and more groups but fewer ransomware families and the number of attacks is increasing globally.[64] This is also reflected in the increasing number of data leaks and websites offering such data. Added to this is the fact that the increased use of AI is giving new threat actors such as FunkSec even easier access to more potential targets.

In Europe and Switzerland, legislative efforts are being intensified to improve the preparation for, detection of and response to cybersecurity incidents. For example, the ‘Cyber Solidarity

---

59 'CyberVolk' hacktivists use ransomware in support of Russian interests (therecord.media)

60 FunkSec - Alleged Top Ransomware Group Powered by AI (checkpoint.com)

61 Dragos Industrial Ransomware Analysis: Q3 2024 (dragos.com)

62 VMware ESXi (CVE-2024-37085) for the installation of ransomware such as Akira, Black Basta and LockBit
Veeam Backup & Replication (CVE-2024-40711) and SonicWall SonicOS (CVE-2024-40766) for the installation of Akira and Fog
Zywall Zyxel (CVE-2024-11667) for the installation of Helldown, see also ch. 3.2.1.
Windows Error Reporting Service (CVE-2024-26169) for the installation of Black Basta

63 Manufacturing Cyber Risk Report 2024 (blackkite.com)

64 Rapid7 Ransomware Radar Report 2024 (rapid7.com)

Act' for the healthcare sector in the European Union[65], the 'Cyber Security and Resilience Bill' in the United Kingdom[66] and the Cybersecurity Ordinance (CySO)[67] in Switzerland.

Recommendations

Each remote access must be sufficiently secured. Two-factor authentication should be set up for every accessible service from the internet. If this is not possible, access should be restricted to specific IP addresses and ports, and appropriate monitoring should be put in place.

Remote access protocols must be monitored for atypical access patterns, in particular access from regions where the company has no employees, from IP ranges assigned to large hosting providers, from known VPN endpoints or from the TOR network.

It is also important to set up regular patch management to fix vulnerabilities in a timely manner and verify them with vulnerability scans. Updates that fix critical security vulnerabilities in systems accessible via the internet should be able to be installed within 24 hours. Software or systems that are no longer supported by the manufacturer ('End of Life', EOL) should be switched off or if possible moved to a separate, isolated network zone.

3.3 Malware on mobile devices

In November 2024, the NCSC, the Federal Office of Meteorology and Climatology (MeteoSwiss) and the Federal Office for Civil Protection (FOCP) received reports of suspicious letters purporting to originate from the Federal Office of Meteorology and Climatology. These letters were forged and originated from fraudsters attempting to load malware onto mobile phones.

In the letter, the recipients were asked to install a new 'severe weather warning app'. However, there is no such Federal Administration app with that name. Instead, the QR code shown in the letter leads to the download of malware called 'Coper' (also known as 'Octo2'). When the supposed storm warning app is installed, the malware attempts to steal sensitive data such as access data from at least 383 smartphone apps (e.g. e-banking apps).

The malware only infects smartphones running the Android operating system. As soon as the malware has been downloaded, it is displayed on affected phones as an 'AlertSwiss' app with a modified logo in which the spelling ('AlertSwiss' instead of 'Alertswiss') and the logo differs from the real app. Instead of a round logo like the original application, the fake one has a rectangular logo in a white circle. The real FOCP Alertswiss app is an app to inform, warn and alert the public, which is used by various federal and cantonal authorities.[68]

---

65 The EU Cyber Solidarity Act (ec.europa.eu)

66 Cyber Security and Resilience Bill (gov.uk)

67 Federal Council launches consultation on Cybersecurity Ordinance (news.admin.ch)[68] Caution: Fake letters on behalf of MeteoSwiss – Instead of a 'Severe Weather Warning App', malware is downloaded (ncsc.admin.ch)

68 Caution: Fake letters on behalf of MeteoSwiss – Instead of a 'Severe Weather Warning App', malware is downloaded (ncsc.admin.ch)

Recommendation

On the NCSC website you will find a list of nine practical tips to make using your mobile phone safer (ncsc.admin.ch).

4 Vulnerabilities

'Time-To-Exploit' (TTE) is a critical indicator in the field of vulnerability management. It measures the time between the publication or discovery of a vulnerability and its active exploitation by attackers. The metric provides information on how quickly organisations need to respond to vulnerabilities in order to prevent potential attacks.
Various factors influence the TTE. On a technical level, aspects such as the availability of exploit details and exploit kits are decisive. The publication of information about a vulnerability, such as a proof of concept or exploit code, reduces the TTE. However, the complexity of a vulnerability is also relevant. While vulnerabilities that are easy to understand and exploit drastically reduce the TTE in some cases, it takes longer for complex vulnerabilities to be exploited. The latter require greater skill and preparation on the part of the attacker.
In addition, while security vulnerabilities used to be searched for less systematically in the past, attackers now use AI and machine learning (ML) to identify vulnerable systems and quickly develop exploits. In addition, the activities of potential attackers on the dark web also contribute to vulnerabilities being exploited more quickly than in the past. Exploits are traded more quickly in forums and on digital marketplaces.

In the longer term, the TTE has demonstrably and continuously shortened over time. Mandiant, an US-American IT security company, began analysing vulnerabilities in relation to this indicator in 2018. The results of the investigations are alarming. While an average TTE of 63 days was still observed in 2018/2019, the time span for 2020/2021 had already been reduced to 44 days. In the following two years, 2021/2022, the average TTE was again 12 days lower at 32 days. And in 2023, a potential exploitation of a discovered or published vulnerability had to be expected after an average of just five days.[69]
This development is the result of technological, organisational and criminal advances that ultimately enable attackers to identify and exploit vulnerabilities more quickly. The shorter TTE means that companies have less and less time to patch vulnerabilities or take other necessary security measures. The pressure on operators of IT infrastructures to act quickly increases significantly as the TTE decreases. In the case of critical vulnerabilities in particular, very little time often passes before the first attacks are observed.

The NCSC warned critical infrastructures of various vulnerabilities in the second half of 2024. The warnings concerned zero-day and N-day vulnerabilities. A zero-day vulnerability is still largely unknown to the general public and the manufacturer. A patch is therefore not yet available for installation, while the vulnerability is already being actively exploited. This constellation poses a high risk for organisations. The NCSC has published corresponding warnings for CVE-2024-47575 (in FortiManager) and CVE-2024-0012 (in Palo Alto Networks PAN-OS), among

69 How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends (cloud.google.com)

others. Both concerned zero-day vulnerabilities in products that have a broad user base in Switzerland. In both cases, the companies effectively had no time to fix them.

This contrasts with the N-Day vulnerability. In this case, a software fix (patch/fix) is already available to users at the time the vulnerability is disclosed, as the manufacturer was involved at an earlier stage and therefore had some lead time to develop countermeasures. In this vulnerability category, the NCSC actively highlighted CVE-2024-40766 (in SonicWall SonicOS), for example. The vulnerability affects widely used services from a network security provider. In this specific case, only 16 days passed between the vulnerability being disclosed by the manufacturer (21 August 2024) and the first observation of a possible exploit (6 September 2024).

Recommendations

The significantly shortened time-to-exploit (TTE) presents organisations and companies with new challenges. Attackers are becoming increasingly efficient at quickly identifying and exploiting vulnerabilities. Therefore, a combination of rapid roll-out of updates, proactive security work and automation is crucial to effectively protect against them. Many organisations are struggling to adapt the speed of patch distribution to the ever-shortening TTE timeframe.

Be sure to take the latest developments in TTE into account and adapt your company's patch management processes to the ever-shorter exploit timeframes. Optimise and accelerate your patch cycles, especially for critical vulnerabilities. Prioritise the elimination of vulnerabilities in exposed parts of your infrastructure. Carry out regular penetration tests and vulnerability scans to proactively identify any security gaps. Use monitoring and available threat intelligence. Real-time monitoring of your infrastructure, coupled with the possibilities of automation, will help you to identify security gaps in a timely manner. Ensure that your company has an up-to-date inventory of the infrastructure and products used.

Accompanying measures such as the use of red teaming, regular security checks or the operation of a bug bounty program in your company can also help to evaluate the effectiveness of response times in terms of overcoming vulnerabilities.

5 Fraud and social engineering

In the second half of 2024, the phenomenon of fraud again accounted for the majority of reports to the NCSC. Almost two thirds of all reports received belonged to the category fraud, or a total of 18,270 reports. While the number of fraud attempts rose sharply over the year as a whole from 30,496 to 41,374, the number of reports received in the second half of the year was 1,052 lower than in the same period of the previous year. The fluctuations in this category are almost exclusively due to the phenomenon of fake threatening calls from authorities.[70] In spring 2024, the NCSC logged record numbers of incoming reports at times. In weeks 12 and 14, for example, the NCSC received more than 1,600 reports per week on this phenomenon alone. These reporting peaks did not occur in the second half of the year. After a decline was observed in

[70] See also Report: Phone fraud in the cyber domain (ncsc.admin.ch)

the summer months, with only double-digit numbers of reports received, the numbers rose again in the fall and have since levelled off at 500 to 700 reports per week.

The NCSC observed a sharp increase in 'fraudulent lotteries' during the reporting period. Compared to the second half of 2023, the number of reports rose from 744 to 2,398. Over the year as a whole, the number of reports received more than tripled from 1,025 to over 3,509. In many cases, the names of well-known food and retail companies, electronics retailers or transport companies were misused. In order to access the supposed prize, the victims are redirected to a website where they have to enter personal data such as credit card details, name, email or mobile phone number. Hidden in the terms and conditions, displayed in very small print on the website or even outside the visible website area, it is pointed out that one is taking out a multi-year subscription. The fee is then immediately charged to the credit card. The approach is characterised by the fact that legal grey areas are exploited here (see ch. 5.4).
There has been a sharp increase in the phenomenon of CEO fraud among the fraud crimes most frequently reported by companies. Organisations in the communal and church environment were particularly affected. The reasons for this are explained in the third subchapter (see ch. 5.3). In contrast, there was a slight decrease in reports of invoice manipulation fraud. This fell by 4 to 114 reports in 2024 as a whole.

5.1 Online investment fraud and recovery scam

Online investment fraud was again the category with the highest reported financial loss in the six months under review. The loss amount per case is sometimes very high and can be in the six-figure range. One variant is the combination with a romance scam. In this variant, the scammers first pretend to be a loving, potential partner online to gain the victim's trust and establish emotional ties. Initial contact is made via dating sites, for example. As soon as trust has been established and sufficiently consolidated, the supposed girlfriend or boyfriend persuades the victim to make allegedly lucrative investments and claims to have made large profits themselves. In this way, the victims are less cautious and less critical of the proposed investment offers, as they come from someone trusted.

But even when the investment scam is over and the victim has come to terms with the financial loss, the danger is not over. In many cases, the fraudsters use the frustration to defraud the victim a second time. To this end, they contact the victim again after a certain period of time, but this time not as an investment company, but as a financial market supervisory authority, law enforcement agency or as organisations that supposedly help victims to recover lost money. In desperation, many victims cling to this hope. Official-looking documents are usually attached to the emails, which also feature stamps, signatures and official logos. However, these are all forged. If a victim responds, fees or taxes are demanded in order to initiate the refund process. New fees are then invented until the victim gives up and stops paying.[71]

[71] Week 38: Investment fraud - Alleged assistance after high loss (ncsc.admin.ch)

Recommendations

The greater the promised return, the greater the risk. Be careful if you are suddenly contacted by alleged lawyers, financial market supervisory authorities or similar bodies and organisations who promise to recover lost money and in turn demand fees in advance. Never pay fees. If companies had recovered the money, they could deduct the fees directly from the amount recovered and transfer the remaining amount to you free of charge.
Moreover, check whether the financial service provider is licensed by the Swiss Financial Market Supervisory Authority (FINMA). You can find information on licensed financial service providers in Switzerland on the FINMA website[72]. If a financial service provider is not licensed, you should exercise particular caution. Check the financial service provider on the basis of experience reports on the internet.

5.2 Variations of fake sextortion

With fake sextortion, the perpetrators claim that the victim's computer or email account has been hacked and that they have collected photo or video material that is supposed to show the email recipient during an alleged visit to pornographic websites. The blackmailers send such messages at random. In these cases, computers and email accounts are neither hacked nor do compromising images exist. In order to make their threats appear credible, the attackers have been using a number of tricks for years. They forge the email sender addresses (spoofing) so it looks as if the email has been sent from their own account. In another variant, the fraudsters mention old passwords from data leaks in the email to also pretend that the email account has been hacked. In some cases, the perpetrators even use these passwords to take over social media accounts and upload illegal content in order to provoke an account block. All this to make the victim believe that the perpetrator has access to compromising data. In the second half of the year, there were two new variants in quick succession. This seems to be a sign that the phenomenon is no longer so lucrative for the fraudsters and they are looking for ways of keeping the business model alive.

Fake sextortion messages in which the recipient is shown part of their telephone number were reported first (see fig. 8). Research by the NCSC has shown that this data is also likely to have originated from a data leak, in these cases probably from the data leak of the cryptocurrency service provider 'Gemini'. All recipients of the fraud emails reported to the NCSC were apparently affected by this data leak.[73]

[72] Approved Institutes: FINMA Authorisation – gaining entry to the financial market (finma.ch)
[73] Week 33: Fake sextortion and data leaks (ncsc.admin.ch)

I know, 76-XXX- is too personal to reach you.

Let me get straight to the point. You do not know anything about me however I know everything about you and you must be thinking why are you receiving this mail, correct?

I actually installed a Malware on porn website and there's more, you accessed same porn web site to experience fun (you get my drift). And while you were busy enjoying those videos, your browser began functioning as a RDP (Remote Protocol) that has a keylogger which gave me accessibility to your screen as well as your camera access. Just after that, my software program obtained all of your data and every one of your contacts from device including your complete photos.

Exactly what have I done?
It's simply your bad luck that I found your blunder. After that I invested in more days than I should have digging into your life and prepared a split screen sextape. First part shows the video you had been viewing and second part shows the view from your web camera (it is someone doing dirty things). Actually, I am ready to delete all information about you and allow you to move on with your regular life. And I will offer you two options that will achieve it. These two alternatives are either to disregard this e mail (bad for you), or pay me a small amount to close this topic forever.

Exactly what should you do?
Let's explore above two options in more depth. First Option is to turn a deaf ear my email message. Let us see what will happen if you choose this path. I will certainly send out your video to your contacts including members of your family, co-workers, and so forth. It does not protect you from the humiliation you and your family will face when relatives and buddies uncover your sordid videotape from me in their inbox. Other Option is to pay me, and be confidential about it. We will name this my "keep the secret charges". Now Lets discuss what will happen if you go with this choice. Your little secret remains private. I will keep my mouth closed. Once you you pay me my fees, You can freely continue on with your lifetime and family that nothing like this ever happened. You'll make the transfer via Bitcoins.

Amount to be paid: $950
My BTC Address: 1J8Sy8pJFa8Z952qNUumNv3NX31u2VzRKf
(Here's QR code, scan it)

Fig. 8: Fake sextortion email with recipient's phone number displayed

In the second new variant, the fraudsters also used residential addresses that they had obtained from data leaks and were thus able to link to the victim's email address (see fig. 9). After such cases were first observed in the USA, the NCSC also received the first reports from Switzerland in the second half of 2024. In contrast to the US variants, however, the fraudsters went one step further and not only mentioned the victim's home address in the blackmail email but also searched for images of the home address or the immediate vicinity on Google Maps and added these images to the blackmail email. In this way, the fraudsters want to convince the victim that they have full control over the computer and also know the victim's personal environment. This combination of digital and physical information considerably reinforces the threat and can tempt the victim to comply with the fraudsters' demands.[74]

74 Week 39: Another fake sextortion scam: Now the scammers know where you live (ncsc.admin.ch)

Important: You got one day to sort this out and I will only accept Bitcoin. I have a special pixel in this e mail, and now I've been notified that you have read through this email message. This email and Bitcoin address are custom-made for you, untraceable. If you are unfamiliar with Bitcoin, google it. You can buy it online or through a Bitcoin ATM in your neighborhood. There's no point in replying to this email or negotiating, it's pointless my price is fixed. As soon as you send the complete payment, my system will inform me and I will wipe out all the dirt I got on you. Remember if I notice that you've shared or discussed this mail with someone else, your video will instantly start getting sent to your contacts and I will post a physical tape to all of your neighborhood next week. And don't even think about turning off your phone or resetting it to factory settings. It's pointless. I don't make mistakes.

Looks familiar?

Fig. 9: Fake sextortion email with phone number, address and picture of the home address on Google Maps

Recommendations

Ignore fake sextortion emails and do not be intimidated. To date, the NCSC is not aware of any cases in which compromising image material has been available.

5.3 CEO fraud at communes, schools and churches

There was a noticeable increase in reports of CEO fraud in the second half of the year. While 487 reports were received in 2023, there were already 719 the year after. In classic CEO fraud, an email from the alleged CEO is often sent to the finance department or an email from the alleged club president to the treasurer. A credible story is used to persuade the person contacted to make a payment. In many cases, a gift card is also purchased and the code is then sent to the fraudsters.

It is particularly striking that certain sectors are affected by this phenomenon to an above-average extent. A remarkable number of communes, schools and churches received such fraudulent requests in the second half of 2024. The explanation for this is simple: In CEO fraud, the fraudsters usually gather the information from public sources to find out the hierarchical structures of companies, organisations or associations. Many companies publicly present their team, including their function and email address, on their website. However, they are nowhere near as consistent as communes, schools or churches. In these areas in particular, it is important for the public to be able to contact them easily. This is why contact details are published very transparently and, in some cases, entire directories of employees can be found on the

internet. What on the one hand is convenient for the public is also a profitable business for fraudsters and is being misused intensively.[75]

Recommendations

Make all employees aware of CEO fraud. Staff in finance departments and in key positions should be informed about these possible methods of attack. In the case of associations, all members with a function on the board should be trained. Establish clear processes for handling payments and enforce compliance with these processes (e.g. dual control principle, joint signatures, etc.).

5.4 Exploitation of legal grey areas

In many cases, the fraud is clearly visible on the websites reported to the NCSC. Phishing webpages, for example, are easy to identify as such. There is very little room for interpretation. This makes it relatively easy to get these sites taken down. In many other cases, fraudulent intent on the part of the website can be suspected, but very rarely proven. This makes it difficult or impossible to take such a website offline. In addition, fraudsters are increasingly trying to operate deliberately in this legal grey area. So-called subscription traps have been obsereved for some time. These websites advertise a free product but only mention in the small print that the free subscription will become a paid subscription after a few days if you do not respond. Once the deadline has passed, an annual or even biennial fee is charged in one go. Such subscription traps are considered to be the origin of all grey area scams.

Another example that has been reported repeatedly in the second half of 2024 is web shops that deliberately deliver incorrect goods of inferior quality. In the event of a complaint, the goods have to be returned at the customer's expense to the seller, who is usually based in the Far East. In these cases, the shipping costs are many times the value of the item, making it uneconomical to return. However, as you would have had the option of returning the goods, it is not clear whether the process can now be described as fraud.

Even more brazen are websites where you can supposedly order extracts from criminal records. However, after placing an order and paying CHF 20, instead of the requested extract, you only receive instructions on how to obtain such an extract. This information is useless, as you could have achieved the same result with a simple search engine query. The small print on the website does state that this is only a guide to ordering and not the order itself. However, it is obvious that the operators are speculating that the victim will overlook these lines. Prosecuting the providers is therefore usually very difficult. A similar approach is found on various websites that claim to help travellers apply for visas. In these cases, the effort involved is practically the same as if the visa were applied for via the official websites of the respective country. The only difference is that the services offered by the supposed help sites are significantly more expensive.

[75] Week 49: Churches, schools, associations and political parties increasingly the victims of CEO scams (ncsc.admin.ch)

Alleged offers for an entry in a more or less well-known business directory also belong to this category. These offers are often sent to companies by email or in a letter disguised as an official invoice. However, the small print indicates that the actual contract is only concluded once the invoice has been paid. Here, too, the invoice senders speculate that the company no longer knows exactly whether it is an existing contract that is to be extended or that it is just an offer.

Recommendations

Read invoices that you do not expect carefully, including the small print. If in doubt, clarify whether the bill is justified. Before registering or giving your credit card details, read the terms and conditions. Be particularly wary of supposedly free offers. Check out the service provider by reading testimonials online.

6 Attacks on the availability of websites and -services and disruption of infrastructure

In attacks on the availability of websites and services – usually in the form of distributed denial of service (DDoS)[76] – attackers attempt to make a service accessible from the internet temporarily unavailable by sending a large number of requests. Such attacks do not result in unauthorised access to data, an outflow of information or lasting damage to systems.
However, the infrastructure can also be disrupted if updates or configuration changes impair operations. Presumably due to malicious manipulation of the login tool systems of Swiss media companies OneLog, login and registration services were unavailable in autumn 2024. This affected dependent functions such as the paywall and comment function of the publications concerned (see ch. 7).[77] Apart from malicious manipulation, the effects of a faulty component update can also lead to malfunctions. This is examined in the second part of this chapter using the incident of the security service provider CrowdStrike as an example.

6.1 DDoS attacks

DDoS attacks on the systems of Swiss organisations resulted in temporary outages of financial services[78] and cantonal websites[79] in the second half of 2024. The number of direct reports to the NCSC on attacks of this type increased only slightly from 41 in 2023 to 48 in 2024. The increase is mainly attributable to the second half of the year. Here, the number rose from 17 to 25 incidents.

DDoS attacks are often enabled by attack infrastructure, which cybercriminals can direct at the targets of their choice if they are paid accordingly. In September 2024, the NCSC recorded an increase in DDoS attacks carried out by a botnet called ‘Gorilla’. This is a DDoS-as-a-service

76 Attack on availability (DDoS) (ncsc.admin.ch)
77 OneLog Update: Login services available again (onelog.ch)
78 DDoS-Angriff trifft Swisscom und legte Twint lahm (inside-it.ch)
79 Informatique: l'Etat de Vaud victime d'attaques ‘très virulentes’ (24heures.ch), Revue des cybermenaces : Septembre 2024 (vd.ch)

service offered on Telegram, which can be rented for a corresponding fee. As an operator of a critical infrastructure in Switzerland was affected, the NCSC has published the findings in a technical report[80]. These DDoS attacks against Swiss infrastructures were DNS amplification attacks. In these attacks, exceptionally large data streams are directed at the victim's infrastructure by misusing the Domain Name System (DNS), thereby overloading it.

On the Sunday of 24 November 2024, when votes were being held, the website of the canton of Schwyz was the target of a DDoS attack[81]. The attack lasted for a long time and resulted in the websites of various communes in different cantons and various cantonal websites also being unavailable for several hours[82]. All of the affected websites were operated by the same service provider and were thus affected collaterally. Nothing was revealed about the motivation of the attack. It was also not possible to establish a direct link to the votes being held that Sunday.

Switzerland was not excessively affected by DDoS attacks when comparing observations with international incidents.[83] In addition to the ongoing attacks by hacktivists in connection with international conflicts, individual events can also provoke DDoS campaigns. For example, the arrest in France of the founder and CEO of the messaging app Telegram, Pavel Durov, triggered a partially coordinated response by several hacktivist collectives under the hashtag #FreeDurov. Over 50 French organisations were targeted by DDoS attacks in this campaign.[84] In some cases, law enforcement agencies were able to identify and arrest the attackers or disable the attack infrastructure. For example, the Spanish police arrested people who had participated in the 'DDoSia' botnet of the pro-Russian group 'NoName057(16)'[85] and provided equipment for attacks.[86] US prosecutors were able to indict two key members of the hacktivist group 'Anonymous Sudan' and confiscate large parts of their attack infrastructure.[87] Meanwhile, German prosecutors were able to take 27 stresser services offline as part of 'Operation PowerOff'. Stresser services are DDoS services that can be hired by third parties to attack any target. Over 300 users of these services were also identified, some of whom have already been arrested.[88]

Despite these successes, DDoS attacks remain a popular means for a wide range of actors to restrict the availability of targets in the short term and thereby attract attention, among other things. The media can counteract this goal through restrained reporting. The continuous expansion of attack infrastructures such as botnets and their advanced methods require network operators to keep their defensive measures constantly up to date.

---

80 See Brief technical analysis of the "Gorilla" botnet

81 DDoS attack on the website of the Canton of Schwyz causes various cantonal and municipal websites to go down (ncsc.admin.ch)

82 Cyber-Angriff: Websites von Gemeinden nicht mehr erreichbar (luzernerzeitung.ch)

83 Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4 (cloudflare.com)

84 Hacktivists Call for Release of Telegram Founder with #FreeDurov DDoS Campaign (blog.checkpoint.com)

85 Detailed analysis report on the DDoS attacks «NoName057(16)» (ncsc.admin.ch)

86 Tres detenidos por delitos de daños informáticos con fines terroristas (interior.gob.es)

87 Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks (justice.gov)

88 Operation „Power OFF": weltweiter Schlag gegen Cybercrime-Infrastruktur (bka.de)

Recommendations

The NCSC website lists various measures to prevent and defend against such attacks under the heading Attack on availability (DDoS attack) (ncsc.admin.ch). You should work with your service provider or host to prepare for a potential attack in order to minimise the impact. For critical systems, it may be advisable to seek support from a commercial DDoS protection provider.

In case of extortion DDoS attacks, the NCSC recommends that you do not respond to the ransom demands. The perpetrators may ask for more money after an initial payment and then continue with the attacks. Instead, you should report the incident to the NCSC and contact the police to make a criminal complaint. In the event of an attack, recommendations under DDoS attack – What next? (ncsc.admin.ch).

6.2 CrowdStrike incident

On 19 July 2024, there was a worldwide disruption to Windows systems that has been described as the most far-reaching IT outage in history. This disruption was not caused by a cyberattack, but was triggered by a faulty update to the CrowdStrike Falcon protection module, which is used to detect and defend against such cyberattacks. The update caused a large number of Windows computers to display the 'Blue Screen of Death', which causes the device to crash and become inoperable.[89] CrowdStrike managed to identify the error within a few hours and immediately stopped the distribution of the faulty update. CrowdStrike and Microsoft subsequently published instructions on how to fix the problem.[90] Fixing the problem required booting each affected system in safe mode and manually removing a specific file. Because Safe Mode boot is typically not available to normal users and the required Bitlocker keys were sometimes located on other systems affected by the incident, certain organisations experienced significant delays in resolving the issue. It is estimated that over 8.5 million systems worldwide were affected by the incident, with total losses estimated at several billion US dollars.[91]

The impact was first seen in Australia, then in India, Europe and the US, depending on the time when the working day started after the faulty update. The organisations affected included numerous large companies, government agencies and public institutions, with the impact being particularly noticeable in the aviation sector. This is also due to the high complexity of air transport and the tightly synchronised flight schedules. The incident also occurred on a Friday in July, a period with particularly high volume of flights in Europe. As a result, there were many delays and flight cancellations at numerous airports. Major international airports such as Heathrow in London and airlines such as Delta Airlines were particularly badly affected and

89 CrowdStrike oopsie crashes Windows workstations across the world (therecord.media)

90 KB5042421: CrowdStrike issue impacting Windows endpoints (microsoft.com), Falcon Content Update Remediation and Guidance Hub (crowdstrike.com)

91 What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk (hbr.org)

had to postpone or cancel thousands of flights. There were also delays and cancellations at Zurich Airport in Switzerland.[92]

The security incident was promptly exploited by criminals to initiate fraudulent activities. The attack methods used by the criminals included phishing emails that simulated support offers from CrowdStrike and malicious scripts that promised an automated recovery of the affected systems. CrowdStrike responded to these incidents with public reports and statements, in particular advising users to only download updates from official sources.[93] In addition, opportunistic scammers posed as airline customer service representatives. The scammers also scanned social media for posts from disgruntled travellers whose flights were delayed or cancelled. The criminals then contacted those affected via fake social media accounts and asked them to provide sensitive information such as their personal details, booking confirmation number or credit card details. [94]

As a result of the IT outage, CrowdStrike reviewed and optimised its internal testing processes for software updates and added a feature that allows customers to choose whether they want to receive content updates immediately or with a delay. The aim is to minimise the risk of future incidents of this nature. One particular feature of Windows systems that allowed such an outage to occur is the extended access rights required by kernel-level software from security vendors such as CrowdStrike. Microsoft has commented on this and emphasised that although security solutions require access at kernel level, it must be subject to better guidelines and innovations should restrict this access in the future. Microsoft also announced that it would intensify its cooperation with partners such as CrowdStrike to limit such risks in future.[95]

Recommendations

Effective patch management is critical to maintaining security and stability. Organisations need to weigh up the pros and cons of immediate installation, which fixes vulnerabilities quickly but risks untested disruptions, and delayed installation, which allows thorough testing but leaves systems unprotected for longer. A staggered update based on the exposure and criticality of the systems can be a suitable strategy to minimise risk.

Staff training in relation to IT failures is essential to ensure a quick and effective response in the event of an emergency.

7 Data management, leaks and extortion

Data leaks and unwanted data exposures were also an issue in the second half of 2024, both in Switzerland and internationally. However, secure and intact data storage can only be achieved if access protection and data management are prioritised by authorities, companies and individuals. This was impressively demonstrated by the cyberincident involving the Swiss

92 CrowdStrike-Softwarefehler - Der Tag, an dem die IT weltweit verrückt spielte (srf.ch)

93 Falcon Sensor Issue Likely Used to Target CrowdStrike Customers (crowdstrike.com)

94 Scammers impersonate airline customer service representatives (ftc.gov)

95 CrowdStrike tells Congress of two process changes to address July outage incident (therecord.media), Windows Security best practices for integrating and managing security tools (microsoft.com)

single sign-on platform OneLog at the end of October 2024. Following a forensic investigation, it was possible to rule out a leak of user data from the media platform.[96] Nevertheless, various media outlets had to offer their content without a paywall for 10 days.[97] This was necessary because the threat actor deleted the user data for authentication with OneLog, which meant that paying customers could no longer be identified.[98] Other cyberincidents also highlighted the value of data, especially when the integrity or availability of data is in doubt. In the cyberincident at the VidyMed practice group in December 2024, data was no longer available, which is why the four practices had to temporarily switch to pen and paper to continue providing medical care.[99] A similar situation occurred at numerous schools in Europe, North America and Singapore that used a digital platform to manage school lessons. After an unauthorised user gained access to the platform at the beginning of August, the data from at least 13,000 students' devices was deleted.[100] Just a few months later, another global provider of teaching software experienced a similar cyberincident: the threat actor stated in an extortion message that they had accessed the data of around 62 million schoolchildren and 10 million teachers.[101] In this case, the incident did not lead to any data being deleted from the devices of schoolchildren and teachers or to the systems being encrypted. However, the immense volume of leaked data can serve as a basis for future crimes in both the digital and physical space. This is because sensitive personal data was also exfiltrated in this case.[102]
Secure data storage is particularly relevant with regard to data leaks, where the leaked data represents a downstream risk for other organisations and private individuals. While companies may have to monitor their access to their own IT infrastructure after a data leak at a supplier, the risk of becoming a victim of attempted fraud also increases (see ch. 5). Similarly, sensitive information of private individuals can be misused for account takeovers, phishing (see ch. 2), identity theft or financial fraud. Threat actors in the ransomware environment play a particularly important role here, as they usually publish the data and/or monetise it, for example by selling it, if the ransom is not paid (see ch. 3.2). In addition to the activities of threat actors, other causes such as inadequate data management in a company's own infrastructure, existing vulnerabilities or technical misconfigurations can also lead to data exposure. This can then be exploited by threat actors in a second step.

Dedicated marketplaces on the internet and the dark web – such as Breachforums – offer cybercriminals the opportunity to sell stolen data and make a profit.[103] Temenos, a Swiss provider of banking software, was the victim of such an incident in November 2024.[104] The hacker claimed that the data contained details of employees as well as details of applications and web

---

96 See press release OneLog informiert über weitere Erkenntnisse nach Sicherheitsvorfall: Keine Hinweise auf Datendiebstahl, Untersuchungen dauern an (ringier.com)

97 Ein Super-GAU für die Schweizer Medienwelt (republik.ch)

98 OneLog provides further information after the security incident: No evidence of data theft, investigation is ongoing (ringier.com)

99 Groupe Vidymed: actualites (vidymed.ch); see press releases dated 7. December 2024, 20. December 2024 and 14. January.2025.

100 Mobile Guardian: Security Incident Report (mobileguardian.com), Hacker wipes 13,000 devices after breaching classroom management platform (bleepingcomputer.com)

101 PowerSchool starts notifying victims of massive data breach (bleepingcomputer.com)

102 Powerschool hat offenbar Daten von 62 Millionen Schülern verloren (inside-it.ch)

103 See Semi-Annual Report 2024/1; ch. 7.2.

104 Hacker verkaufen Daten von Temenos Quantum Fabric (inside-it.ch)

services for banks and other customers. To lend additional credibility to the claims, the hacker added screenshots. In some cases, hackers also offer to buy back the stolen data from the organisations to prevent publication or resale. The problem with such offers is that victims can never be sure to whether the cybercriminals will keep their word.

Hacktivists use sensitive data from targets to spread their social, political or ideological interests. One of the most popular methods used by these groups is to hack IT systems and then publish the captured personal data and information. This approach is also known as hack-and-leak. For example, a pro-Palestinian hacktivist group published personal information of Israeli athletes on social media during the Summer Olympics in France. In addition to names, telephone numbers, addresses, passwords and photographs, medical information such as blood type was also published.[105] Such information is particularly problematic for individuals and companies when it becomes easily accessible as structured data for threat actors. This increases the risk of the information being systematically exploited for fraud or other malicious activities. In mid-November, the user 'Nam3L3ss' published various data records from 25 large corporations on the dark web platform 'Breachforums'. Two Swiss companies were among the victims.[106] After a month of further activity, the number had risen to around 100 data records published by the same user.[107] Unlike other platform users, this user claimed that he had not collected the data by hacking, but had simply released data unintentionally exposed by the companies. This was the case, for example, when data was sent unencrypted during transmission or when data was stored online without password protection. Data that ransomware groups used for blackmail is also part of these data sets. According to Nam3L3ss, it did not intend to sell the data, but by distributing the adjusted data sets, it wanted to emphasise its political ideas for more responsibility in data management. In Switzerland, such an approach violates the Data Protection Act because a private actor such as Nam3L3ss may only collect, process and publish personal data with the consent of the data subjects.[108] This applies especially to personal data that is considered particularly worthy of protection.

Recommendations

The various incidents in the second half of 2024 make it clear that securing sensitive data must be a priority. Once content has been published on the internet, it is almost impossible to delete it permanently. Therefore, the general rule is:

In line with the 5Ws of data storage, it is important to determine who should store and processes which data, in what form, where and with whom it should be shared. In addition to conservative data storage practices, you should regularly review data and delete data that is no longer required. Archive data that is worth keeping but no longer actively used offline. Establish clear, workable processes for handling and protecting data, and monitor their implementation. Furthermore, protect access to systems, accounts and data with strong passwords

105 Israeli athletes doxed at Olympic Games by Zeus hacking group (bitdefender.com)

106 Amazon, UBS und Firmenich von Breach betroffen (inside-it.ch)

107 Conversation with a 'Nam3L3ss' Watchdog: Preface (databreaches.net)

108 See also Art. 31 DSG (Data Protection Act)

and, wherever possible, with multi-factor authentication (MFA).[109] Only grant access to people who really need it.

Data from previous breaches can be reused in subsequent attacks. Check regularly to see if your credentials have been exposed in a data leak, for example on the Have I Been Pwned (haveibeenpwned.com) website or the Hasso Plattner Institute's Identity Leak Checker (hpi.de).

8 Cyberespionage and -sabotage

State or state-sponsored threat actors pose a particular type of threat in cyberspace. Often referred to as 'Advanced Persistent Threat' (APT)[110], these groups carry out espionage or, more rarely, sabotage attacks if it serves their interests. In contrast to financially motivated cybercriminals, they select their targets specifically and go to great lengths to obtain the desired information or achieve the intended effect. Accordingly, potentially affected organisations must also make their defensive measures against this type of threat more robust.

8.1 Cyberespionage

Typhoon season

At the end of September 2024, the Wall Street Journal reported that a group called 'Salt Typhoon', allegedly operating for the Chinese authorities, had compromised several US telecom providers.[111] Following these initial revelations, the US authorities CISA and the Federal Bureau of Investigation (FBI) announced on 25 October 2024 that they were investigating unauthorised access to telecommunications infrastructure by actors linked to the People's Republic of China.[112] At the time, this announcement coincided with several media reports that Salt Typhoon had targeted data from phones used by President Donald Trump and Vice President J.D. Vance, as well as employees of the former Vice President Kamala Harris and other Democratic Party figures, through access to key US telecom providers. In addition, there have been further revelations of a possible compromise of the system used by the US government to request phone surveillance. The exact extent of this campaign is still difficult to assess. In December 2024, the White House stated that it had identified nine telecommunications companies as victims through which the perpetrators could potentially attack specific targets over a long period of time. In this case, privileged access allows the attacker to record calls, locate users and access mobile device metadata.[113] According to the security company Trend Micro, there is also the possibility that the campaign targeted institutions outside the USA. The company sees similarities between the activities of Salt Typhoon and an actor it has observed called 'Earth Estries'.[114]

---

[109] See Protect your accounts (ncsc.admin.ch)

[110] APT – Glossary (csrc.nist.gov)

[111] Chinese-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack (wsj.com)

[112] Joint Statement by FBI and CISA on PRC Activity Targeting Telecommunications (cisa.gov)

[113] US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage (reuters.com)

[114] Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions (trendmicro.com)

Salt Typhoon's goal is most likely to gain access to particularly sensitive information. In this area, compromising telecom providers provides an ideal entry point to many high-value targets, especially prominent politicians. However, other attacks, also attributed by the US authorities to Chinese state actors, appear to be more about gaining control of critical infrastructure. This is the case with the 'Volt Typhoon' group, which was mentioned in the last NCSC semi-annual report[115]. The US authorities fear that these access points could be used to sabotage US infrastructure in the event of a crisis.[116]

The attention paid by the United States to China's allegedly hostile activities is also reflected in official reactions. On 18 September 2024, the US Department of Justice announced the dismantling of a botnet presumably operating on behalf of the Chinese APT 'Flax Typhoon'. In their announcement, the US authorities emphasised that the botnet was operated by the Chinese company Integrity Technology Group. Subsequently, on 3 January 2025, the US Treasury Department announced that it had imposed sanctions on the same company for its role in hacking attacks on US institutions attributed to Flax Typhoon.[117] In a striking coincidence of timing, the US Treasury Department had shortly before publicised a compromise of its IT systems, also perpetrated by an actor with suspected ties to the Chinese state. The attackers used a support key that had been stolen from a third-party provider with privileged access.[118]

New APT29 campaign

The NCSC report on the first half of 2024 provided information about numerous espionage activities attributed to the 'APT29' group. The group allegedly operates for the Russian foreign intelligence service. APT29 was also held responsible for a large-scale campaign that was probably also carried out for espionage purposes. Starting on 22 October 2024, Microsoft observed this actor, which Microsoft names as 'Midnight Blizzard', sending a series of highly targeted spear-phishing emails with a signed Remote Desktop Protocol (RDP) connection file. This connection file, when executed, connected to a server controlled by the actor.[119] According to Microsoft, this campaign targeted government agencies, universities, defence organisations and non-governmental organisations in dozens of countries, primarily in Europe, Australia and Asia. Similar activities were also reported by the Computer Emergency Response Team of Ukraine (CERT-UA) under the name 'UAC-0215' and by Amazon.[120] The phishing emails in this campaign were sent from email addresses of legitimate organisations. These email addresses had been collected in previous compromises.

Further development of procedures

The most sophisticated groups active in cyberespionage have the ability to continuously develop and improve their offensive arsenal. This allows them to exploit new opportunities and circumvent existing defences. The reporting period provided two highly illustrative examples of this very specific know-how.

---

115 Semi-annual report 2024/1 (ncsc.admin.ch)

116 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (cisa.gov)

117 Treasury Sanctions Technology Company for Support to Malicious Cyber Group (treasury.gov)

118 US Treasury says Chinese hackers stole documents in 'major incident' (reuters.com)

119 Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files (microsoft.com)

120 Amazon identified internet domains abused by APT29 (aws.amazon.com)

In October 2024, the security software provider ESET attributed a series of attacks on a government organisation in Europe to the APT actor 'GoldenJackal'. According to ESET, this actor developed two different steps to compromise physically isolated systems (air gap) using a USB stick. In the first step, the USB stick is inserted into a system connected to the internet that has already been compromised. The method used for this first compromise is not yet known. The same USB stick then infects the isolated system as soon as it is plugged in. Finally, the data is tapped again via the system connected to the internet as soon as the USB stick is plugged back into this system. An air gap is generally used for critical networks, such as industrial control systems or high-security networks. The resources required to develop such a tool suggest state involvement. ESET does not give a clear indication but sees similarities in the approach with suspected Russian APTs, in particular 'Turla'.[121]

In November 2024, the cybersecurity company Volexity described a new, creative approach used by 'GruesomeLarch', an alleged Russian APT (also known as 'APT28' or 'Sofacy'). The group is believed to be operating for Russian military intelligence. To achieve its cyberespionage objectives, it penetrated the networks of its targets by connecting to the company's Wi-Fi network. The attacker's strategy was to infiltrate another organisation adjacent to the target, then spread out within that organisation to find dual-connected systems, meaning systems with a wired and a wireless network connection, and connect to the victim's corporate Wi-Fi network from that compromised neighbouring system.[122]

Conclusion

The high willingness of such attackers to invest time and resources in tools enables them to penetrate even the most secure networks. As a basic rule, USB sticks should not be allowed to be inserted into any devices in secure and physically isolated systems. Only certain, precisely defined connections should be possible to the outside world and those connections must be monitored. The compromise of a neighbouring company can also pose a security risk. With Wi-Fi, it is important to distinguish between the guest network and the more heavily protected company network.

Alleged IT staff

Actors suspected of working on behalf of the North Korean government have long occupied a special place among offensive state cyberactors, as they not only engage in cyberespionage but also carry out a large proportion of their activities for financial purposes. This trend is in line with the priorities of the North Korean regime, which needs foreign currency due to wide-ranging economic sanctions.

In particular, actors associated with North Korea have frequently attacked cryptocurrency trading platforms. In the final days of the reporting period, the US and Japanese authorities blamed a state actor from North Korea for stealing USD 308 million from the DMM trading platform in

121 Mind the (air) gap: GoldenJackal gooses government guardrails (welivesecurity.com)

122 The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access (volexity.com)

May 2024.[123] In this case, as in many others, the attack vector consists of an alleged recruitment process for IT employees in an attempt to transmit malicious code to the target.[124] Recently, however, the actors have regularly resorted to another method in which they place their agents as IT employees working remotely for Western companies. To do this, they use false identities and technical tools (especially VPNs) to disguise their whereabouts. They also do not shy away from using AI to generate photos or videos.[125] This method is proving to be very profitable. For example, in an indictment published on 12 December 2024, the US Department of Justice held 14 North Korean nationals responsible for a six-year fraud of this kind, in which USD 88 million is said to have flowed to the North Korean regime.[126]
This threat has many facets, and the access of such employees to Western corporate networks can be used profitably in various ways. On the one hand, these employees earn money in the form of the salary they receive for their work in the companies. On the other hand, cases have also been observed in which they have stolen sensitive data and then blackmailed their former employers. These actors do not only appear to be pursuing financial goals; their access to company networks can also be used for espionage purposes under certain circumstances.

Recommendations

The defence against this type of threat must be carried out on several levels. First and foremost, it is about recognising conspicuous behaviour or elements in the recruitment process, but also about carrying out checks during the recruitment process to ensure the identity of applicants.[127]

8.2 Threat to industrial control systems and operational technology

Digitalisation is not only leading to the increasing use of IT in the data and information space, but is also increasingly extending to and influencing physical processes. The operational technology (OT) used for this, such as industrial control systems (ICS), which used to be mostly isolated is becoming increasingly networked with the rest of the system landscape and is thus also exposed to risks from its environment.
People who do not work in an industrial environment are most likely to come into contact with this development through advances in building automation as part of smart home projects. It

123 FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com (fbi.gov)
124 On this method, see in particular the details of a campaign called ‘contagious interview‘: Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Install New Variants of BeaverTail and InvisibleFerret Malware (unit42.paloaltonetworks.com)
125 In this context, the company Knowbe4 has shared a concrete example of a recruitment process with such an applicant with bad intentions: How a North Korean Fake IT Worker Tried to Infiltrate Us (blog.knowbe4.com)
126 Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions (justice.gov)
127 The latest in North Korea's fake IT worker scheme: Extorting the employers (therecord.media)
This comprehensive document from the UK authorities contains a number of recommendations: OFSI Advisory on North Korean IT Workers (gov.uk)

is therefore not surprising that security specialists in the industrial environment have observed an increase in attempted attacks on building automation.[128]

Successful attacks against such industrial systems with serious consequences in the physical world continue to be recorded almost exclusively in the context of ongoing conflicts. At the end of July 2024, for example, it became known that a sabotage attack was responsible for a two-day outage of a heating system for around 600 residential buildings in Ukraine. The specially designed malware 'FrostyGoop' was used via the Modbus protocol, which is applied in the environment of cyber-physical industrial systems.[129] The second conflict, in which cyberattacks repeatedly play a supporting role, is raging in the Middle East. For example, actors already associated with the Iranian Revolutionary Guards in previous attacks used the 'IOCONTROL' malware to manipulate IoT and OT devices.[130] On the other side, hacktivists calling themselves Red Devil claimed to have sabotaged water treatment plants in southern Lebanon.[131]
In addition to cyberattacks, physical interventions also have an impact on information and communication technology. For example, Hezbollah pagers and radios were manipulated in the manufacturing and supply chain and detonated after delivery.[132] In the Baltic Sea, the repeated destruction of underwater cables prompted the affected coastal states to increase security measures to protect them.[133]

Outside of conflict areas, hacktivists linked to the belligerent parties have also carried out isolated attempts at sabotage. For example, the pro-Russian group 'Z-Pentest' tampered with Danish pump control systems, but the effects were brought under control.[134]

In future, the Cyber Resilience Act (CRA), which came into force at European level on 10 December 2024, could make an important contribution to ensuring that OT and IoT systems can be better protected by making manufacturers responsible for providing a minimum level of security functionality.[135]

Recommendations

Secure your industrial systems to prevent attacks as described in this chapter. The NCSC suggests measures to protect industrial control systems (ICSs) for this purpose. The ICT minimum standards developed by the Federal Office for National Economic Supply (FONES) in cooperation with the respective industry organisations are somewhat more comprehensive.

128 2024 Global Threat Roundup (forescout.com)
129 Impact of FrostyGoop ICS Malware on Connected OT Systems (dragos.com)
130 Inside a New OT/IoT Cyberweapon: IOCONTROL (claroty.com)
131 Israeli Group Claims Lebanon Water Hack as CISA Reiterates Warning on Simple ICS Attacks (securityweek.com)
132 Lebanon pager and walkie-talkie explosions: What we know so far (apnews.com)
133 We assume damage to Baltic Sea cables was sabotage, German minister says (theguardian.com)
134 'Koden var 1234': For første gang er dansk vandforsyning blevet angrebet af prorussiske hackere (jyllands-posten.dk)
135 Cyber Resilience Act (digital-strategy.ec.europa.eu)