6 May 2024 | National Cyber Security Centre NCSC

Semi-annual report 2023/II (July–December)

Information assurance

Situation in Switzerland and internationally

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Overview/contents

Management summary

The National Cyber Security Centre (NCSC) became a federal office on 1 January 2024, although it will still be known by the same name in English. The NCSC is using this change as an opportunity to highlight the Confederation's various fields of activity in the area of cybersecurity, which are the focus topic of this report. Two guest articles examine the challenges involved in prosecution and in certifying the cybersecurity of communal authorities.

Increase in reports in the second half of 2023

The NCSC received 30,331 reports of cyberincidents in the second half of 2023, almost twice as many as in the second half of 2022 (16,951 reports). This increase was driven primarily by fraudulent job offers and supposed calls from the police.

Fraud and scams were once again among the cyberincidents most frequently reported to the NCSC in the second half of the year. Fraud attempts reported by businesses were up slightly, and mostly fell into the categories of "CEO fraud", which accounted for 253 reports (compared with 190 in the same period in 2022), and "business email compromise" (63 reports, up from 45 the year before). By contrast, reported ransomware attacks on businesses were down. The NCSC received 54 such reports in the second half of 2022, and 42 in the period under review.

Fraud attempts using artificial intelligence

During the period under review, the NCSC saw an increase in reports of attempted fraud involving the use of artificial intelligence (AI). These included sextortion with AI-generated images, scam calls and investment fraud in the name of celebrities. Given the comparatively low number of reports in this area, the NCSC believes that these are likely to be initial attempts by cybercriminals to explore how AI can be profitably used for cyberattacks in the future.

Phishing still the second most frequently reported phenomenon

Reports of phishing more than doubled year on year, from 2,179 to 5,536. Of particular note here is "chain phishing", where phishers use hacked email accounts to send emails to all the addresses linked to that account. Because the sender is supposedly known to the recipients, they are more likely to fall for the scam. The phished email account is then used to email all the contacts of that account.

Editorial

The National Cyber Security Centre: strengthening Switzerland's cybersecurity

On 1 January 2024, the National Cyber Security Centre (NCSC) became a federal office and was transferred from the Federal Department of Finance (FDF) to the Federal Department of Defence, Civil Protection and Sport (DDPS).

It retains the same name in English and its core remit also remains unchanged: to protect Switzerland from cyber risks through preventive action, to provide support during cyberincidents and to identify opportunities to position Switzerland strategically and effectively in cyberspace. Its primary objective is to enable organisations and individuals to understand cyber risks and to design their cybersecurity in line with their own risk tolerance. To this end, the NCSC works with its partners to establish economic and civil-society mechanisms that reduce systemic risks, while also keeping the costs of addressing cyber risks as low as possible. This will make Switzerland an attractive location for businesses which operate in the digital space.

Current challenges in Swiss cybersecurity include the high vulnerability of IT systems, sometimes still weak capabilities to respond to systemically important cyberincidents and crises, and in many cases a lack of transparency and data to assess and critically question statements by experts and organisations on cybersecurity. These risk factors mean that cyberattacks are too often successful, which in turn results in high levels of economic damage and a high risk of critical infrastructure outages. Reports of cyberincidents resulting in damage increase by an average of around 30% per year. While the situation sounds dramatic, it must also be borne in mind that these figures are perfectly understandable given the ever-increasing use of the digital space. In an international comparison, Switzerland is in the middle of the field. That said, the situation does need to be taken seriously, and action is required to improve it. To this end, the NCSC is focusing on four strategic areas: promoting understanding of cyberthreats, providing means to prevent cyberattacks, reducing damage from incidents and enhancing the security of digital products and services. What this means in practice can be found in the NCSC's newly published strategy.

The NCSC's staff is key to its success. The NCSC wants to be an attractive employer in order to recruit and retain talented employees who will align its services and products as efficiently and effectively as possible with the needs of policymakers, business and civil society. To achieve this, the NCSC must be flexible, speedily adapting its organisational structure to new requirements and economic realities. This is only possible if its teams can act as autonomously as possible and decisions can be made as independently as possible, or at least significantly influenced, by employees who have the necessary expertise. Such decisions often have to be taken quickly, which in turns enables an open and objective error culture. I would rather have us make mistakes in a controlled way and be innovative, than not make mistakes and not move forward. This makes it all the more important to maintain a high level of operational excellence and to deliver reliable and consistent results. Central to all this, is a workforce that is as diverse as possible, and willing to repeatedly question both itself and management in a constructive fashion. This is an ideal and we are not quite there yet. But we have taken important steps in this direction, and that is reflected in the fact that, in my view, our staff is doing an excellent job.

It is important to us that you, esteemed readers, give us feedback and in particular constructive criticism when the NCSC fails to live up to your expectations. In this critical phase of the federal office's development, this matters more than ever. Ultimately, we want to work with you to create a free and safe cyberspace for the benefit of all.

Florian Schütz, Director National Cyber Security Centre

1 Focus: cybersecurity challenges

Cybersecurity, and therefore protecting Switzerland against cyberthreats, is a joint task for society, the business community and the state. All parties involved are required to take appropriate measures within their sphere of responsibility and influence.

As in many areas, the first principle of cybersecurity is personal responsibility. However, there are challenges that exceed the ability and capacity of individuals and organisations, where the state must step in to provide support or perform certain tasks.

With the National Cyber Security Centre (NCSC[1]), which acts as the federal government's competence centre for cybersecurity, the Federal Council has created a structure that enables the state to tackle various cybersecurity challenges:

1.1 Identifying and informing about cyberthreats

It is important to be aware of the latest phenomena in order to know what to look out for and what measures to take. Information about what is going on and what developments are under way is useful when it comes to assessing risks and making decisions. The NCSC has a good overview of current events and threat types thanks to reports from the public and businesses (see ch. 1.5 and 3), contacts with operators of critical infrastructure (see ch. 1.6) and a national and international network of partner organisations.

It tailors this data to specific target groups and provides various recipients with relevant information needed to raise awareness (see ch. 1.2) and take protective measures (see ch. 1.3 and 1.5).

Recommendations:

Consult past semi-annual reports and visit the NCSC website regularly.

You can also check out other websites such as cybercrimepolice.ch (in German) and "eBanking – but secure!" (ebas.ch) for details of the latest phenomena, threats and protective measures.

[1] National Cyber Security Centre, cf. Finland: NCSC-FI (kyberturvallisuuskeskus.fi); Ireland: National Cyber Security Centre (ncsc.gov.ie); Latvia: National Cyber Security Centre (nksc.lt); Netherlands: National Cyber Security Centre (ncsc.nl), Norway: Norwegian National Cyber Security Centre (nsm.no) and United Kingdom: National Cyber Security Centre (ncsc.gov.uk). Some countries have their own specific names for the relevant bodies, such as Germany: BSI – Federal Office for Information Security (bsi.bund.de); France: ANSSI – French Cybersecurity Agency (cyber.gouv.fr) and the United States: Cybersecurity & Infrastructure Security Agency – America's Cyber Defense Agency (cisa.gov). Australia and Canada emphasise the country name in the title: Australian Cyber Security Centre (ACSC) (cyber.gov.au) and Canadian Centre for Cyber Security (CCCS) (cyber.gc.ca). See also Centre for Cybersecurity Belgium (belgium.be) and Cyber Security Agency of Singapore (csa.gov.sg).

1.2 Awareness

Awareness-raising and prevention measures are fundamental to cybersecurity, as dealing with a cyberincident is much more complex and extensive than taking a few simple steps that allow everyone to operate safely in the digital space. With this in mind, the NCSC publishes information on cybersecurity and recommended measures to prevent cyberattacks. For the National Cyberstrategy (NCS), it worked with representatives from business, public authorities, educational institutions and the public to develop approaches on informing and raising awareness about the issue. It also produces recommendations aimed at specific target groups, enabling the individuals and organisations concerned to take proactive measures to protect themselves.

To fulfil this remit in line with requirements, the NCSC can draw on its own findings from its operational activities, while also coordinating efforts to bolster cyber-resilience nationwide. It designs measures in close cooperation with external partners such as Swiss Crime Prevention, the "eBanking – but secure!" platform run by the Lucerne University of Applied Sciences and Arts, the Swiss Internet Security Alliance and other bodies and organisations. These measures and recommendations can be implemented by the defined target groups, which together make up the public, on their own responsibility and based on how affected they are by the issues concerned.

For example, some pilot projects are carried out in the private sector, such as the logistics industry, the metalworking industry or family businesses. Ideally, the resulting findings are then discussed with the relevant industry associations, developed further and made available to the respective economic sectors. Together with external partners, the NCSC mounts nationwide campaigns aimed at the population. They familiarise the general public with cybersecurity-related content and are intended to provide every user of the internet and digital devices with easy-to-use tools to protect them from cybercrime online. All efforts are continuously evaluated and reviewed with a view to optimising their implementation and effectiveness.

Recommendations:

Keep abreast of current events that could affect your cybersecurity or that of your business. You will find a large variety of information for individuals, companies, authorities and IT specialists on the websites of the NCSC, Swiss Crime Prevention (SCP), "eBanking – but secure!", the internet security platform iBarry and the prevention campaign s-u-p-e-r.ch.

Talk to employees, relatives and acquaintances about cybersecurity, data handling and cybercrime.

1.3 Providing guidance on how to stay safe and boost resilience

The Federal Office for National Economic Supply (FONES) joined forces with the NCSC and the business community to develop the ICT minimum standard, which provides companies with systematic guidance on how to organise their cybersecurity. The ICT minimum standard summarises various internationally recognised standards and sets out recommendations on

enhancing ICT resilience. The standard and the associated assessment tool are updated regularly.

Industry standards have been developed and published for various critical sectors, in collaboration with industry associations and sector representatives, the aim being to better meet sector-specific requirements. These are also essentially recommendatory in nature.

For some sectors, aspects of the ICT minimum standard are also prescribed. For example, the Swiss Federal Office of Energy (SFOE) has declared the ICT minimum standards for electricity and gas supply to be mandatory. The obligation applies to electricity from 2024 and to gas from 2025 on. Meanwhile, the Federal Office of Transport (FOT) published the Railway Cybersecurity Directive (CySec-Rail Directive) in fall 2023. The new directive describes the minimum requirements for an information security management system (ISMS), which railroad companies must set up and maintain. The CySec-Rail Directive, which will come into force on July 1, 2024, refers to the "ICT minimum standard for public transport", which has been published since 2020.[2]

For its part, the NCSC provides support in the form of instructions and recommendations on different topics such as website security,[3] protection of industrial control systems[4] and Internet of Things (IoT) devices,[5] and cooperation with IT service providers.[6]

Conclusion/recommendation:

The NCSC website offers extensive information on cybersecurity.

The ICT minimum standards and ICT minimum standards by sector developed by FONES in conjunction with the private sector serve as recommendations and points of reference to protect against threats from cyber risks.

1.4 The cyber-safe.ch label – experiences of a Vaud commune

Guest article by Kilian Cuche, member of Pomy (VD) communal council

Home to 900 residents, the commune of Pomy in the Jura-Nord Vaudois district of the canton of Vaud was awarded the Swiss Cybersecurity Label (cyber-safe.ch) at the end of 2023, after around two-and-a-half years of work. This article aims to explain the process, from performing the current status assessment through to the benefits of implementation, and to highlight the challenges and opportunities for local authorities.

2 Richtlinie zur Cybersicherheit (bav.admin.ch)

3 Measures to secure content management systems (CMS) (ncsc.admin.ch); Measures to counter DDoS attacks (ncsc.admin.ch)

4 Measures to protect industrial control systems (ICSs) (ncsc.admin.ch)

5 Security in the Internet of Things (IoT) (ncsc.admin.ch)

6 Cooperation with IT service providers (ncsc.admin.ch)

1.4.1 Journey towards cybersecurity awareness

The idea of ascertaining the current state of cybersecurity in the commune of Pomy and introducing improvements came about in 2021, following an event on cybersecurity organised by the Vaud Association of Communes (UCV). The cyber-safe.ch label was showcased at the conference, which provided us with a starting point. Of course, the whole communal council first had to be convinced to invest in cybersecurity. To this end, the association cyber-safe.ch showed us, based on an initial questionnaire, what costs we could incur in the event of a cyberattack, taking into account the scope and scale of our infrastructure and data. This report was very useful as it highlighted the cost-benefit ratio of investing in cybersecurity. The council was quickly convinced of the need for investment and started the process to obtain the label in spring 2021. The cyberattack on the commune of Rolle a few months later only strengthened our determination to enhance our own cybersecurity.

1.4.2 Process for obtaining the cyber-safe.ch label

The first step in obtaining the cyber-safe.ch label was a report based on questionnaires, phishing tests and an analysis of our IT infrastructure (scan to detect security vulnerabilities). This report determined the current state of the commune's cybersecurity and identified priority measures that had to be implemented in order to obtain the label. In other words, we were given a list of completed and outstanding items, which enabled us to draw up an action plan to prepare for certification. Then came the most important part of the work: implementing the corrective measures. From managing updates to checking backups, training users and physically securing our infrastructure, all key elements of cybersecurity were scrutinised, reviewed, adjusted and corrected. Two years later, we underwent our first audit, which identified a few remaining areas of non-compliance. We then worked on rectifying these issues and finally, after a second audit, achieved cyber-safe.ch certification.

1.4.3 Benefits, challenges and opportunities for communes

The cyber-safe.ch label was an excellent means for us to improve our cybersecurity. An external appraisal of our infrastructure, independent of our administration and IT service provider, allowed us to fully and comprehensively identify the potential for improvement. We were offered professional support, with an understanding of the challenges faced by small councils. This includes, in particular, the fact that all of our council members are "part-time" politicians with other commitments, meaning they have limited time, skills and knowledge of cybersecurity. All of this was taken into account, resulting in a solution tailored to our specific circumstances. It is also encouraging to see that several cantons are increasingly making funds available to communes to help them improve their cybersecurity. These efforts should be rolled out and coordinated nationwide.

1.4.4 Summary

Although our infrastructure is very modest, comprising two workstations, a server and a few BYOD[7] devices, the amount of work required to obtain a cybersecurity label such as cyber-

[7] BYOD stands for "bring your own device", see Bring your own device (wikipedia.org)

safe.ch should not be underestimated. Indeed, with most of the measures, the size of the infrastructure is irrelevant. However, the label's officers were able to offer us pragmatic support, adapting to our needs and the various realities on the ground. So obtaining the label is far from being "mission impossible". With sound guidance, change management for employees and the support of IT service providers, improving cybersecurity is something that all Swiss communes can do and should be part of every communal IT plan. Ultimately, it is about safeguarding our citizens' data and protecting the critical infrastructures for which communal councils are responsible.

1.5 Recording incidents and issuing recommendations to those affected

The NCSC collects reports of cyberincidents and cyberthreats. To this end, it operates a national contact point for cyberthreats, which categorises the reports received and carries out an initial analysis. This serves as a basis for taking action and carrying out further in-depth investigations. As far as possible, everyone submitting a report should receive quick, hassle-free and competent support and have their questions answered directly. They are also given recommendations on what to do next and/or referred to the relevant authorities. As the centralised, national contact point for reports and questions about cyber issues, the NCSC works closely with stakeholders from the Confederation, cantons, prosecution authorities and private partners such as service providers, as well as with international partners and organisations. It also ensures that fraudulent websites, email addresses, telephone numbers, etc. are made known to the relevant authorities so that they can take appropriate action.

Based on the reports received, the NCSC identifies the latest trends and techniques in the cyber-realm. The overview of cases derived from the reports feeds into its overall view of the current situation (see ch. 1.1). The development of these phenomena is continuously analysed so that the public and businesses can be warned if the threat increases. The data collected is an important tool for prevention and raising public awareness of cyber risks (see ch. 1.2). Insights gleaned from this can sometimes prevent future offences and thus avoid further victims.

Recommendations:

Help us to detect dangers on the internet by reporting incidents and cyberthreats to the NCSC using the reporting form: NCSC Report (ncsc.admin.ch)

1.6 Protecting and supporting critical infrastructure

Critical infrastructures are processes, systems and facilities that are essential for the functioning of the economy and the welfare of the population. The NCSC supports operators of critical infrastructure in Switzerland to help protect against cyberthreats and so minimise cyber risks. To this end, it runs a national Computer Emergency Response Team (CERT), which acts as a national centre of expertise for the technical management of cyberincidents and the technical analysis of cyberthreats.

The NCSC provides critical infrastructure operators with tools and datasets to bolster the cybersecurity of the infrastructure and its users. This includes, for example, technical information on IT infrastructures that are misused to spread malware or operate phishing websites.

1.7 Reducing vulnerabilities

Software and/or system configurations may have vulnerabilities that can be exploited by attackers to gain unauthorised access. To reduce the attack surface and prevent incidents, such vulnerabilities must be identified and quickly remedied.

The NCSC receives daily reports on IT system vulnerabilities from partners and various internal and external sources. It carefully examines this information and, after analysing the individual reports, derives the necessary measures for federal systems and external bodies. For example, the NCSC has the option of warning critical infrastructure operators about particular security vulnerabilities via its own information platform and publishing relevant security advice.

It also often informs affected companies directly by email, telephone or registered letter. In many cases, this enables vulnerabilities to be fixed promptly, in cooperation with the businesses concerned.

The NCSC is also the official contact point for reporting security vulnerabilities in Switzerland and is recognised by MITRE[8] as a CVE Numbering Authority. In this role, it ensures the coordinated publication of the vulnerabilities reported to it, which is key to preventing or minimising exploitation of these vulnerabilities.[9]

Awareness-raising measures also help to reduce the attack surface. For example, the NCSC encourages businesses, organisations and administrations in Switzerland to implement the security.txt standard,[10] thereby making an essential contribution to cybersecurity.

In order to enhance the cybersecurity of federal IT infrastructure and reduce cyber risks, the NCSC is also responsible for operating its own bug bounty programme. In conjunction with other security measures, the purpose of bug bounty programmes is to identify, document and fix any vulnerabilities in IT systems and applications in collaboration with ethical hackers.

Recommendations:

Update your installed apps and programs as soon as updates become available. If possible, activate the automatic update function.

Be mindful of the product life cycle of devices and software and replace them when the manufacturer stops issuing security updates.

For businesses: Keep an up-to-date inventory of installed hardware and software and make sure you receive information about vulnerabilities and updates.

---

8 Solving Problems for a Safer World (mitre.org)

9 NCSC now part of global network for managing IT system vulnerabilities (ncsc.admin.ch)

10 Security.txt - Include your security contact on your website (ncsc.admin.ch)

1.8 Prosecuting cybercrime

Guest article by Serdar Günal Rütsche, head of the Digital Crime Investigation Support Network (NEDIK)

Ransomware is currently by far the biggest cybercrime threat facing Switzerland. Although we are actually very well protected in this country, all organisations and individuals that use online services are potential targets for such attacks. While digitalisation opens up new growth and employment opportunities for the economy, it also requires new processes and leads to greater dependence on functioning information and communication technology. Criminals take advantage of these dependencies, and are using increasingly sophisticated methods to gain access to networks, steal data or paralyse entire systems. From small craft businesses to large corporations, a cyberattack can pose an existential threat to companies.

The number of reported cybercrime and digital offences rose sharply in 2023, with economic cybercrime in particular seeing significant growth. Threats in cyberspace are among the most sizeable risks facing companies, public authorities, individuals and critical infrastructures. Technological progress in the area of artificial intelligence (AI) is opening up new attack vectors for criminals. These can be used for a variety of applications, making their job easier. The Digital Crime Investigation Support Network (NEDIK) brings together Swiss police forces to jointly combat digital and cybercrime. NEDIK coordinates case handling, ensures prompt exchange of information, compiles current and national cyber case overviews, shares knowledge, develops intercantonal projects and cooperates with relevant national and international partners to this end. All police forces play a part in this. Having an interdisciplinary platform of this kind means that phenomena and threats can be detected and counteracted at an early stage. Active collaboration, the establishment of new cooperation partnerships and operational prevention work aim to curb crime in the digital space and protect the Swiss population. In 2023, NEDIK supported projects in priority areas such as online investment fraud, paedophile crime and expanding cooperation with civil market leaders.

In the years ahead, a lot will change in the realm of cybercrime. Ransomware will remain a major threat for Switzerland, and we must therefore continue to work on raising public awareness. AI will significantly change the threat situation. By enabling new means of attack such as voice cloning and deepfakes, it will massively expand the capabilities of cybercriminals. While AI alone cannot create a completely new cyberthreat from existing malware, a combination of AI and human intelligence has the potential to do so. In addition, fraud offences will become more sophisticated and tailored through the use of AI. To protect ourselves from these threats, we will continue to need highly specialised security teams and to exercise care in our handling of data. To this end, appropriate budgets must be made available, training places created in Switzerland and the legal framework improved. IT security is not just a matter of technology: It is a collective responsibility requiring mandatory cooperation.

2 Reports from businesses and the public

2.1 Reports received on cyberincidents – overview

The total number of reports received by the NCSC rose again in 2023. At 49,380, the figure was significantly up on the previous year (34,527 reports). The year-on-year increase in the second half of 2023 was even more pronounced. While 16,951 reports were received in the second half of 2022, this climbed to 30,331 in the period under review. This near doubling was mainly due to an increase in two phenomena: “fraudulent job offers”[11] and “fake calls in the name of the police”[12].

The ratio of reports from the general public (88%) to those from companies, associations and authorities (12%) remained stable. The second half of the year saw a slight rise in fraud offences typically reported by companies, namely CEO fraud[13] and business email compromise.[14] Reports of CEO fraud in the second half of 2023 stood at 253, up from 190 in the same period in 2022, while reports of business email compromise rose from 45 to 63. There was a slight drop in the number of reports in regard to ransomware attacks[15] on businesses in the second half of the year. The NCSC received 54 such reports in the second half of 2022, compared with 42 in the period under review. Reports of ransomware attacks on private individuals fell sharply, down from 22 to 3 year on year.

11 Fraudulent job offers (ncsc.admin.ch)
12 Calls in the name of fake authorities (police, duty) (ncsc.admin.ch)
13 CEO fraud (ncsc.admin.ch)
14 Business Email Compromise (ncsc.admin.ch)
15 Ransomware (ncsc.admin.ch)

Reports to the NCSC in the second half of 2023 (per week)

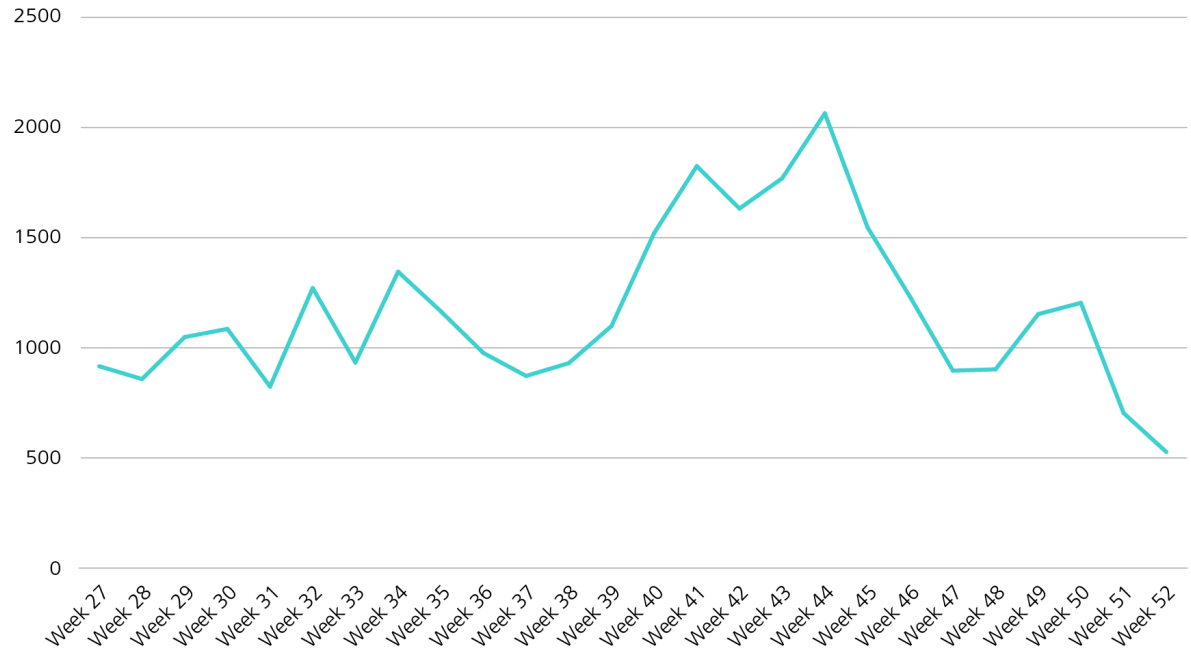

Fig. 1: Number of reports received per week by the NCSC from July to December 2023, see also Current figures (ncsc.admin.ch).

Reports to the NCSC in the second half of 2023 (by category)

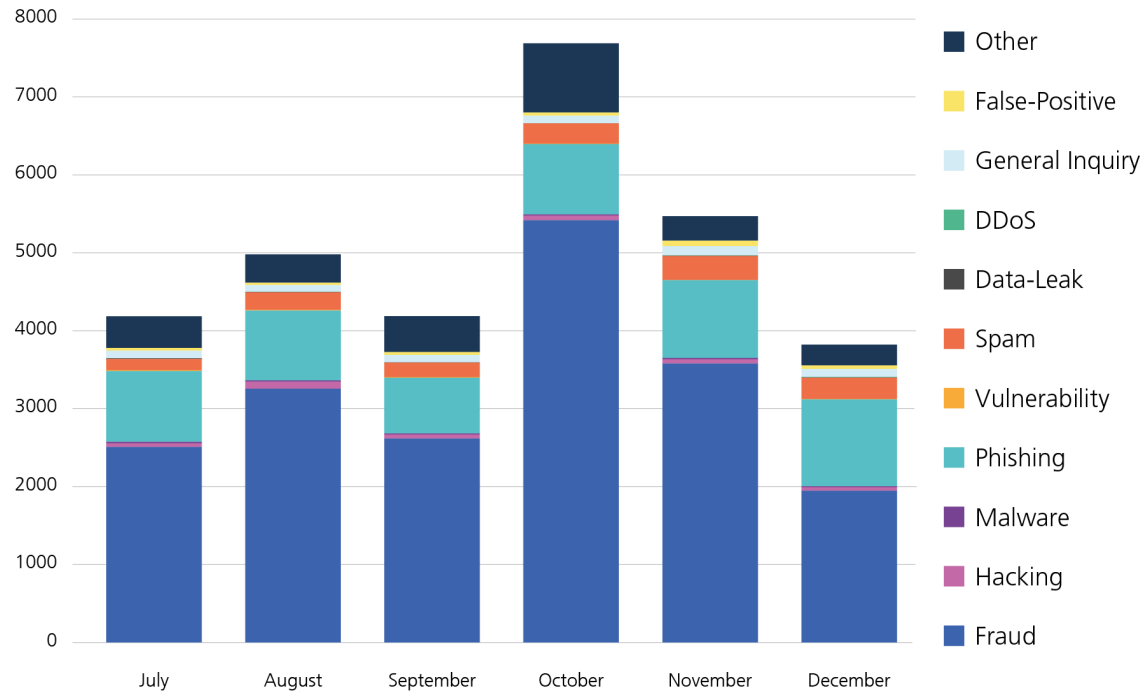

Fig. 2: Reports to the NCSC in the second half of 2023 by category, see also Current figures (ncsc.admin.ch).

2.2 Fraud

2.2.1 Fraud still the leading cause of reports

Fraud remained by far the most frequently reported phenomenon in 2023, accounting for over 30,000 reports. The rise in the second half of the year was particularly striking. Compared with the second half of 2022, the number of fraud reports almost doubled, from 10,503 to 19,323. As in the previous year, threatening emails claiming to be from law enforcement authorities accounted for a large proportion of these reports, with 4,461 such reports received in the second half of 2023. These threatening emails claim that the person contacted has been found guilty of serious misconduct (usually linked to child pornography) and that the charges can only be dropped if money is transferred.[16]

A change of tactics came to the fore in the second half of the year, leading to an increase in the number of reports received. This variant starts with a phone call apparently from the police. A computer-generated voice informs the victim that their personal banking data, for example, is connected with a crime. For further information, the call recipient should press 1. If the victim presses 1, they are connected to an “employee” and told to download a remote access tool and grant the attacker access to their computer or mobile phone. The attackers attempt to gain access to the victim’s e-banking account in this way and issue payments in the background via the remote access tool. Reports regarding this phenomenon skyrocketed in the second half of 2023, and peaked in calendar week 44, when the NCSC received a record 2,059 reports, around half of which (914) concerned threatening calls.[17]

The second half of the year also saw an increase in reports of fake job offers. Purportedly from recruitment agencies, they were mainly sent via WhatsApp and lured applicants with promises of exceptionally high earnings. The “employees” received a list of assignments via an online platform, e.g. writing online reviews. A certain amount was paid for each review, which was credited to the employee’s account via the platform. However, the number of available assignments quickly dropped to zero. In order to speed up the process and avoid having to wait for new assignments, the platform offered the option of generating new assignments for a fee: for example, 50 new review assignments could be purchased for a few dollars. The promised profit, which in turn was to be credited to the platform, far exceeded the cost, which supposedly made this model worthwhile for the victim. The rude awakening came when the victim wanted to cash out their accrued earnings. In order to receive the salary, the platform operator demanded fees for as long as it took for the victim to realise that it was a scam.[18]

2.2.2 First fraud attempts using AI

Artificial intelligence (AI) has become a hot topic over the past year, garnering widespread public attention thanks to ChatGPT, among other developments. Like any technology, it can be used for good but also has the potential to cause harm. It is therefore no surprise that cybercriminals should seek to harness AI for their own purposes. However, based on the re-

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

17 Week 43: Company-like structures among fake support scammers (ncsc.admin.ch)

18 Week 35: Fake job offers 2.0 (ncsc.admin.ch)

ported cases, the NCSC assumes that AI is not yet being systematically deployed by cybercriminals. Rather, the fraudsters are testing the waters to find out what is possible and profitable.[19]

2.2.2.1 Sextortion with AI-generated images

Sextortion is an extortion method in which victims are blackmailed with pictures and video material showing them performing sexual acts and/or naked. They have previously been contacted on social media by an attractive woman or man and lured into undressing in front of the camera. All these actions are secretly recorded. The perpetrators then threaten to publish the footage on YouTube together with the victim's name or email it to their family members, friends or employer.[20]

The NCSC is also aware of a number of cases where fraudsters have used AI to create compromising photos or videos in order to blackmail victims. All they need is a harmless video or photo that they have previously taken themselves or that is publicly available online. The AI then creates pornographic videos or nude images from these innocuous videos/photos. The potential inherent in this was brought home by the Taylor Swift deepfake pornography controversy.[21] The NCSC expects this form of extortion to increase significantly in the coming years. However, this cloud also has a silver lining. Since such fake videos can be created of practically anyone who has photos and videos of themselves online, this is likely to lead to a blunting effect which could also mitigate the threat in cases where genuine compromising videos exist.

2.2.2.2 Telephone calls

Most fraud attempts are still made in writing via email or messenger services. Only a small proportion takes place by phone. While written communication gives the scammers time to translate their phrases into the respective national language using DeepL or similar technology, a telephone call requires them to speak the language and respond to the other person in real time. In the future, AI is also likely to play a role here by simultaneously translating telephone conversations using a predefined voice and language. There are already some initial signs of AI being used in phone calls. Several businesses have reported incidents to the NCSC where people sounding like employees have called them to glean internal company data or to initiate payments. However, the employee concerned had no knowledge of these calls. These calls are probably generated by deepfake technology. There are also cases where parents are rung up by someone sounding like their children, claiming that they have had an accident. However, the extent to which AI is already involved in this remains unclear.

2.2.2.3 Communication in Swiss German

Phishing emails in Swiss German also crop up occasionally. The NCSC reported on this in the previous six-month period.[22] AI may also be behind these emails. However, this approach is surprising, given that High German is the norm in the business world. A supposedly official

---

19 Week 49: Use of artificial intelligence in fraud attempts (ncsc.admin.ch)

20 Sextortion (ncsc.admin.ch); Swiss Crime Prevention | Sextortion (skppsc.ch)

21 Deepfake-Pornos: Ein manipuliertes Video kann ein Leben ruinieren (srf.ch)

22 Week 14: Phishing in Swiss German and an invoice from Schweizerische Rettungsfahrtwacht (imitation of Swiss Air-Rescue) (ncsc.admin.ch)

email in dialect from a bank would probably make victims suspicious rather than convince them to click on the link in question. This was therefore probably a case of attackers testing the waters. However, there is another area in which dialect is commonly used for communication. In the last half-year period, the NCSC observed several cases involving communication in dialect, particularly in connection with classified ad scams. This creates trust in the victim, as the seller and buyer appear to come from the same (language) region. Presumably AI is also used in such cases.

2.2.2.4 Celebrity investment fraud

In online investment scams, images of celebrities are often used to give the dubious offers a veneer of credibility. As well as using publicly available images or videos, other tactics include generating deepfake videos. One example was the deepfake video of Elon Musk coinciding with the launch of the Starship space vehicle. The fraudsters used the launch of the vehicle by Musk's company SpaceX as an opportunity to advertise a giveaway scam. In a video on a website, "Musk" promised to double and return any cryptocurrency amounts transferred to him.[23]

Conclusions/recommendations:

Using AI applications, cyberactors can create content for credible-looking emails and text messages that are deceptively similar in language and presentation to a legitimate communication and are now virtually indistinguishable from the work of a linguistically adept human being. This makes it difficult for the recipients to spot it as a scam.

AI can also be used to create deceptively realistic photos and videos as well as real-sounding voices (deepfakes). These can be leveraged for social engineering attacks. Voice imitations can convince the target that they are talking to someone they know, who needs money or other assistance.

Fraudsters are constantly devising new scenarios to encourage victims to react rashly. Using AI-generated content and social engineering, they aim to get the victims to perform actions guided by the perpetrators, without arousing suspicion. Therefore, make sure not to be caught off guard. Think about the situation calmly and, if in doubt, ask other people or the NCSC for a second opinion.

[23] Week 17: Advertisement using a deepfake video for a giveaway scam (ncsc.admin.ch)

2.3 Phishing reports

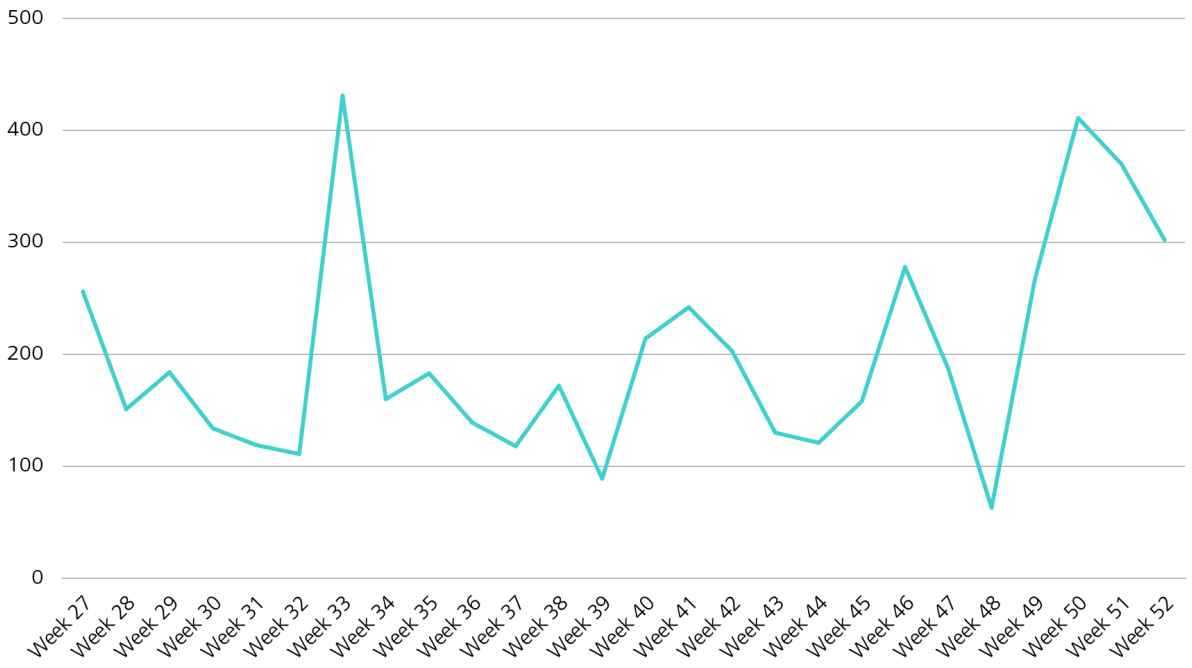

Fig. 3: Number of phishing URLs checked and confirmed by the NCSC per week in the second half of 2023.

2.3.1 Chain phishing, parcel post phishing and twice-paid bills

Phishing was once again the second most common phenomenon reported via the reporting form after fraud. Compared with the same period the previous year, the number of phishing reports more than doubled, rising from 2,179 to 5,536 in the second half of 2023. Across the year as a whole, the NCSC received 9,415 reports of phishing in this way. The NCSC also gets phishing reports via the platform antiphishing.ch. These are then processed in a semi-automated way.[24]

The vast majority of phishing attacks involve widely distributed messages sent out en masse. Often integrating numerous errors, they are cheap and easy to disseminate. They typically feature an impersonal salutation such as “Dear customer” or even just the email address.

The most frequently reported phishing attempts remained unchanged from the previous year. Thousands of fake parcel notifications are still being sent.[25] Bogus refund emails supposedly from providers, SBB or the tax authorities are also part of the standard repertoire of phishers.[26] The attackers primarily exploit the high likelihood that someone is actually expecting a parcel or has paid a bill issued by a provider, etc. This makes the email more plausible.

On the other hand, the NCSC has seen an increase in phishing attacks targeting businesses. The pressure on access credentials for company emails and Office 365 accounts in particular

---

[24] See also the Anti-Phishing Report 2023 (ncsc.admin.ch).

[25] Parcel subcription scam (ncsc.admin.ch); Week 23: How a phishing attempt turns into a subscription scam (ncsc.admin.ch); see also the Anti-Phishing Report 2023 (ncsc.admin.ch)

[26] Week 46: Phishing involving a purported tax refund and crypto wallet phishing (ncsc.admin.ch); Week 41: Office 365 and SBB phishing – variations on a theme (ncsc.admin.ch)

continued to augment. More and more phishing attempts based on the snowball principle were observed. This involves hacking into a company email account and then sending a phishing email, supposedly from the victim, to all contacts that the attackers find in the hacked account. This can amount to several thousand contacts, especially if the employee is customer-facing. As the sender is known to the recipient in these cases, the recipient is more likely to believe the content and fall for the phishing attempt. If they get compromised, their contacts are targeted and the game starts all over again. This approach is also known as “chain phishing”.

2.3.2 The renaissance of voice phishing

Voice phishing still only accounts for a small proportion of phishing reports. However, as the calls are highly targeted and the caller also responds to the victim, the chances of success are likely to be many times greater. This undoubtedly explains why the phishers take this extra effort.

Towards the end of 2023, there were more and more reports of calls from supposed bank employees claiming that they wanted to block a fraudulent payment. In some cases, the telephone number displayed even matched the bank’s official number, having been spoofed (i.e. falsified) by the fraudsters to appear credible. In many cases, the caller claimed, for example, that an amount had been debited for a flat screen purchased from an electronics retailer. They recommended calling the cantonal police fraud division immediately, and provided the relevant telephone number. This one of course also belonged to the phishers.

However, what seems plausible at first glance is actually not even possible. Although the bank can see the amounts debited in its system, it does not know anything about the products or services purchased by the client. This means that a bank generally has no way of knowing what a client has bought.

The callers usually pretend to be employees of major banks. With big banks, it is more likely that the person being called actually has an account with the bank the fraudster claims to be from. But even if they fail to guess the right bank when making the call, the scammers have found a workaround. During the phone call, they try to find out which bank the victim is actually with, and then ring up again a short time later, but this time posing as the “correct” bank.

As reports to the NCSC show, the attackers also use publicly available information. In one case, for example, the victim was called by an alleged bank employee and asked whether he had actually transferred a large sum in the last few days. Amazingly, the alleged recipient was known to the victim from a previous job. An internet search by the NCSC revealed that the name and telephone number of both the victim and the supposed recipient were contained in a public presentation that they had given together. This highlights that attackers are systematically combing the internet for such information, which they can then use for targeted social engineering attacks. Until recently, this approach had mainly been observed in connection with CEO fraud, but it now appears to be widening to include voice phishing too.

2.4 Malware and hacking reports

2.4.1 Ransomware

An increase of reports was not observed for all phenomena. Especially in the ransomware category, the statistics show a significant decrease in number on 2022. With around 109 reports received, there was a drop of almost 40 reports year on year. However, the decline mainly concerned individuals rather than companies. Only 11 reports relating to individuals were received in 2023, compared with 56 the year before. Home network-attached storage (NAS) systems, which are a particular target concerning individuals, have only occasionally been attacked. This may be partly because there was no serious vulnerability in 2023, and partly because such attacks are less likely to be enough lucrative.

The downward trend in the number of reports concerning ransomware at companies was much more moderate, with the number of reports received remaining more or less at the previous year's level, i.e. 98 versus 103 reports. It should be noted that the attacks are now almost always accompanied by a data leak, which further increases the extent of the damage (see ch. 3.3 on ransomware).

LockBit ransomware remained particularly active. Other reported ransomware families include Play, MedusaLocker, BlackCat/ALPHV, Phobos, BlackByte, Black Basta, Babuk, eCh0raix and Akira.

Recommendations:

On the NCSC website, you will find a list of preventive measures to protect against ransomware as well as guidance on what to do in the event of an incident.

2.4.2 Hacking reports

2023 also saw an increase in hacking. Compared with the second half of 2022, the number of reports rose from 276 to 351 in the period under review. Social media accounts came under particular pressure, with a total of 186 reports in this category received by the NCSC (up 78). Here, attackers are increasingly focusing on business accounts that are linked to a credit card. They can then use this account to place adverts, e.g. for dubious offers, at the victim's expense. In addition to the damage caused by the loss of the social media account, the financial loss can amount to several thousand Swiss francs.

2.4.3 Hotels in the firing line

The second half of 2023 saw a particular focus on hotels, their customers and specifically, in this context, the platform booking.com. Back in early 2023, the NCSC warned about incidents in which a bogus receptionist contacted a hotel guest in order to obtain credit card details.[27] The attackers knew all the booking details and used this information to convince the person that the request really was from the hotel. At the time, it was suspected that the attackers were able to gain access to the hotel's booking.com account.

[27] Week 4: Malware in hotels: booking data used for fraud against hotel guests (ncsc.admin.ch)

The second half of the year produced further evidence of how the attackers obtain data to access portals such as booking.com. Various social engineering methods are being used to trick hotel staff into clicking on a link and installing malware.

In one variant, it is claimed that a guest is currently being blackmailed with pornographic images that were allegedly taken in the hotel room. The guest gives the hotel two days to clarify the facts and name the perpetrator, otherwise the hotel will make itself an accomplice. All of the documentation relating to the case has been archived as evidence and the relevant file can be downloaded from the link provided. Clicking on the link downloads malware that records all the access data entered by the victim and sends it to the attackers. This allows the perpetrators to access the hotel's current bookings via online platforms such as booking.com.[28]

As well as emails with malware attached, there are also ordinary phishing emails in circulation that are aimed directly at hotel staff. Also in this case, the aim is to trick the employee into revealing booking.com access details.

Recommendations:

Hotels in particular have to open many documents sent by guests. However, executable files must not be opened under any circumstances. Consider a strategy in which computers for guest-related communications are separated from the rest of the network (network segmentation). Always keep systems up to date.

3 Situation

3.1 Initial access using malware (Trojans)

Trojans belong to the category of malware that allows access to a victim's system by inserting a backdoor. They are often installed after users have been tricked, for example, by integrating the malicious code into another program or hiding it in some other way. This type of malware is regularly distributed by email, either as an attachment or via a link. The context of the email is also used to trick the user into unwittingly executing the malicious code. To make the malicious email look more legitimate, some attackers use previous email correspondence that they have fraudulently obtained. This approach was particularly observed with operators of Qakbot, a malware used as an initial access tool that regularly resulted in ransomware infections. However, Qakbot activity declined dramatically in the second half of 2023 following a multinational operation targeting Qakbot-infected systems and the infrastructure used by the malware operators.[29] Despite the takedown, the criminal actors responsible were able to continue their activities in an adapted form. After Qakbot's takedown, malware campaigns using PikaBot and DarkGate malware were increasingly observed. These have several similarities with Qakbot activity, including the use of previous email correspondence and the deployment of some of

[28] Week 47: Cybercriminals target hotels (ncsc.admin.ch)

[29] Qakbot Malware Disrupted in International Cyber Takedown (justice.gov)

the same infrastructure.[30] However, new distribution channels were also added, such as instant messaging software for professional use (e.g. Microsoft Teams and Skype) and fraudulent search engine advertising (malvertising).[31]

Conclusion/recommendation:

Do not open any attachments or click on links in suspicious emails. If in doubt, check with the alleged sender whether the email is really from them.

When searching for software on the internet, check that you are on the manufacturer's website or another trustworthy website (e.g. a well-known computer magazine) before downloading it.

Be wary whenever a download window pops up.

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

Do not insert unknown or found USB devices into your computer.

3.2 Vulnerabilities: Ivanti CVE-2023-35078 and CVE-2023-35081

Ivanti is a provider of unified endpoint management, zero-trust security and service management solutions, giving organisations centralised control to protect and maintain their devices. Over 40,000 companies worldwide rely on this manufacturer's products.

A vulnerability was discovered in Ivanti Endpoint Manager Mobile (EPMM), formerly known as MobileIron Core, in summer 2023. The manufacturer informed its customers on 24 July 2023 and provided a patch for installation.[32] This vulnerability was reported as number CVE-2023-35078 and impacted all product versions supported at that time, namely 11.10, 11.9 and 11.8. Older versions that had not been supported for some time were also affected.

The critical vulnerability with a maximum CVSS[33] score of 10.0 allows an unauthenticated attacker from the internet to access certain API[34] paths. This may enable personally identifiable information (PII) such as names, phone numbers and other mobile device details to be viewed. An attacker could also make configuration changes and create an EPMM administrator account. This in turn opens up other, more far-reaching possibilities for an intruder to manipulate the vulnerable system.

As is often the case, the vulnerability had already been exploited by the time the details were published. For example, the Norwegian National Security Authority informed the public on

---

30 Week 42: Dynamite phishing – DarkGate follows Emotet and Qakbot (ncsc.admin.ch);
Are DarkGate and PikaBot the New QakBot? (cofense.com)

31 PikaBot distributed via malicious search ads (malwarebytes.com);
Microsoft Teams used to deliver DarkGate Loader malware (malwarebytes.com)

32 CVE-2023-35078 - New Ivanti EPMM Vulnerability (ivanti.com)

33 The Common Vulnerability Scoring System (CVSS) is an industry standard for assessing the severity of potential or actual security vulnerabilities in computer systems. See Common Vulnerability Scoring System (wikipedia.org).

34 An API (application programming interface) is a programme component made available by a software system to other programs for connection to the system. See API (wikipedia.org).

24 July 2023 that there was evidence that the vulnerability had been used for an attack on Norwegian ministries.[35] The manufacturer Ivanti also stated in its advisory that it was aware of a limited number of customers that had already fallen victim to such an attack.

While many affected organisations were still busy fixing CVE-2023-35078, the next vulnerability in EPMM was announced just a few days later, on 28 July 2023, with the identifier CVE-2023-35081.[36] This was detected during investigations into CVE-2023-35078. Once again, the manufacturer provided information and patches to fix the vulnerability.

The second vulnerability was slightly less critical than its predecessor, with a CVSS score of 7.2. Nevertheless, it would enable an authenticated administrator to install malicious files on EPMM servers (arbitrary file write). If exploited in conjunction with CVE-2023-35078, this vulnerability would allow administrator authentication and ACL[37] restrictions to be completely bypassed. As with the first vulnerability detected, this vulnerability affected all product versions supported at the time of publication as well as older versions that had not been supported for some time.

The manufacturer Ivanti also confirmed on its website that the attack complexity for CVE-2023-35081 had been proven to be reduced for an intruder if a system operator had not yet fixed the first published vulnerability CVE-2023-35078 on an affected system.

The NCSC actively warned critical infrastructure operators and many other Swiss organisations about both vulnerabilities. Based on technical analyses by the NCSC, potentially affected companies were also personally informed and specific recommendations for action were issued. Despite the high criticality of both vulnerabilities, the number of confirmed Swiss victims is relatively small.

Conclusion/recommendations:

Multiple serious vulnerabilities for the same product being made public within just a few days is a distinct possibility, as the Ivanti case powerfully demonstrates. Time is an extremely important factor in vulnerability management. Published patches should always be installed on affected systems as soon as possible, and it is vital that the manufacturer's recommendations are followed. However, it is also essential that every organisation and business knows about its infrastructure and keeps an up-to-date inventory of the products in use.

Acting quickly to fix vulnerabilities ensures that IT systems can operate securely while also reducing an organisation's attack surface. In some cases, this can also successfully prevent an attacker from exploiting "vulnerability chaining". This is where an intruder combines multiple existing vulnerabilities to compromise a system. If a system operator continuously fixes vulnerabilities using an established vulnerability and patch management process, this makes it more difficult to the attacker and reduces the chances of a successful attack.

---

35 Nulldagssårbarhet i Ivanti Endpoint Manager (MobileIron Core) - Nasjonal sikkerhetsmyndighet (nsm.no)

36 CVE-2023-35081 - Remote Arbitrary File Write (ivanti.com)

37 An access-control list is a software technology that can be used to restrict access to data and functions. See Access-control list (wikipedia.org).

3.3 Ransomware

3.3.1 Ransomware incidents

Companies providing IT solutions for public administrations and SMEs were among those affected by ransomware attacks in the six months under review. These increasingly frequent attacks on the supply chain emphasise how important it is to introduce simple but effective preventive measures to protect against cyberattacks, to share experiences – nationally and internationally – and to communicate effectively during and after an incident.[38]

3.3.1.1 A vulnerability in the supply chain

In November 2023, the IT service provider Concevis AG, whose clients include public administrations, fell victim to a ransomware attack.[39] In response to the cyberattack, many customers temporarily suspended their use of Concevis services in order to protect their systems from possible contagion via interfaces with the service provider.

Meanwhile, cybercriminals are increasingly turning their attention to supply chains. For example, the Everest ransomware group has refocused its operations on acting as an initial access broker. In other words, it has specialised in identifying backdoors in organisations' systems and selling these access points to other cybercriminals, instead of carrying out attacks itself as before. According to the FBI,[40] this activity is based on gaining initial access to victims' IT environments through third parties. This involves exploiting vulnerabilities in remote access controlled by vendors or third-party services, and using legitimate system management tools to elevate permissions within the affected organisations.

Conclusion/recommendations:

Attacks on and incidents in its supply chain can also affect a company's own operations and cause major (consequential) damage. It is therefore essential to address cybersecurity and data protection with partners, to regulate these issues contractually and also to review them.[41]

3.3.1.2 Offline backups and regular software updates

In August 2023, the government-owned Lanka Government Network (LGN) in Sri Lanka was hit by a ransomware attack involving the encryption of LGN systems and data. Although the systems were restored within 12 hours, some of the data could not be recovered. The lack of offline backups meant that online backups had to be used, but these were also corrupted by the attack. As a result, certain data, such as emails sent and received between 17 May and

38 See NCSC's recommendations on Cyberattack – how to communicate? (ncsc.admin.ch)

39 Federal Administration also impacted by Concevis hack (ncsc.admin.ch)

40 FBI Private Industry Notification 231108.pdf (ic3.gov)

41 Supply chain security guidance (ncsc.gov.uk); ICT Supply Chain Resource Library (cisa.gov); Cooperation with IT service providers (ncsc.admin.ch)

26 August 2023, were irretrievable. The ransomware attack was successful in part because LGN was still using outdated versions of Microsoft Exchange (2013).[42]

Conclusion/recommendations:

Back up your data regularly, including on an external medium.[43]

Update your software whenever security updates are available. Anticipate the end of a software's life cycle and replace it in good time.

3.3.1.3 Careful communication required when dealing with an incident

In May 2023, Unico Data AG, a Swiss provider of IT solutions for SMEs, fell victim to a ransomware attack by the Play group, which took most of its services offline. The company responded quickly, forming a crisis team to rectify the problems caused by the attack, reporting the incident to the relevant authorities and informing affected customers. As Unico Data AG did not pay a ransom, the ransomware group published the stolen data on the dark web. Some time later, the firm's CEO commented publicly on the incident, addressing the financial impact of the attack and the human and time resources required to resolve the problem.[44] He also discussed the lessons that the company had learnt from the incident. He urged other businesses to prepare for cyberattacks, focusing on disaster recovery plans but also on communication, both internal and external, and stressed the importance of defining which information is communicated by which people via which channels.

Conclusion/recommendations:

Careful, proactive communication allows victims of cyberattacks to contextualise the incidents, inform their employees, customers, partners, the media and the public objectively and prevent speculation.

Read NCSC's recommendations on Cyberattack – how to communicate? (ncsc.admin.ch)

3.3.2 Tracking ransomware variants and actors

Ransomware groups adapt quickly to changing circumstances, whether it be new vulnerabilities, technical or personnel developments in the relevant arena, measures taken by authorities or new legal requirements. An example of the first of these is the exploitation of a new vulnerability in Atlassian's Confluence software, which was used to spread C3RB3R ransomware.[45]

---

42 Sri Lankan government loses months of data following ransomware attack (therecord.media); Crisis & Consequences: An Emerging Cyber Quandary for Sri Lanka (capsindia.org)

43 S-U-P-E-R.ch – What to bear in mind when backing up data (ncsc.admin.ch)

44 "Der Cyberangriff hat uns insgesamt weit über 1 Million Franken gekostet" (inside-it.ch)

45 C3RB3R Ransomware | Ongoing Exploitation of CVE-2023-22518 Targets Unpatched Confluence Servers (sentinelone.com)

3.3.2.1 Development of actors and their services

The period under review saw further changes in ransomware groups and their activities. These groups often change their composition, their name and the nature of their activities, sometimes merging with other groups or offering their services to them, e.g. in the form of ransomware as a service (RaaS). The ransomware market is flourishing like never before, opening up easy opportunities for even less experienced actors to create and customise malware themselves. This was the case with the LockBit 3.0 ransomware builder, for example, whose code was leaked in September 2022. Researchers from Kaspersky found 396 distinct samples containing this code.[46] The many variants of LockBit that exist make it difficult for cybersecurity researchers to attribute attacks to specific groups or individuals and track their activities. Another difficulty is the large growth in new ransomware actors and variants.[47]

The Royal group, for example, seems to have been replaced by BlackSuit. This could be a change of name or a rebrand, and/or a derived variant, as the BlackSuit malware has certain code features that are similar to those of Royal.[48]

In 2023, not only were existing variants reconfigured, but new, innovative and unique ransomware families also emerged, such as the Rhysida RaaS. This has a self-deletion mechanism and is compatible with Microsoft operating systems older than Windows 10. It was written in the C++ programming language and compiled with the MinGW development tool and shared libraries. Rhysida has been active since May 2023.[49]

3.3.2.2 Response to police action

In late 2023, the FBI led an international operation against the BlackCat/ALPHV group.[50] For several days, the group's data leak site (DLS) was labelled as "seized". Law enforcement authorities were able to recover 946 key pairs that gave them access to the perpetrators' encrypted communications with victims, sites containing stolen data and the group's partner panel. Shortly afterwards, however, the cybercriminals announced the launch of a new DLS, which immediately listed six alleged victims. Since then, the LockBit ransomware group has been trying to recruit partners and developers from BlackCat/ALPHV.

There is currently no universal decryption tool for BlackCat/ALPHV ransomware. However, some victims can recover their data using the keys that are available thanks to the police action.

3.3.2.3 Extortion techniques adapt to regulatory developments

Cybercriminals also adapt to new rules and regulations, such as the introduction of reporting obligations.

---

46 Leaked Lockbit ransomware builder analysis (securelist.com)

47 Orange Cyberdefense publishes a regular listing of different ransomware variants and actors: Map tracking ransomware, by OCD World Watch team (github.com)

48 Investigating BlackSuit Ransomware's Similarities to Royal (trendmicro.com); BlackSuit ransomware - what you need to know (tripwire.com)

49 Kaspersky crimeware report: GoPIX, Lumar, and Rhysida. (securelist.com)

50 Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant (doj.gov)

For example, the new group RansomedVC uses an extortion tactic in which it warns victims of the fine they will be hit with under data protection legislation (e.g. GDPR) if they do not pay the ransom demanded and the case is made public. The group calls its ransom demand a “digital peace tax”. Similarly, the LockBit ransomware group describes its operations as a “post-payment penetration testing” service.

3.3.2.4 Attractive sectors for cybercriminals: energy and healthcare

The energy and healthcare sectors are popular targets for ransomware actors. Both can tolerate only short downtimes due to the nature of the services provided. In the case of healthcare organisations, there is the added fact that they offer essential – and in many cases life-saving – services to patients, and increasingly rely on networked systems, electronic patient files and telemedicine. This can lead to critical infrastructure operators complying quickly with ransom demands in order to regain access to their systems.

In the incidents that occurred in the healthcare sector in the second half of 2023, patient treatment was mostly able to continue without major restrictions and the clinics’ services remained available. However, affected hospitals are deregistering from the emergency care system, possibly as a precautionary measure, which can lead to patients being redistributed to neighbouring hospitals.

In regards to incidents in the energy sector (incl. nuclear facilities and research institutions), there has been a resurgence in ransomware attacks since 2022. In many cases, such an incident impacts the IT systems and results in files being encrypted, but does not disrupt production or distribution, meaning that power supply can continue without interruption.

Recommendations:

On the NCSC website, you will find a list of preventive measures to protect against ransomware as well as guidance on what to do in the event of an incident.

3.4 Data leaks and data management

Data is the gold of the information age. Data leaks not only have far-reaching consequences for the organisations directly affected, but the stolen data can also be used for further attacks. This implies that private individuals may also be targeted by threat actors. Cybercriminals are aware of this development which is why data procurement malware (known as infostealers) and illegal data-selling platforms are becoming increasingly popular.[51] Two major leaks made the headlines in December 2023. Firstly, over Christmas, various hackers offered millions of items of sensitive personal data from data leaks around the world free of charge on the dark web.[52] Secondly, the company 23andMe, which supplies genetic tests for genealogical research, announced that the personal and genetic data of almost 7 million customers had been

[51] See Trend Micro study on data and marketplaces: Your Stolen Data for Sale (trendmicro.com)

[52] Cybercriminals launched “Leaksmas” event in the Dark Web exposing massive volumes of leaked PII and compromised data (resecurity.com)

compromised by a data leak in October 2023.[53] The attack exploited weak and reused user passwords originating from previous data leaks. This increases the risk for those affected, particularly the risk of further attacks such as account takeovers, phishing attacks, identity theft or financial fraud. These incidents once again raise the question of organisations' responsibility for adequately protecting their customers' sensitive personal data. However, individuals too have a responsibility to protect their accounts with strong security measures. People also need to be more aware of which data they are willing to share with which organisations.

Recommendations:

Only store data that you really need (data minimisation) and delete data that is no longer required or archive data offline if it is worth keeping but is no longer actively used. Protect access to accounts and data with strong passwords and, where possible, with multi-factor authentication (MFA).[54]

Note:

The fully revised Federal Act on Data Protection (FADP) came into force on 1 September 2023. Among other things, this requires any breach of data security to be reported to the Federal Data Protection and Information Commissioner (FDPIC).[55]

3.4.1 Data leaks in the healthcare sector (international)

The trend towards major data leaks in the healthcare sector continued in the second half of 2023. Globally, the healthcare sector ranks third in terms of the frequency of data leakage, particularly in English-speaking countries. In Europe, healthcare organisations are being targeted by cyberactors too.

As many threat actors are financially motivated, their specific choice of target is largely opportunistic. The healthcare sector is especially attractive to hackers based on the assumption that hospitals, health insurers and healthcare service providers are more likely to pay a ransom to prevent the publication of such sensitive personal data and the consequential damage, such as loss of trust or legal implications arising from privacy and data protection violations. The consequences for customers and patients can also be devastating. For many people, knowing that their health data could be viewed by unauthorised persons causes psychological distress. This is one of the reasons why stolen data can be used to blackmail the patients themselves (data extortion). However, it can also be used for identity theft, insurance fraud and other offences or simply be sold to third parties.

Attacks differ in complexity and form. Threat actors use various attack vectors such as phishing (see ch. 2.3) and social engineering techniques[56] or they exploit vulnerabilities in software and cloud solutions as well as attacks on third-party service providers. Attacks on the supply chain (see ch. 4.5.2 in semi-annual report 2023/1) contributed significantly to the rise in reports.

---

53 23andMe confirms hackers stole ancestry data on 6.9 million users (techcrunch.com)

54 See Protect your accounts (ncsc.admin.ch)

55 DataBreach (edoeb.admin.ch)

56 Social Engineering - the "Human Factor" (bsi.bund.de)

Some trends already described in the first half of 2023, including data leaks by the Cl0p group and attacks on software service providers, continued in the second half of the year.[57] While certain actors may combine data theft with encryption software (e.g. Hunters International[58] and BlackCat/ALPHV). Others, such as the Karakurt group, focus purely on data theft. In the past, some threat actors have said that they deliberately avoid attacking healthcare organisations because of their criticality. However, groups that sell their ransomware as a service (RaaS) and are currently among the most active players – such as LockBit or BlackCat/ALPHV – have moved away from this stance.[59]

While Swiss healthcare institutions are currently not specifically targeted by threat actors, opportunistic attacks can also affect the country's healthcare sector. A cyberattack on the digital healthcare solutions provider Medgate in August and a follow-up attack in September 2023 were successfully repelled, although they did result in short-term service interruptions.[60] Meanwhile, in October 2023, an encryption attack on Psychiatrie Baselland led to a technical systems failure lasting 12 days, although the incident was managed without serious consequences.[61] The NCSC is not aware of any data leaks in connection with these incidents.

3.4.2 Data leak at Baden town council

On 4 December 2023, a data leak was reported in Baden in the canton of Aargau.[62] Around 3 GB of the town council's data was offered for download on the hacker forum BreachForum. An in-depth analysis found that the data included names, addresses, telephone numbers, IBANs and invoices of residents, as well as details of council investments.[63]

Baden town council reacted promptly by calling in outside experts to investigate the incident, informing the public in a press release[64] and setting up a reporting form[65] for those who may have been affected. It also reported the incident to the police. According to the council's own information, in mid-October 2023, its IT services recorded an attempt by unknown persons to gain unauthorised access to the information and communication technology (ICT) servers of the towns of Aarau and Baden. However, the vulnerability was fixed immediately and further

---

57 The mass exploitation of a vulnerability in the document transfer software MOVEit began in May 2023 and has now affected the data of around 90 million people worldwide (as at December 2023), see Unpacking the MOVEit Breach: Statistics and Analysis (emsisoft.com).

58 For example, attacks on the Fred Hutchinson Cancer Center and Crystal Lake Health Centers in the United States: Hunters International ransomware gang claims to have hacked the Fred Hutch cancer center (securityaffairs.com); Ransomware gang claims to have stolen Crystal Lake Health Centers data (databreaches.net)

59 ALPHV abandoned this restriction in an announcement in December 2023, allegedly in response to repressive measures by US law enforcement: ALPHV/BlackCat Claims Healthcare Restrictions Removed for Affiliates (hipaajournal.com). LockBit attacked a US children's hospital in December 2023, despite earlier promises to the contrary: Ransomware-Bande Lockbit wirft Skrupel über Bord (inside-it.ch)

60 Press release: Cyberangriff auf Teile der IT-Infrastruktur von Medgate.pdf (medgate.ch)

61 Psychiatrie Baselland nimmt Normalbetrieb wieder auf - Psychiatrie Baselland (pbl.ch)

62 Baden ist Opfer eines Hackerangriffs geworden (nzz.ch)

63 Hackerangriff auf Baden: Meldeformular eingerichtet (badenertagblatt.ch)

64 Press release: IT-Sicherheit der Stadt Baden (baden.ch)

65 Meldestelle Datenexposition (baden.ch)

security measures introduced. The nature of the data suggests that it originated from an internal administrative system used to manage invoices to and from Baden town council.[66] There was no evidence that any other systems had been compromised.

This incident exemplifies the development of a threat actor trying to get established in the criminal world and gain credibility. The data was first published on a hacker forum by someone using the persona DragonForce. This individual was not yet an established user of the site, having only registered on the platform some days earlier. The fact that the data was made available free of charge is also unusual. Normally, this only happens in data extortion cases when the victim refuses to cooperate (see ch. 3.3) or in hack-and-leak operations by hacktivists.[67] However, the Baden town council did not receive a ransom demand[68] and DragonForce did not air any grievances. There are strong indications that the threat actor wanted to make a reputation in the criminal world. This is also supported by the fact that DragonForce set up a data leak site on the dark web in mid-December and once again listed the Baden town council as a victim, alongside other alleged victims. The list of victims spread around the world makes it clear that the actor is operating opportunistically rather than specifically targeting Swiss companies or organisations.

Conclusion/recommendations:

Essentially, the following applies: Data is valuable. Criminals therefore have an incentive to obtain it by dishonest means and sell it or to blackmail victims by threatening to publish sensitive data. Consequently, discussions around data security should move away from asking *whether* a data breach could happen to asking *when* it will happen and how the data can be rendered useless to the attacker, even in the extreme case that it is leaked. Full protection against data breaches is nearly impossible, especially in the case of very sophisticated threat actors with high levels of cyberexpertise. Hard-to-control factors such as vulnerabilities have a role to play here. Therefore, it is important to consider key principles of data security and management.

The **5Ws** of data management: Determine **who** stores and processes **which** data, in **what form, where** and **with whom** it is shared. This means in particular that a conservative approach to data storage is advisable: the less data is stored, the less data needs to be protected from unauthorised access. Data should also be reviewed regularly and unnecessary data deleted. Also check whether digital data can be archived offline.

Technical aspects are also crucial: in addition to the usual cyberhygiene measures,[69] data should be stored in encrypted form where possible.

Awareness: Regular efforts should be made to raise employees' awareness of the issue. Clear, workable processes for data handling and protection should be defined, implemented and monitored. Last but not least, everyone should be aware that information is publicly available online, whether intentionally or unintentionally. Actors with malicious intent can exploit this

[66] Stadt Baden: "Nur Rechnungsdaten betroffen" (inside-it.ch)

[67] See semi-annual report 2023/1 (ncsc.admin.ch), ch. 2.3

[68] Press release: IT-Sicherheit der Stadt Baden (baden.ch)

[69] Key issues in good cyberhygiene include: password management (e.g. hashing and salting), the principle of least privilege, network segmentation, and patch and product life-cycle management.

data for social engineering. If an incident occurs, do not let yourself be pressurised, keep calm and seek specialist assistance if necessary.

Check and review: Data from earlier breaches can be reused for subsequent attacks. Check periodically whether your credentials have been involved in a data leak, e.g. on the website Have I Been Pwned: Check if your email has been compromised in a data breach (haveibeenpwned.com) or the Hasso Plattner Institute's Identity Leak Checker (hpi.de). If possible, use several such websites. Just because your credentials do not show up on one data-breach website, it does not necessarily mean that they have not been leaked.

3.5 Industrial control systems (ICSs) and operational technology (OT)

The interconnection and digitalisation of all areas of life is advancing inexorably. This also affects the industrial environment. Integrated into digital business processes, OT-based process controls enable significant gains in efficiency and more flexible implementation. However, such an interlinkage of the physical and digital spheres also facilitates larger-scale attacks on industrial system landscapes. State actors, and increasingly also hacktivists, are targeting inadequately protected ICSs in order to manipulate processes or sow insecurity among the population concerned. However, ransomware attacks on neighbouring and insufficiently isolated IT systems remain the greatest threat to the operation of ICSs and can impair the continued operation of the entire network, at least temporarily.

3.5.1 State actors displaying greater agility on OT

While media coverage of the Russia-Ukraine War was dominated by missile attacks on Ukrainian cities and critical infrastructure, the threat actor Sandworm, which is part of the Russian military intelligence service, carried out a cybersabotage attack against a Ukrainian power supply operator on 10 October 2022. According to a November 2023 report by cybersecurity service provider Mandiant,[70] the attackers gained access to the infrastructure used for operating a microSCADA control system that controlled the OT environments of the electricity company's substations. The access was then leveraged to execute commands to switch off the substations. What made the analysed attack unusual was the method of using existing functionalities for the attack. This living-off-the-land (LOTL) approach has been observed in IT for some time and has now also found its way into the OT environment. Compared with self-developed malware,[71] such as that used in the attacks on the power supply system around Kiev in 2016, this approach enables a faster progression from gaining network access to executing the actual sabotage attack. Because the misused components are also deployed in many other system landscapes, this modus operandi can also be adapted more flexibly to other targets.

As well as attacks on the power supply system, cybersabotage attacks against Ukrainian agricultural targets were also observed, coinciding with missile attacks.[72]

---

70 Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology (mandiant.com)

71 CrashOverride Malware (cisa.gov)

72 Russian influence and cyber operations adapt for long haul and exploit war fatigue (blogs.microsoft.com)

3.5.2 Water supply disrupted by hacktivists

In the context of international conflicts such as the war in Ukraine or the escalation in the Middle East, hacktivists are liable to sabotage exposed OT devices as well as carrying out distributed denial of service (DDoS) attacks and publishing intercepted information (see also ch. 3.6). For example, the hacktivist group Cyber Av3ngers has started to attack devices made by Israeli manufacturer Unitronics.[73] Its activities have disrupted water and wastewater treatment systems in at least the United States[74] and Ireland.[75] The group is affiliated with Iran's Islamic Revolutionary Guard Corps.[76] It uses the publicity generated to spread its anti-Israeli propaganda message (see Fig. 4).

Fig. 4: Propaganda message on compromised devices.[77]

In retaliation, the Predatory Sparrow group once again disrupted the operation of petrol stations in Iran.[78] Similarly, in the context of the war in Ukraine, hacktivists such as Team OneFist and the People's Cyber Army of Russia repeatedly publish alleged documentation of attacks against ICSs on their social media channels.

Conclusion/recommendations:

Secure your industrial systems to prevent th kind of attacks described in the previous section. The NCSC suggests a number of measures to protect ICSs on its website.

---

73 Exploitation of Unitronics PLCs used in Water and Wastewater Systems (cisa.gov)

74 Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa (waterisac.org)

75 Two-day water outage in remote Irish region caused by pro-Iran hackers (therecord.media)

76 IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (cisa.gov)

77 Iranian Cyber Av3ngers Compromise Unitronics Systems (secureworks.com)

78 Iran petrol stations hit by cyberattack, oil minister says (reuters.com)

For more comprehensive guidance, see the minimum standards by sector drawn up by the Federal Office for National Economic Supply (FONES) in partnership with the relevant industry bodies.

A useful tool to check whether your own security measures are sufficient for current threats in the industrial environment is MITRE's EMB3D framework.

3.5.3 IoT devices misappropriated as attack infrastructure

The misuse of devices as attack infrastructure against other targets is even more common than attacks on OT-controlled processes or the devices themselves. This applies particularly to (I)IoT[79] devices such as routers, cameras and alike that are poorly protected or at the end of their service life. In November 2023, Danish cybersecurity centre SektorCERT[80] published an analysis of a series of compromises of Zyxel routers belonging to its member organisations in the energy supply sector in May 2023. Vulnerabilities in these devices were immediately exploited by multiple actors, for example to integrate them into botnets, enabling subsequent DDoS attacks against other exposed targets on the internet, such as websites. Several Zyxel routers were also compromised in Switzerland. The NCSC notified the operators of these routers so that the devices could be cleaned.

Apart from this, old Cisco and Netgear devices were also exploited to develop the KV-botnet[81] attributed to the threat actor Volt Typhoon. Volt Typhoon has been linked to reconnaissance attacks on critical infrastructure in the United States.

The EU has introduced the Cyber Resilience Act[82] to make the misuse of such devices less probable in the future. The new law introduces EU-wide cybersecurity requirements for the design, development, production and provision of hardware and software products on the market. The regulation will apply to all products that are connected either directly or indirectly to another device or to a network.

Conclusion/recommendations:

As well as actual network devices such as routers, many other electronic devices at home are now networked and constantly online. These devices must also be adequately secured, and updated if vulnerabilities are detected.[83]

79 Internet der Dinge (wikipedia.org); Industrial internet of things (wikipedia.org)

80 The-attack-against-Danish-critical-infrastructure.pdf (sektorcert.dk)

81 Routers Roasting on an Open Firewall: the KV-botnet Investigation (blog.lumen.com)

82 Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products (consilium.europa.eu)

83 Cybertip: Things to watch out for in the Internet of Things (ncsc.admin.ch); Security in the Internet of Things (IoT) (ncsc.admin.ch)

3.6 Cyber in conflicts

Alongside an overview of key events in cyberspace linked to the Russia-Ukraine War, the last semi-annual report noted that there were no signs of a decline in malicious activity and an increased risk of collateral damage in connection with hacktivist groups wanting to carry out destructive attacks.[84] Both forecasts proved accurate, as attested by the main developments in conflicts in the second half of 2023.

3.6.1 War in Ukraine

In the context of the war in Ukraine, malicious cyberactivity continued at an increasing rate in the second half of 2023. Ukraine's Computer Emergency Response Team (CERT), for example, reported that it dealt with a total of 2,543 incidents in 2023, 15% more than in 2022, including malware dissemination, phishing, and account and system compromise.[85] Public administration, defence, energy supply and telecommunications were among the most targeted sectors. Ukraine also reported on Russia's increasing efforts to wage espionage campaigns against Ukrainian authorities investigating possible Russian war crimes. In addition, it recorded repeated attempts to hit targets that had already been attacked in the past.[86] A new approach by Ukrainian authorities is to officially disclose the results of cybercampaigns. In November 2023, for example, the Ukrainian military intelligence service reported that it had obtained numerous confidential documents from the Russian Federal Air Transport Agency through a complex cyberoperation.[87] However, the most notable incident during this period was one targeting Ukraine. On 12 December 2023, Ukraine's largest telecommunications provider Kyivstar, which supplies mobile and internet services to over half of the country's population, was hit by a cyberincident. The attack disrupted services for Kyivstar users, as well as services hosted by Kyivstar. This resulted, for example, in restricted access to financial services for some of the population, and air raid warnings no longer being received. Services were partially restored on the evening of 13 December 2023, but it took more than a week for all services to be available again.[88] The hacktivist groups Killnet and Solntsepek claimed responsibility for the attack. Killnet provided no evidence and had previously boasted about incidents for which it was not responsible. Solntsepek, on the other hand, published screenshots showing privileged access to Kyivstar's systems. According to Ukraine and various Western IT security companies, the Sandworm group, which is linked to the Russian military intelligence service and has already targeted telecommunications companies in the past, was actually behind the attack and was using Solntsepek as a front.[89] The incident is said to have been a combination of DDoS attacks and the deployment of data erasure malware (wipers). Solntsepek claims to have "destroyed" more than 10,000 computers and 4,000 Kyivstar servers, including all cloud storage and backup systems. Preliminary attempts had already been made to penetrate the organisation's systems in March 2023. In May 2023, the attackers finally succeeded in gaining initial access

---

84 See semi-annual report 2023/1 (ncsc.admin.ch), ch. 4.7

85 The CERT-UA Team has processed 2,543 cyber incidents over 2023 (cip.gov.ua)

86 How russian government-controlled hacking groups shift their tactics, objectives and capacities (cip.gov.ua)

87 Defence Intelligence of Ukraine conducted a cyber operation against Rosaviatsia (gur.gov.ua)

88 NetBlocks on X: Metrics show that connectivity on Ukraine telco Kyivstar is now largely restored (twitter.com); Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

89 Hacker Group Linked to Russian Military Claims Credit for Cyberattack on Kyivstar (wired.com); Russia's Sandworm blamed for Kyivstar telecom cyberattack (theregister.com)

by compromising the account of a Kyivstar employee and propagating through the systems.[90] This access, which went undetected for months, would have made it possible, among other things, to obtain customer information, locate mobile phones, intercept text messages and compromise internet accounts (e.g. Telegram) protected by authentication linked to a mobile phone number.

While Switzerland is highly unlikely to be the target of similar sabotage attacks by state actors, it is likely to be targeted by hacktivist groups involved in a conflict. By way of example, the pro-Russian hacktivist group NoName057(16) carried out DDoS attacks on Swiss websites five times in the second half of 2023, having previously conducted a campaign of such attacks on Swiss websites in June 2023.[91] These attacks were mainly in response to Swiss actions in connection with the war in Ukraine. For example, on 28 November – three days after the Swiss president's visit to Ukraine – NoName057(16) attacked websites of the Federal Administration and organisations active in the financial sector and tourism. Although these attacks had only a minor impact (there was no significant curtailment of availability), they are nonetheless used by hacktivist groups for propaganda purposes.[92] In contrast to previous campaigns, NoName057(16) no longer attacks websites from the same country continuously over the course of a week, but changes its focus from day to day.

3.6.2 Middle East conflict

Following the attack by Hamas on Israel on 7 October 2023, which led to a renewed escalation of violence in the region, numerous hacktivist groups announced their involvement in the conflict. The hacktivism in this conflict bears many similarities to that of the Russia-Ukraine War. Much of the activity of these hacktivist groups is concerned with propaganda and/or disinformation. Only a relatively small number of hacktivists have carried out actions in cyberspace with a direct impact on computer systems. These actions mainly involved website defacement and DDoS attacks and were also observed against targets outside the conflict zone, mostly in response to declarations of support for one of the protagonists.[93] However, a number of hacktivist groups carried out more sophisticated and damaging actions. The Cyber Toufan group, for instance, is said to have compromised more than a hundred Israeli organisations, publishing sensitive data after disrupting the organisations' infrastructure using "wipers".[94] The Karma group is also said to have infiltrated several Israeli organisations to deploy a unique wiper that has one version for Windows and another for Linux systems.[95] The Cyber Av3ngers group targeted Israeli-made industrial control systems, defacing their user interface to render them unusable. The systems were targeted irrespective of their location, triggering incidents in various countries outside of the conflict zone.[96] Some of these groups are suspected to be a front

---

90 CEO of Ukraine's largest telecom operator describes Russian cyberattack that wiped thousands of computers (therecord.media); Exclusive: Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

91 See semi-annual report 2023/1 (ncsc.admin.ch), ch. 2.1
Detailed analysis report on the DDoS attacks 'NoName057(16)' (ncsc.admin.ch)

92 Ukraine-Krieg: Russische Hackergruppe schürt in der Schweiz Verunsicherung (nzz.ch)

93 Hacktivist Involvement in Israel-Hamas War Reflects Possible Shift in Threat Actor Focus (securityscorecard.com)

94 Cyber Toufan goes Oprah mode, with free Linux system wipes of over 100 organisations (doublepulsar.com)

95 Mission "Data Destruction": A Large-scale Data-Wiping Campaign Targeting Israel (securityjoes.com)

96 See ch. 3.5.2

for, or backed by, state actors, in particular Iran.[97] The fact that such links are difficult to prove allows states to deny responsibility while at the same time generating increased media coverage for their actions.

3.6.3 Future developments

There is nothing to suggest a decline in cyberactivity linked to the war in Ukraine or the conflict in the Middle East. The tendency for hacktivist groups, whether organised entirely at civil society level or acting as a front for a third-party state, to be involved in cyberspace in the context of conflicts appears to be consolidating and establishing itself as the new norm. Although, according to current information, these groups do not appear to have been decisive for any of the protagonists, their activities could also help to galvanise and attract the attention of state forces in the cyber arena. Furthermore, this additional background noise, combined with the incomplete view resulting from the conflict, make it more difficult to assess the situation.

97 Iranian Hacktivist Proxies Escalate Activities Beyond Israel (checkpoint.com);
Iran surges cyber-enabled influence operations in support of Hamas (microsoft.com)