Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

Reporting and Analysis Centre for Information Assurance
MELANI
www.melani.admin.ch

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2019/2 (July – December)

30 APRIL 2020

REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE MELANI
https://www.melani.admin.ch/

1 Overview/contents

2 Editorial

Federal Cyber Security Delegate

Florian Schütz is the Federal Cyber Security Delegate and Head of the National Cybersecurity Centre.

MELANI is becoming the "National Cyber Security Centre". This was the title of an article on the MELANI homepage at the beginning of 2020. This move is a further step towards establishing responsibilities in the Confederation, as defined by the Federal Council on 30 January 2019 (see figure 1). The details of how the National Centre for Cyber Security (NCSC) will be organised are part of ongoing work and have not yet been finally agreed. What is already clear, however, is that MELANI is an important part of the new centre and should be further strengthened and expanded. In this editorial I would therefore like to look back on my experiences with MELANI in the second half of 2019 and discuss three future challenges.

Since MELANI was founded on 1 October 2004, information and communication technology (ICT) has continued to influence the economy, research and society. ICT is at the heart of digitalised processes and can be found in almost all areas of life. A general situation analysis is no longer sufficient in view of the diversified threat. Instead, specific analyses are needed for economic sectors, areas of politics, research and society. As a first measure, a specific situation analysis for the financial sector is currently being tested in a pilot project.

A further challenge is the scaling of incident processing. Fifteen years ago, in MELANI's first year of operation, less than 500 incidents were recorded. In contrast, more than 500 reports were submitted to us in January of this year alone. In order to process this volume, a national contact point for cyber security was created as an initial measure in the second half of 2019. It receives reports, analyses them and ensures that they are dealt with by the right authorities.

In addition, the automation of analysis and processing and the seamless integration of the authorities involved, e.g. law enforcement agencies, will be an important task.

"You have been weighed, you have been measured, and you have been found wanting" is a quote from the film "A Knight's Tail". Although MELANI enjoys an excellent reputation internationally, we hear from time to time in public discussions that MELANI is not considered to be good enough. While there is undeniably room for improvement, this generic criticism does not do justice to the good work the teams do. We believe that the reason for this criticism is that the lack of public key performance indicators (KPIs) makes it difficult to differentiate and thus, depending on the situation, some wrong conclusions are occasionally drawn. For this reason, in the future we will establish KPIs to enable differentiated criticism and to better measure success.

We have already taken one criticism to heart: The MELANI semi-annual report was not technical enough for some. In order to continue to satisfy the target group of politicians, managers and interested private individuals, but also to offer something to professionals, we have prepared a technical appendix for the first time. We would be very pleased to receive any

comments and suggestions regarding this. Let us know whether or not we should expand it in future.[1]

MELANI has achieved and delivered a great deal over the past fifteen years, as this semi-annual report also shows. The challenges will certainly increase in the coming years. However, I am convinced that we will master them and create a solid foundation for the future with the new organisation as part of the National Cyber Security Centre.

Florian Schütz

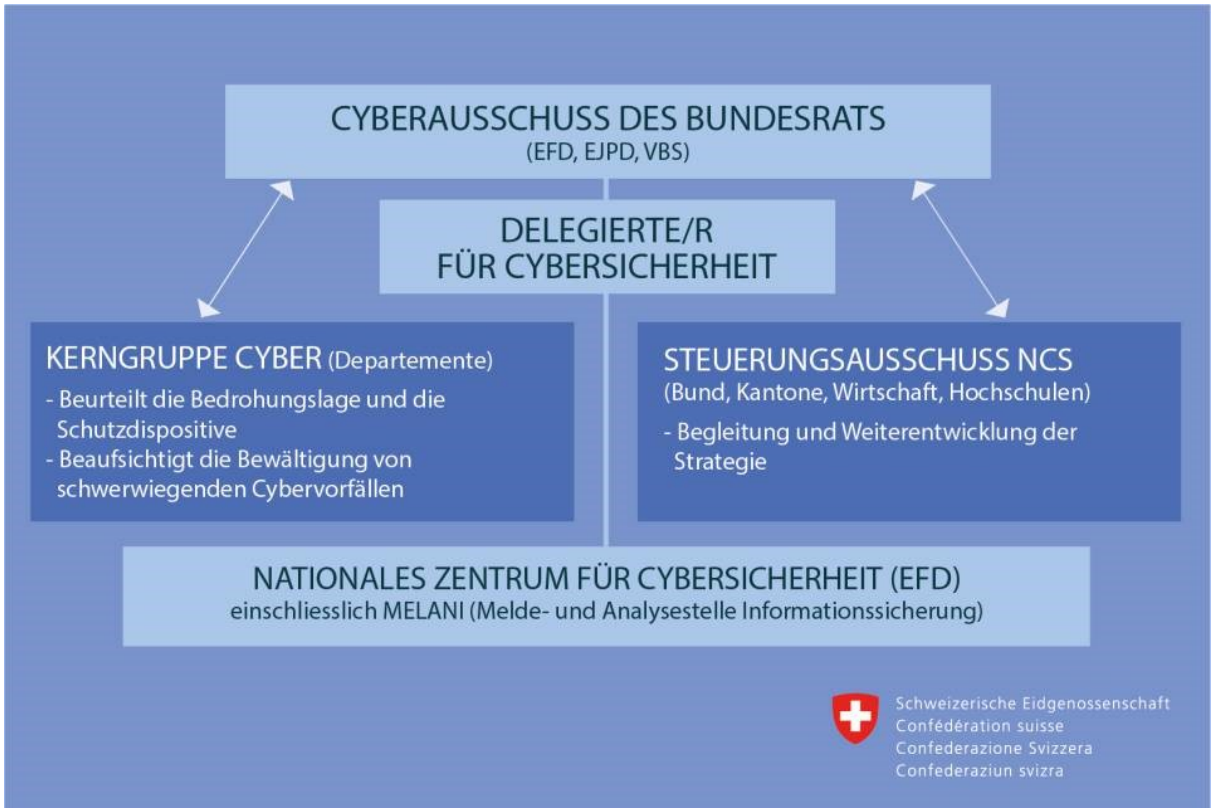

Fig. 1: Cyberorganisation in the Confederation

[1] We invite you to give feedback on this report by filling out the evaluation form on our website: https://www.melani.admin.ch/melani/en/home/dokumentation/reports/evaluation-halbjahresbericht.html

3 Key topic: personal data on the internet

3.1 Introduction

Most data processing today is done electronically and on devices that are more or less directly connected to the internet. In many cases, data is stored and can be accessed in any cloud.

"Our data" or more precisely "data about us" is stored by a wide variety of players in a variety of locations and hardly anyone has a complete overview of who has what data about us and where it is processed.

Data is collected, traded and aggregated – and often stolen, whereby "stealing" is misleading as data is simply copied and is not taken away from its owner. The same applies to the "sale" of data. Data is often "sold", duplicated and resold. This makes it much more difficult to trace the route a data set takes until it reappears somewhere.

Self-determination over one's own data is almost impossible and the prosecution of data protection violations poses a great challenge for both the individuals concerned and the responsible authorities.

Data leaks or openly accessible data caused by misconfiguration make the headlines on an almost daily basis.[2] In the case of the largest incidents, there is now talk of over a billion data sets being affected.[3] Data leaks were the key topic in the MELANI semi-annual report 2017/2.[4]

3.2 Data from the online world

We live in the age of networked information. It is impossible to imagine our everyday life without the internet. We order goods, obtain services and information, exchange opinions, images and much more via the global communications network. As a result, we each have numerous online accounts with countless providers, which we set up quickly and which are sometimes forgotten just as quickly. These accounts usually use an email address and password. Some services also require you to provide your name, address, date of birth, telephone number, photos or credit card details. The operators of these services most likely have information about what we have accessed with the account or what we have uploaded to the web. In particular, we reveal a lot about ourselves through social media accounts: who we are friends with and communicate with, who we follow, what we like or share and how much time we spend on which topics. This information allows highly detailed personality profiles to be created.

Even when simply browsing the web, we generate digital traces in the form of data that is stored on the service providers' servers, advertising networks and other content providers. Or on our devices, in the form of cookies, for example. Some browser extensions (add-ons and plug-ins) also collect data and store or forward it.[5] Although the data is not necessarily assigned

---

2 https://www.helpnetsecurity.com/2019/11/14/breaches-2019/; https://www.immuniweb.com/blog/stolen-credentials-dark-web-fortune-500.html

3 https://securityaffairs.co/wordpress/94275/breaking-news/elasticsearch-social-information-1-2b-people.html; https://www.wired.com/story/billion-records-exposed-online/

4 MELANI semi-annual report 2017/2, chapter 3.

5 https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/

to a name, it is linked pseudonymously. This allows the creation of a personality profile and, among other things, personalised advertising to be sent or other content that may be of interest to us to be offered. If this data is linked to a personal identifier, e.g. in the form of an email address or a social media account, it can also be removed from the context of the survey and processed and used independently in relation to an individual.

3.3 Data from the analogue world

Since the advent of electronic data processing (EDP), data from the analogue world has been stored digitally, initially in stand-alone computers or purely internal company networks, but now data is stored on devices that are all more or less directly connected to the Internet. Correspondence, planning, customer files, accounting and employee administration are largely digitalised. For example, we often keep our private address books only on our computers and smartphones or in the cloud.

As part of digitalisation, data from more and more areas is being processed electronically. Examples include healthcare with digital patient files and fitness apps, mobility with online tickets for public transport and bicycle rentals via apps, living with smart home devices, delivery services for food and other orders, to name but a few.

Public authorities have also been running databases electronically for some time now, are now networked and are expanding eGovernment services. If unauthorised parties gain access to government systems, large parts or even the entire population can be affected.[6]

3.4 Special situation for public registers and databases

Even for traditional public registers that have been made available online as a result of digitalisation, some aspects inherent to the internet must be taken into account. Information that was previously sent individually as a hardcopy or could be consulted at an office can now be consulted from anywhere in the world and then stored locally. The relevant ordinances stipulate that the systems should be "protected against serial searches"[7] and that certain entries should be "made available free of charge for individual searches on the internet"[8]. However, depending on its technical configuration, an entire register can be read with a little patience and programming effort. Accordingly, this creates a conflict between the statutory (also electronic) public access to data and the protection against its improper use. The legislation does not specify whether it must be possible to carry out a search anonymously. In order to effectively prevent or at least detect abusive mass searches, it would be necessary to identify those who carry out searches and to store the details of their searches for a certain time, which in turn requires a legal basis.

---

6 Ecuador https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/; Chile https://www.zdnet.com/article/voter-records-for-80-of-chiles-population-left-exposed-online/; Bulgaria https://www.inside-it.ch/articles/55013

7 Article 27 of the Land Register Ordinance (LRO), SR 211.432.1: https://www.admin.ch/opc/de/classified-compilation/20111142/index.html#a27

8 Article 12 of the Commercial Register Ordinance (CRO), SR 221.411: https://www.admin.ch/opc/de/classified-compilation/20072056/index.html#a12

Telephone directories were digitalised as early as the end of the 1980s and at that time could still be purchased on CD. Before long, this data was also made available on the internet, as it was already publicly available and this was therefore permitted. Even if the telephone directories rarely contain mobile numbers or email addresses, data from these directories can serve as master data, i.e. as a basis for data collection, especially for those who are not concerned with the legality of processing it.

A notable example is the previously publicly accessible information in the "Whois domain" directory. Among other things, this directory publishes the owners of domain names. This data is now no longer readily accessible. Originally, the purpose of Whois was that owners and operators of websites were made known and could be contacted easily. Transparency was a matter of course in the early days of the internet, which was characterised by idealistic values. However, over time, the misuse of published data soon led to discussions about the form, purpose and necessity of this register. Under pressure from the European General Data Protection Regulation (GDPR), action was finally taken and domain name information is now often anonymous.[9] Access to Whois information on Swiss domain names is also to be restricted with the pending revision of the telecommunications law.

3.5 Data protection legislation

Data processing and also the trading of personal data is permitted, depending on the circumstances and the legal system in force. However, data protection regulations vary considerably from one country to another. With its General Data Protection Regulation (GDPR), the EU provides worldwide uniform protection for the data of its citizens. Although many questions remain unanswered regarding the international enforcement of this regulation, the GDPR has already had some impact. Since its entry into force in May 2018, many players have taken data protection and data security much more seriously.

It has been repeatedly predicted that data leaks will cause more serious damage in the near future and that more will be invested in data security.[10] This is against the background that since the GDPR came into force, companies have been heavily fined for data protection violations. The calculation of damages takes particular account of the potential fines of up to EUR 20 million or 4% of annual turnover (whichever is higher) to which companies can be subjected.

The revision of the Swiss Data Protection Act includes criminal provisions according to which "private persons", i.e. employees of companies, rather than the companies, are punished. Only if a fine is for less than CHF 50,000 can a business be ordered to pay it if investigating the offender involves disproportionate effort. It remains to be seen to what extent this leads to tensions within companies when the management (does not) make decisions and (does not)

---

9 https://www.icann.org/resources/pages/gtld-registration-data-specs-en

10 https://securityintelligence.com/articles/11-stats-on-ciso-spending-to-inform-your-2020-cybersecurity-budget/; https://www.business2community.com/cybersecurity/10-cybersecurity-trends-in-2020-you-need-to-keep-an-eye-on-02275883; https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/; https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/

set rules, the consequences of which data protection officers or simple employees will have to bear.

3.6 Risks and side effects

It is rare that anyone talks about the consequential damages of data protection violations that affected individuals may suffer. They are also difficult to quantify. Data such as name, addresses, dates of birth, telephone numbers, email addresses, etc. are not "particularly sensitive" personal data, but in the wrong hands, such data can already be used to cause a lot of harm. Increased quantities of spam is the least of the problems. Leaked data is used by criminals for tailor-made social engineering attacks which aim to install malware, obtain further (more sensitive) data, trigger unjustified payments or achieve other objectives that have a negative impact on those concerned.[11] Personal information can also be misused to establish identities; people can impersonate other people by using their data. This allows them to create social media accounts, register domain names or place orders using someone else's identity. Fraud involving the contacts belonging to people whose email account has been compromised or data otherwise leaked also occurs regularly.

It is difficult to assess the consequences of unauthorised acquisition and further processing of data. In the age of big data and machine learning, automated merging of different data sources is becoming increasingly simple. Whether this is done by companies for legitimate purposes, in legal grey areas or by criminals is only superficially relevant. It can be assumed that every database will be hacked sooner or later and that the data sets will find their way into the underground market.

3.7 Conclusion

"Our data" or "data about us" is stored by many players in many locations. The collection, gathering and merging of data is a business model in both legal and illegal circles and leads to the trade in this data. We must therefore expect that commercial or advertising companies and criminals will have access to more or less large data sets on us and will be able to use them to target us. If personality profiles are also created from the data, this opens up possibilities for specific psychological influence, not only in terms of consumption and susceptibility to fraudulent practices, but also on how opinions are formed and thus ultimately on voting behaviour. Internet advertising is already individualised in many cases. This trend will continue and is likely to be increasingly used by political players to distribute targeted election and voting propaganda.

Criminals will continue to improve their methods of attack and tailor them more individually to potential victims. A personalised greeting in an email has long since ceased to be a suitable criterion to prove its seriousness. Criminals have been filling their emails with names, addresses, telephone numbers and other personal details of the recipients for some time now. Fake sender addresses are also regularly chosen in such a way that it appears as if the email

[11] See https://www.microsoft.com/security/blog/2019/12/02/spear-phishing-campaigns-sharper-than-you-think/ and the "Social engineering" chapters in the MELANI semi-annual reports.

comes from a known individual, that is if the email or social media message is not actually sent with the alleged sender's real, yet compromised, account.

Assessment/recommendations

Even though the internet offers many advantages and has greatly simplified access to valuable information, remember not to believe everything you read on the web or in your inbox. Caution and a healthy dose of scepticism are called for when browsing and communicating on the internet. If in doubt, it is better to discuss issues, incidents and unusual messages with your friends and acquaintances. In you are unsure, contact the supposed sender before you click on a link or open an attachment.

Anyone who processes and stores personal data must ensure that it is adequately protected against unauthorised access. Public registers should allow standard searches, but must prevent mass searches. In the case of other databases which may have restricted access, e.g. with test or demo access, care must also be taken to ensure that these restrictions cannot be overridden. Players who are specialised in collecting data try to circumvent technical restrictions, for example by automatically generating numerous test accounts or otherwise pretending to be a large number of users.

4 Situation

You can use the online MELANI[12] report form to notify us of incidents and ask questions. Reports help us to identify trends in internet dangers, to provide information and to recommend or take countermeasures. The chart below shows the type and number of reports for the second half of 2019 and gives an indication of the Swiss population's concerns during this period.

There is a lot of lying and cheating on the internet. This can be seen from the reports on phishing, fraud and *fake sextortion*. These phenomena are incidents that are typically relatively easy to detect and therefore often lead to reports. When such reports are made, it can be assumed that the majority of affected users have realised that they are scams and were not victims themselves. We cannot provide any reliable information on the success rate of these attacks. In contrast, with reports on ransomware, it can be assumed that the original incident caused at least some damage. Other malware incidents occur unnoticed in the background and are therefore neither detected nor reported by those affected (see section **Errore. L'origine riferimento non è stata trovata.** on the drive-by situation in Switzerland).

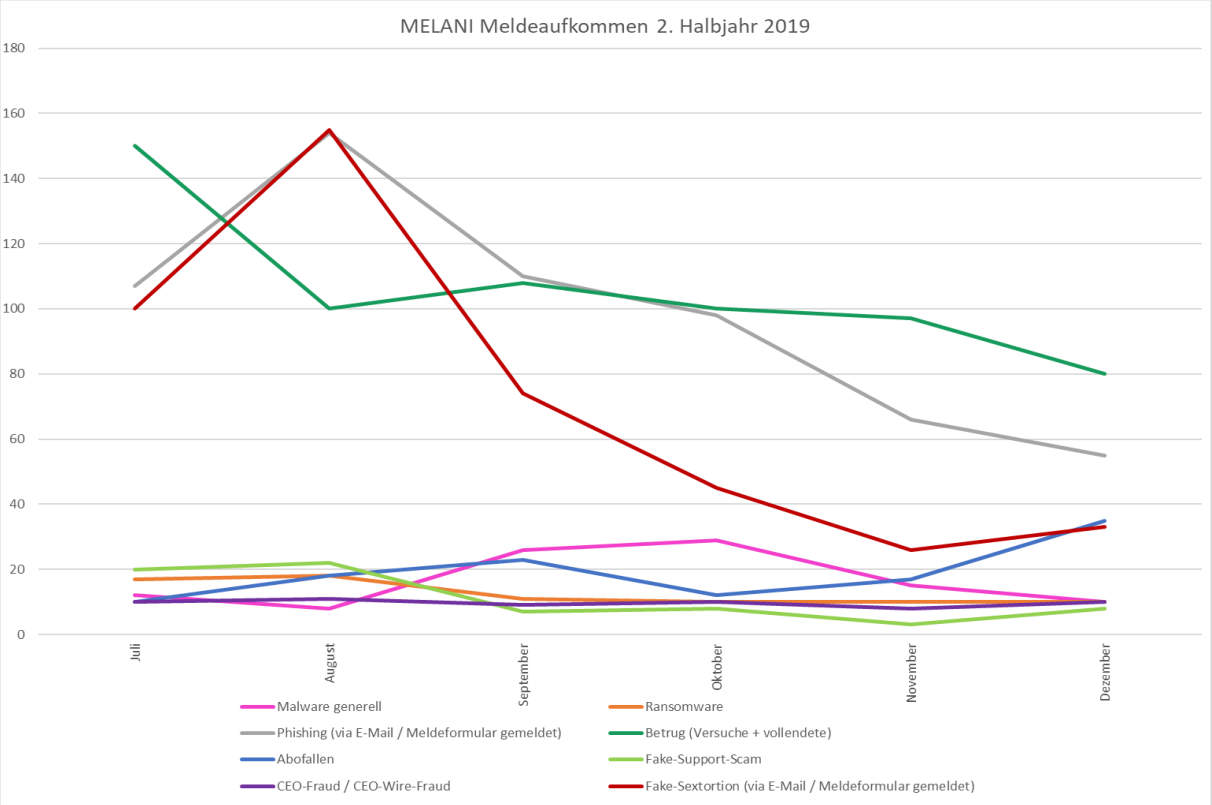

Fig. 2: Reports received via the online report form. Reports via other channels are not included.

12 https://www.melani.admin.ch/melani/en/home/ncsc/form.html

4.1 Espionage

In the second half of 2019, cyberespionage continued to be a popular tool used by governments to gather information and steal intellectual property. Google's Threat Analysis Group (TAG) is focused on detecting and defending against cyberattacks aimed at its users. For example, it reported 12,000 *spear phishing* attempts in 149 countries in the third quarter of 2019 alone (July to September).[13] It is believed that more than 270 groups linked to government agencies, operating in at least 50 countries, were responsible for these incidents. In addition to classic espionage, disinformation campaigns aimed at promoting the interests of a particular country or discriminating against political movements were also recorded. Like dissidents and activists, politicians also belong to the high-risk group. This is evidenced by hundreds of attempted attacks against political organisations registered by AccountGuard, Microsoft's security service. This platform was set up to warn campaigning candidates and offices that have been targeted by cyberattacks. However, large companies are thought to be most affected by targeted, state-sponsored attempts at cyber-compromising. In terms of numbers, they are said to account for over three-quarters of the 10,000 users reported by Microsoft in 2019.[14] The software giant has compiled a list of the five most active attack groups, known as *advanced persistent threats* (APTs), in 2019. According to Microsoft and other security companies[15], of the groups listed, "Holmium" aka "APT33" is said to be sponsored by the Iranian government. Its main aim is to target organisations active in the civil and military aviation and petrochemical energy sectors. Among other reasons, the campaign hit the headlines because between 2016 and 2017 both a US company active in aviation and a Saudi Arabian organisation active in the same sector were attacked.[16] Microsoft also points to "Strontium", also known as "Fancy Bear", "APT28" or "Sofacy", as being another particularly active group. Several governments (notably UK and USA) as well as some security companies (e.g. CrowdStrike) allege that the group is connected with the Russian military intelligence service (GRU). The group has been linked to the attacks against the German Bundestag (2015), the US Democratic National Committee (2016) and the World Anti-Doping Agency (2016), among others.

4.1.1 Cyberattacks on sport and anti-doping organisations

Sports and anti-doping organisations have been the target of cyberespionage campaigns for several years now. As described in the MELANI semi-annual report 2018/1 (section 4.1.1), the ICT infrastructure of the Winter Olympic Games in Pyeongchang (South Korea) was attacked by the "Olympic Destroyer" worm in the same year. The security service provider Kaspersky Lab found analogies in this worm with "Sofacy". It appears that the "Fancy Bears" group is also linked to this campaign. At the beginning of the same year, the team published data that had

---

13 https://blog.google/technology/safety-security/threat-analysis-group/protecting-users-government-backed-hacking-and-disinformation/

14 https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/; https://arstechnica.com/tech-policy/2019/07/microsoft-warns-10000-customers-theyre-targeted-by-nation-sponsored-hackers/

15 https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

16 See MELANI semi-annual report 2017/2, section 5.1.2.

been stolen from the International Olympic Committee and the USA National Olympic Committee between the end of 2016 and beginning of 2017. This included emails of the organisation as well as medical records of athletes.

On 28 October 2019, Microsoft's Threat Intelligence Center announced the identification of numerous attacks that were believed to have been carried out by "Sofacy" against at least 16 anti-doping authorities and sports organisations across three continents. The attacks probably began in mid-September, shortly before the decision by the World Anti-Doping Agency (WADA) to exclude Russia from the Tokyo 2020 Olympic Games was announced.[17]

This campaign is by no means the only one in connection with the Summer Games, which were to be held in Japan from 24 July to 9 August 2020 but is now moved to take place in 2021 due to the coronavirus crisis. The organisers warned against email campaigns that misuse the name of the Organising Committee of the Olympic and Paralympic Games to redirect recipients to *phishing* sites or infect their devices. One phishing campaign specifically targeted 170,000 individuals in Japan and the USA. Some details of this attack, such as its intent and scope, were found in a chat on the dark web.[18] The evidence in this case appears to indicate that the culprit here was different to that involved in the attempted infiltration of sports and anti-doping organisations last October.[19]

What makes these targets so attractive? Before the competitions take place, the attacks can be used to gather information about athletes from other countries, their abilities, weaknesses and plans, in the hope of using this information to develop possible winning strategies. A further reason could be the falsification of doping test results. In some countries, sport is more than a contest amongst athletes. It is part of social cohesion and can be used for political purposes: Political leaders may profit off the popularity of successful athletes. In addition, major sporting events provide an ideal platform for people to showcase their IT skills. Potentially, by using *false flag* techniques, such attacks also offer the opportunity to reshape international politics. Finally, such attacks in a sanctioned country can satisfy the need for gratification.

4.1.2 Winnti industrial espionage campaign

According to the latest revelations, the number of German multinationals that have become the target of cyberattacks is rising. Communications giant Siemens, for example, recently confirmed that it had become the victim of a cyberattack in June 2016, but apparently no data was leaked. Also affected was Covestro, a manufacturer of plastics and adhesives, which also escaped without damage. The pharmaceutical giant Bayer announced in April that it had already been the victim of cyberespionage in 2018. According to various security experts, all these attacks are said to have been triggered by Winnti. This name is used to describe both a group and the malware it uses, which is known, among other things, for having infiltrated the steel producer ThyssenKrupp in 2016.[20] The same experts believe the origin of these attacks to be in China.

---

17 https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

18 https://www.bleepingcomputer.com/news/security/tokyo-2020-staff-warns-of-phishing-disguised-as-official-emails/

19 https://english.kyodonews.net/news/2018/09/e2d8f3727275-phishing-scam-on-2020-olympics-tickets-spotted.html

20 https://www.waz.de/wirtschaft/spionage-mehrere-dax-konzerne-von-hackern-angegriffen-id226573145.html; see also MELANI semi-annual report 2016/2, section 5.1.3.

Initially, the group focused on attacks against online gaming platforms for purely financial motives. However, by 2015 at the latest, it had expanded its activities to include industrial espionage. It appears to be particularly targeting the chemical and pharmaceutical sectors, and companies specialising in cutting-edge technologies. In addition to the victims already mentioned, an in-depth analysis by the Bayerischer Rundfunk and Norddeutsche Rundfunk radio stations identified older infections which have not made the headlines thus far. They mentioned, for example, the company Henkel, which, like Covestro, produces adhesive products for industry and was infiltrated in 2014. Another confirmed victim is BASF ("Badische Anilin- und Soda-Fabrik"), one of the world's largest chemical companies, which is also based in Germany. The 2015 attack had no serious consequences.[21]

After infiltrating a company's network, the hackers create a map of the network and then search for the strategic points where the malware can be hidden. In this way, they can operate invisibly in the background for as long as possible and collect information about the company and its products in the hope of finding trade secrets. One of the main characteristics of Winnti is its perseverance. By installing backdoors, the perpetrators gain permanent access to a business network. In October 2019, the IT security company ESET reported that it had discovered a previously unknown backdoor that were based on Microsoft SQL (MSSQL) and used by Winnti".[22]

Although Winnti came into the limelight in Germany after the attack on ThyssenKrupp, the campaign is also active in other countries in Western Europe, Asia and the USA. Research by ESET has revealed that the group is believed to have infected a major Asian-based manufacturer of mobile hardware and software via PortReuse, a backdoor that emerged in March 2019. It is possible that by compromising the company in this way, the hacker group was preparing for a far-reaching attack via the supply chain.[23]

Finally, the malware is also used for political espionage. According to Kaspersky Lab experts, there are currently at least two groups that use this attack tool. This makes it difficult to determine whether those responsible for industrial cyberespionage are the same as those who are more likely to engage in political espionage – be it against the Hong Kong government or the Indian telecommunications provider in the region which is home to the headquarters of the Tibetan government in exile.[24]

---

21 http://web.br.de/interaktiv/winnti/

22 https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/; https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

23 https://www.bleepingcomputer.com/news/security/winnti-group-uses-new-portreuse-malware-against-asian-manufacturer/

24 http://web.br.de/interaktiv/winnti/

Conclusion/recommendations:

For several years now, the problem of advanced persistent threats (APT) has no longer been confined exclusively to government and military agencies. Increasingly, international organisations and private industry from different sectors are also confronted with highly complex attacks. These developments may be explained with the increasing "democratization" of such attacks, as the tools necessary are more broadly available (see chapter 5.1.1 of the semi-annual report 2019/1). For this reason, the number of active attackers has risen and they pursue many different goals. Many private sector companies have neither the financial resources nor the expertise to combat such threats.

One possible solution is to outsource their own computer security to IT experts such as cloud service providers and cloud security providers. However, this does not release companies from the responsibility of taking further internal measures to raise awareness and train employees. The risk of (former) employees granting third parties access to the company's internal system should not be underestimated. This is a simple way for them to earn money, act out of personal resentment or wilfully harm their employer.

It is advisable to join one or more public or private networks that exchange information on current threats and that also provide tips on how to identify risks and what you can do to protect yourself.

Technical measures:

If an internal risk analysis shows a clear danger for your organisation or institution, you should protect yourself with a number of technical measures to limit the possibility of infection:

At system level:

- Use of AppLocker (or a comparable function) to prevent the execution of unknown binary files, namely from the user profile folders;
- Restriction of non-essential user rights;
- Use of an alert for when system execution tools are run.

For the Active Directory (AD):

- Careful monitoring of the AD to detect unusual or large requests;
- Introduction of multi-factor authentication for the AD and especially for remote access;
- In addition, Microsoft clients are recommended to use RAP as a Service on a regular basis (see https://services.premier.microsoft.com/assess/).

At network level:

- Archiving of log data for at least two years for important gateway systems such as Proxy DNS;
- Execution of Passive DNS for quickly checking suspicious domains;
- Introduction of signature-based Intrusion Detection System (IDS) "Snort";
- Use of an internal segmentation policy (it is generally better to avoid client-to-client communication);
- Collection of network flow data at various locations on the internal network;
- Choice of a central control point for internet access that is carefully monitored;
- Out-of-band management of servers with LAN management – no browsing or email from the management station;
- Proxy whitelisting for international servers that have to communicate externally.

4.2 Industrial control systems

In its first semi-annual report in 2005, MELANI wrote in an article on new directives on the IT security of nuclear plants in the USA: "The main problems relating to the security of so-called SCADA systems in power plants (Supervisory Control and Data Acquisition) can be found with respect to data and command transmissions that so far have largely been unencrypted, connections to public networks, and the lack of standardisation of the technologies".[25]

Since then, security awareness in the area of industrial control systems (ICSs) has increased considerably. The attacks on the integrity of ICS-controlled processes that have come to light in the last 15 years have certainly contributed to this. In addition to attacks on the systems themselves, which can of course damage them, attacks that target the process controlled by the systems have attracted attention. "Stuxnet"[26] in 2010, "Industroyer/CRASHOVERRIDE"[27] at the end of 2016 and "Triton/Trisis",[28] discovered in 2017, are the most famous examples in this category. Section 4.2.1 illustrates the attempt to inflict process-related damage on the electricity supply in Ukraine by means of "CRASHOVERRIDE".

The extended networking of control systems as well as actuators and sensors have added to the increased criticality of the appropriate protection of such system landscapes. The Industrial Internet of Things (IIoT) enables promising new automation processes, but at the same time increases the scope for these processes to be attacked. Ensuring an adequate level of security measures remains a challenge that has yet to be solved across the board.

4.2.1 Power supply remains a target

The electricity supply in Ukraine fell victim to a cyberattack in December 2016, leading to a power outage.[29] However, Ukrenergo technicians at the substation just north of Kiev succeeded in restoring the power supply by manual switching operations after just under an hour. However, new analyses[30] of this attack involving the "CRASHOVERRIDE" malware show that the attackers, if successful (see figure 3), would have caused the physical destruction of network elements during precisely this process. Part of the attack was aimed at the protection relays of the transmission network. However, the objective of the attack, to disable the protective function of the relays (denial of service), failed. The protection provided by the relays, combined with a lack of visibility into the attacked control systems, prevented an unfavourable switch-on sequence which would have damaged parts of the network and led to significantly longer downtimes in addition to the physical damage.

---

25 MELANI semi-annual report 2005/1, section 7.1.

26 MELANI semi-annual report 2010/2, section 4.1.

27 MELANI semi-annual report 2017/1, section 5.3.

28 MELANI semi-annual report 2017/2, section 5.3.2.

29 MELANI semi-annual report 2016/2, section 5.3.1.

30 https://dragos.com/resource/crashoverride-reassessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack/

Fig. 3: Intended path of attack (source: dragos.com)

Our knowledge that attackers have such intentions shows the importance of keeping risks in critical areas as low as possible. A report by the Federal Electricity Commission (ElCom)[31] in 2019 noted that there was still potential for optimisation in the implementation of adequate security measures in Switzerland's electricity supply.[32] ElCom therefore required that "OT systems be regularly tested for security vulnerabilities", among other things. During the period under review, for example, a whole series of vulnerabilities[33] in the VxWorks real-time operating system, which forms the basis of many application-specific control systems, became public knowledge. This deep integration requires the involvement of a whole chain of system manufacturers and operators in order to close the vulnerabilities in the operational process control systems. The number of known security vulnerabilities in process control could increase noticeably in the future, as the Pwn2Own[34] vulnerability research competition will in future include ICSs in its list of systems to be investigated, in addition to classic IT systems. As well as the systems in use, more and more elements are being connected to the network,[35] which further complicates the coordinated implementation of security specifications involving all the suppliers concerned.

Furthermore, an increasing number of attackers are targeting the power supply industry[36] and its supply chain[37]. In late summer 2019, two waves of *spear phishing* against power distributors in the USA were observed as they attempted to inject the "LookBack" malware into the downstream companies. To do this, the attackers imitated licensing bodies that are recognised in the industry in order to entice recipients to open the attachments. Once installed, the

---

31 https://www.elcom.admin.ch/dam/elcom/de/dokumente/2019/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf.download.pdf/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf

32 https://www.tagesanzeiger.ch/schweiz/standard/fuer-hacker-stehen-die-einfallstore-offen/story/20223699

33 https://www.armis.com/urgent11/

34 https://www.darkreading.com/vulnerabilities---threats/pwn2own-adds-industrial-control-systems-to-hacking-contest/d/d-id/1336191

35 https://www.zdnet.com/article/ameo-concerned-about-nation-state-attacks-on-power-grids/

36 https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

37 https://www.wired.com/story/iran-apt33-industrial-control-systems/

malware itself acted as a Remote Access Trojan (RAT), which provided the attacker with extensive functionalities on the infected systems via remote access.

With the shift from fossil fuels to electromobility, the supply of electricity is also becoming increasingly important for this societal aspect. At the same time, energy policy objectives are shifting electricity production further away from large centralised power plants towards smaller, decentralised plants that produce renewable energy. This is coupled with the computerisation of the electricity supply (SmartGrid). MELANI, together with electricity producers and network operators, is endeavouring to protect Switzerland's power supply from information security risks as far as possible. The reliability of the electricity supply is a central factor in ensuring that the economy and society function properly and that our prosperity is maintained.

Recommendation:

If you discover openly accessible or poorly secured control systems on the internet, notify us of the details so that we can contact the operator(s).

MELANI reporting form
https://www.melani.admin.ch/melani/en/home/ncsc.html

Checklist with measures for the protection of industrial control systems:
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-for-the-protection-of-industrial-control-systems--icss-.html

4.3 Attacks (DDoS, defacements, drive-bys)

4.3.1 DDoS attacks for blackmail purposes or to hinder services

In the last week of 2019, DDoS attacks were made against Swiss online media[38] which left some websites temporarily unavailable. The motivation behind these attacks remains unclear to this day.

A DDoS (distributed denial of service) is a type of attack on computer systems which has the aim of making them unavailable. The last six months have seen a renewed rise in the frequency of extortion-related DDoS attacks.[39] The attackers often carry out a test attack in advance to show that they have these abilities. They demand that the victim pay a ransom to

[38] https://www.20min.ch/digital/news/story/Technische-Probleme-auf-20minuten-ch-12858361; https://www.nzz.ch/wirtschaft/cyberattacke-gegen-schweizer-medien-ld.1530906

[39] For more on this approach, see MELANI semi-annual reports 2016/1, section 4.4.1 and additional content in the MELANI semi-annual reports 2018/1, section 4.3.1, 2017/2, section 4.3.1, 2016/2, section 4.4.1, 2015/2, section 4.3.4, 2015/1, section 4.4.1.

avert another, more serious attack. Such attacks can also be politically motivated, as the DDoS attack on the UK Labour Party websites showed.[40]According to some security researchers, however, the tendency is for low-intensity attacks, so that the DDoS defences are not activated (straight away), but the performance of websites or servers is still affected.[41]

Recommendation:

MELANI recommends various preventive and reactive measures to deal with DDoS attacks.

Checklist of measures to counter DDoS attacks

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/massnahmen-gegen-ddos-attacken.html

4.3.2 Drive-by: Situation in Switzerland

There are several ways in which a device can be infected with malware. A common method is to hack websites and put in place a script. By testing *exploits*, this script looks for open security vulnerabilities in the browser or in other applications such as FlashPlayer. Since calling up a manipulated website can be enough to become infected, this is known as a "drive-by download".

In the second half of 2019, MELANI identified around 500 infected websites in Switzerland and informed their operators so that they could remove the malware from their websites.

Internet users who discover such infected websites are asked to report them to MELANI and help contribute to general cybersecurity.

Recommendations:

1. Install at least two different browsers so that you can switch to another browser at short notice if a serious security vulnerability becomes known in the first.
2. Always install the latest updates for your browsers, preferably via automatic security updates.
3. Whenever possible, use an *ad blocker* and restrict the use of *JavaScript* as much as possible.
4. If a website unexpectedly asks you to download a file, do not agree to this under any circumstances.

40 https://www.theregister.co.uk/2019/11/12/labour_party_reports_cyber_attack/

41 https://www.zdnet.com/article/ddos-attacks-getting-smaller-sneakier-and-more-dangerous/#ftag=RSSbaffb68

4.3.3 Cyberattack on Upbit cryptocurrency platform

Cryptocurrency platforms are always a lucrative target for attackers, as a successful attack can result in a lot of money being stolen. This was also true in the case of the South Korean platform Upbit, where attackers stole 342,000 *Ethereum* from the *exchange's hot wallet*. At the time of the theft, these Ethereum were worth USD 48.5 million. According to speculation, this could be an "exit scam", i.e. insiders transfer platform users' money to their own account and claim that a cyberattack was the cause. However, it is difficult to turn the stolen Ethereum into cash, as it would have to be laundered[42] with considerable effort to prevent its origin from being traced.[43]

4.4 Social engineering and phishing

4.4.1 Phishing

The second half of 2019 saw a large number of phishing attacks, especially in the name of various Swiss brands. The content of the emails varied little: some requested credit card data for "verification" purposes, while others directed the victim to linked pages requesting usernames and passwords for online services. Frequently, phishing emails contain the logos of well-known companies or of the service in question so that the emails are made to look official. Email services continue to be a frequent target, as the access data for email accounts opens up a wide range of other attack options.

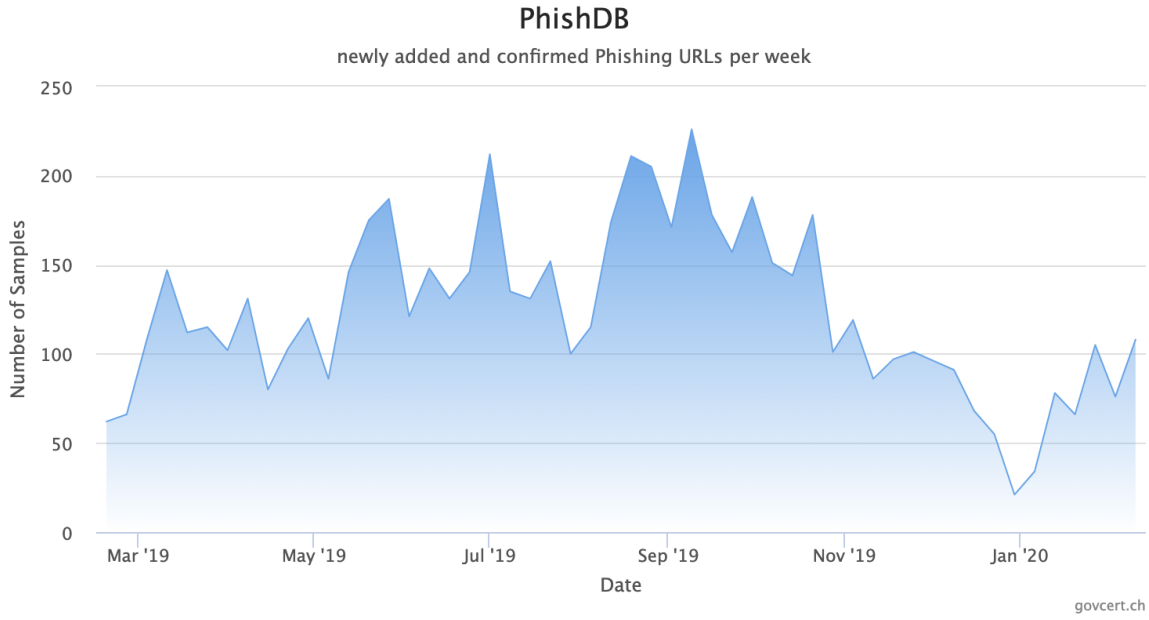

Fig. 4: Reported and confirmed phishing sites per week on antiphishing.ch in the past year, as at 9 February 2020.

42 See also section 5.3.

43 https://www.zdnet.com/article/upbit-cryptocurrency-exchange-loses-48-5-million-to-hackers/

4.4.2 Phishing websites with 404 error pages

404 error pages are used to inform website visitors that a subpage they wish to visit does not exist (or no longer exists) at the address requested. Most website operators include a 404 error page in their website design for such situations and store it as a standard error message. This allows them to display content of their choice when the 404 error occurs, thus informing website visitors in a targeted manner and redirecting them if necessary. Unfortunately, as with any website, malicious content such as phishing or drive-by downloads can also be placed on these pages. Microsoft reported last August that it had discovered such a phishing campaign targeted at its users. A phishing page which perfectly imitated the Microsoft account login portal was placed as a 404 error page on a website of a domain registered by criminals. This meant that whenever any non-existent URL on the website was called up, visitors were directed to the manipulated 404 error page, i.e. the phishing site.[44] This method allows attackers to randomly create an unlimited number of phishing URLs, making it difficult to detect and block them using the links in the emails, as the URLs only share the domain name.

Criminals behind phishing sites are constantly looking for new ways to trick users into following malicious links. Remember to think twice before clicking on a link in an email or message on your smartphone. You will find many recommendations on our website:

https://www.melani.admin.ch/melani/en/home/themen/phishing.html

You can report cases of phishing at the following address:

https://www.antiphishing.ch/

Your reports help us to take measures to protect other users.

4.4.3 Blackmail supported with claims – new variants

Criminals continue to send emails claiming they have access to a computer and webcam and threaten to publish compromising images or video material of the recipient if no ransom is paid in a cryptocurrency within a certain period of time (*fake sextorsion*). These emails often contain passwords and/or telephone numbers that really are connected to the potential victim. MELANI is aware of recent examples in which potential fraud victims were "followed up" before the end of the deadline. They were reminded by email of the impending deadline and the resulting consequences.

Recently, cases have also been recorded in which the sender claims to be in possession of video files showing the recipient consuming illegal pornography with children. In order to intimidate the recipients, files are attached that are personalised with their names or email addresses. This scam can of course also be targeted at both male and female users.

44 https://www.bleepingcomputer.com/news/security/microsoft-warns-of-phishing-attacks-using-custom-404-pages/

Examples were also reported in which cryptocurrencies other than bitcoin were used. These are probably used as it is assumed that the instruments for tracking payments do not yet work properly for less popular cryptocurrencies. QR codes have also been used instead of plain text wallet addresses, as security software recognises the latter in emails and often considers them as fraudulent and blocks them accordingly. This once again shows the importance of combining technical security measures with awareness campaigns in order to prevent cyberattacks efficiently.

MELANI is also aware of threats of acid attacks and the involvement of contract killers. However, this type of blackmailing email was not as common as the fake sextorsion scam. This is certainly due to the fact that people are less hesitant about reporting threats of physical violence to the authorities than they are about fake sextorsion, where reference is made to alleged past intimate acts.

IT security researchers[45] have discovered why the sextorsion campaigns have been reported in such large waves. With the help of the Phorpiex malware, more than 450,000 computers have now been infected and combined to form a *botnet*. Criminals use this botnet to send their electronic blackmail messages en masse. The recipients' email addresses are randomly drawn from an email database. The contents of the emails are created from boilerplate texts, which further increases the level of automation. The sending frequency is relatively high, at around 30,000 sextorsion emails per hour. The campaign's reach is estimated to be 27 million potential victims.

Do not be intimidated by claims, do not react to blackmail messages and contact the authorities in case of doubt. Further information about fake sextorsion emails can be found at https://www.stop-sextortion.ch/, where you can also report such emails. If you are still using the password mentioned in the email, you should change it immediately. As a rule, you should change passwords regularly and do not use the same password for multiple internet services. For efficient prevention against cyberattacks, be sure to combine technical security measures with awareness campaigns.

4.4.4 Business email compromise: a resilient and ever-evolving approach

Since 2013, MELANI has addressed *CEO fraud* scams several times in its semi-annual reports.[46] This phenomenon has undergone many changes over time and criminals are constantly improving their methods to reach new targets and victims.

In recent years, fraudsters have increasingly adopted the identity of suppliers and sent invoices with modified IBANs to their customers. Often, hacking an email account or online collaboration platform hands criminals the necessary information on a silver platter and original invoices can

[45] https://m.pctipp.ch/news/artikel/user-pc-fuer-sextortion-spam-missbraucht-93135/

[46] MELANI semi-annual reports 2013/1, section 3.4; 2016/1, section 4.5.1; 2016/2, section 4.5.1; 2017/1, section 4.3.3; 2018/2, section 4.4.3; 2019/1, section 4.4.5.

then be forged.[47] The latest statistics from the Financial Crimes Enforcement Network (FINCEN) in the United States confirm this trend of increasingly adopting the identities of external business partners of the victim company.[48] FINCEN's analysis also provides interesting figures on the areas of activity concerned. In the United States, manufacturing and construction industries are particularly targeted. This can perhaps be explained by the fact that these sectors are particularly dependent on external suppliers and work with many subcontractors. Nevertheless, all sectors remain potential targets for cyberattacks of all kinds.

However, fraud attempts in which the attacker poses as an individual from within the target company are still common. Criminals seek to use technological advances to improve their methods. In September 2019, the Wall Street Journal reported on a case in which fraudsters did not only use email to pose as the CEO. With the help of voice software and artificial intelligence, the criminals were able to imitate the voice of the CEO and initiate fraudulent money transfers by telephone.[49]

A variant of this type of fraud has recently been observed in Switzerland as well, where criminals pose as company employees. They write to the people responsible for paying salaries (usually the human resources team) and inform them that "their" salary should be paid into another bank account with immediate effect. This phenomenon has already been documented in detail by the security provider Trustwave at the beginning of 2019[50]. In the case described by Trustwave, fraudsters created addresses using free email services. Before doing so, they simply took the information required for the attack, such as the identity of the payroll employees, from open sources (company website, social networks, etc.).

Conclusion/recommendation:

Given criminals' extremely high level of creativity and their ability to constantly adapt their techniques, the fight against fraud attempts remains a challenge for all companies. Ensure that employees are aware that all processes and security measures defined by the company must be complied with at all times. In particular, all funds transfers should be carried out according to the dual control principle with collective signatures. Special attention should be given to notifications of changes of bank details.

Information and recommendations on CEO fraud:

https://www.melani.admin.ch/melani/en/home/themen/CEO-Fraud.html

47 See MELANI semi-annual report 2018/2, section 4.4.3.

48 https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

49 https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/

50 https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bec-payroll-scam-your-salary-is-mine/

4.4.5 Online investment fraud

In the six months under review, MELANI received various reports of bogus online trading platforms and websites advertising them, all of which promised large and quick profits with cryptocurrencies. This fraudulent advertising is often disseminated via social networks and misuses celebrities to enhance its credibility. In fictitious interviews, celebrities such as Roger Federer and DJ Bobo explain that they have made part of their fortune with bitcoins. There are warnings on the internet that any money invested will be lost.[51] Fake news is a widespread phenomenon at the moment and you can protect yourself from it by taking a critical approach towards any reports which appear strange or come from dubious sources.

Trading on the stock markets is always a risky business. Impersonal messages from trading platforms (e.g. in a social network, by email, text message or WhatsApp) are an indication that it is part of a dubious mass mailing. An explanatory video from the Swiss Financial Market Supervisory Authority (FINMA) describes the problem in detail and explains how to protect yourself against investment fraud.[52] FINMA has also published a list of recognised electronic platforms.[53] It should be noted that (mass) advertising for dubious offers can be automatically designed to include names and other individual details.

4.5 Data leaks

4.5.1 Patient data accessible

In the course of an investigation[54], several million patient files from various countries were discovered unprotected on the internet in the summer of 2019. This involved highly sensitive medical data on unsecured internet servers that had been accessible to all for years. The X-ray images were high-resolution and included personal data such as first and last name, date of birth, date of examination, as well as information about the doctor treating the patient and the treatment itself. The examinations with imaging procedures are sent from the X-ray machines to special servers that are used for image archiving using PACS (picture archiving and communication system). 16 million data sets in around 50 countries were said to have been affected. Patients in the United States were particularly affected, and 13,000 data sets were involved in Germany. The German Federal Office for Information Security (BSI) informed 46 countries and is in contact with the operator of the German PACS server. It is also examining supervisory measures ranging from recommendations for improved IT security to the imposition of a fine. Analyses by MELANI have not provided any evidence of Swiss patient data being involved, although a few PACS servers were located in Switzerland.

The following example illustrates the far-reaching responsibilities of company management bodies:

Certain manufacturers of medical technology devices not only distribute them, but also provide after-sales technical support. As a service provider, a company is required to comply with

---

51 https://www.20min.ch/schweiz/news/story/Wieso-stoppt-niemand-die-Bitcoin-Betrueger--13654244

52 https://finma.ch/en/dokumentation/finma-videos/schutz-vor-anlagebetrug/

53 https://www.finma.ch/en/finma-public/authorised-institutions-individuals-and-products/

54 https://www.br.de/nachrichten/deutschland-welt/millionenfach-patientendaten-ungeschuetzt-imnetz,RcF09BW

common and industry-specific security standards, as well as any that are contractually agreed. This knowledge is of central importance for risk management in medical companies: recipients of a third-party service are responsible for ensuring that they are informed about the service provider's actual security measures and must have them documented. This ensures that data produced internally by external service providers is appropriately secured, maintained and archived. These security concepts should be checked by an independent external body.

Two other data leaks in the healthcare sector demonstrated the scope of data leaks and the effort required to handle such incidents: two US-based companies, a medical centre and a medical supplier, reported data leaks that affected a total of approximately 220,000 people.[55] The data leaks occurred as a result of a phishing incident and a ransomware attack.

As part of a targeted phishing campaign, hackers gained access to employees' Office 365 accounts, allowing them to access their email accounts undetected for around two months. The attackers were potentially able to access and acquire current and former patient and employee information. Information that was possibly leaked included names, addresses, dates of birth, social security numbers, employee identification numbers, medical information, health insurance information, financial information, payment information, driver's licence information, passport information, password/PIN, as well as account login and billing information.[56]

In the case of the ransomware attack, the medical centre, which is an association of various service providers in the healthcare sector, suffered the encryption of one of its member's databases. Backup copies enabled access to the medical data to be restored. However, those responsible were not able to restore access to all the information involved. The company assumes that the incident did not result in the patient information being leaked to unauthorised third parties.

In both cases, the individuals affected were informed and free credit monitoring services were offered to them for a certain period of time to get notified in case of identity theft.

Recommendations:

Comprehensive risk management is crucial for companies. Third-party providers are also regularly involved in cases of major data leaks. Companies in all sectors must formulate precise security requirements for third-party providers and include them in their contracts. Incident management and crisis and business continuity management (BCM) should additionally be discussed in this context. You should likewise check that the third-party provider's cyberinsurance is sufficient to cover the financial loss which would result from the loss of all of your clients' data.

55 https://www.inforisktoday.com/2-health-data-breaches-affect-total-220000-a-13440

56 In a similar case, hackers also had access to information such as diagnoses and medical treatment: https://www.bleepingcomputer.com/news/security/phishing-incident-exposes-medical-personal-info-of-60k-patients/

4.5.2 Data leak at FSB industry partner Sytech

On 13 July 2019, a contact person at Sytech for the Russian secret service FSB is said to have been hacked. BBC Russia reported that the hackers had stolen 7.5TB of data from the contractor's network. This data included information about numerous secret projects developed by Sytech on behalf of the Russian government and its intelligence service. The stolen data was then passed on to another hacker group, which shared it with the Russian media. According to BBC Russia, this is the largest data leak in the history of the Russian secret service.[57]

The data covers a wide range of projects, including:

1. "Mentor" was allegedly being developed for Russian military unit no. 71330, which is the radio-electronic intelligence agency of Russia's FSB. This project would monitor selected email accounts at certain intervals in order to collect information on specific phrases.
2. "Nadezhda" ("hope") is a project that aims to visualise how Russia is connected to the rest of the internet. This research is part of Russia's attempts to create a "sovereign internet" in which Russia can isolate itself from the rest of the internet.
3. "Nautilus" is a project that was developed between 2009 and 2010 to collect information about the users of social networks like Facebook, LinkedIn and MySpace.
4. "Nautilus-S" is research into the de-anonymisation of users in the Tor network through the creation of exit nodes controlled by the Russian government.

The Sytech website (www.sytech.ru) has now been deactivated and the company did not respond to requests from the BBC.

[57] https://www.bleepingcomputer.com/news/security/russian-fsb-intel-agency-contractor-hacked-secret-projects-exposed/

4.6 Crimeware

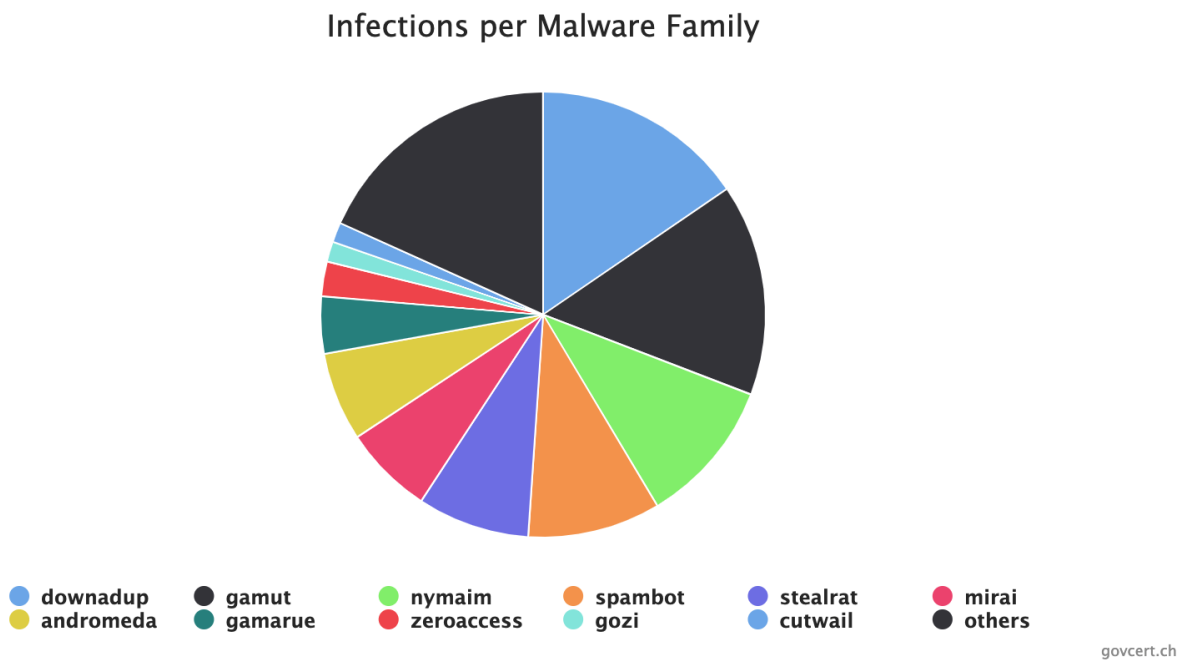

Fig. 5: Distribution of malware in Switzerland known to the NCSC through DNS sinkholes, as at 9 February 2020. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Ransomware: Latest developments

Imagine you want to buy tickets for the game of your favourite team but the online presale is currently unavailable. Instead, you confidently head to the ticket counter, but you unfortunately do not have any cash with you and the card reader is not working. The nearest cash dispenser is a few kilometres away, and you will have to walk to it because no buses are running anymore either. All this because of a malware infection that has paralysed several computer systems in order to blackmail someone.

This scenario is only partly fiction. In fact, an attack with ransomware was carried out on a Swiss football club during the six months under review, with the aforementioned consequences for the ticket and payment system.[58] A hacker attack also caused a minor disruption to public transport.[59] The scenario is fictitious in that the two events did not take place simultaneously nor in the same city.

The severe and persistent ransomware wave, which led MELANI to dedicate the main topic of the last semi-annual report to this threat, has not eased. In the last six months, there were also numerous attacks at both national and international level, and new trends were observed.

---

58 https://www.inside-it.ch/de/post/der-gehackte-fc-basel-und-die-konsequenzen-20191205

59 https://www.20min.ch/ro/news/romandie/story/Les-TPF-victimmes-d-une-attaque-informatique-23708264

Internationally, the healthcare sector continued to be strongly affected in the second half of 2019. In November, the offline computer systems of Rouen University Hospital in France were affected by ransomware, meaning that staff had to temporarily process the data manually.[60] A few months earlier, the servers of 18 hospitals in Germany were encrypted.[61] A look further afield reveals even higher figures. In the United States, the encryption Trojan Ryuk attacked the IT company Virtual Care Provider Inc. (VCPI), which hosts data in the cloud and secures and manages access from over 100 nursing homes. The attack prevented access to patient files.[62] Ryuk targets mainly companies and organisations with high turnovers in order to extort large ransoms. Companies that manage the IT infrastructures for a large number of clients are a strategic target because they allow the infection to be spread easily and can be very lucrative. In October, Ryuk encrypted the data of 400 veterinary hospitals in the United States that are owned by the National Veterinary Associates. It appears that the *Active Directory* and an *Exchange server* had already been infected in the summer. Since the infection could not be completely eliminated, it struck anew after it had had time to spread again.[63] Ryuk is often spread following a prior infection by Emotet or Trickbot Trojans, as was the case with at least one of the attacks referred to above (for more information on the multi-stage attack structure, see MELANI semi-annual report 2019/1, section 3.4.1).

However, Ryuk is not alone in using a procedure involving several infection stages. This apparently lucrative approach has recently become more common. One in Switzerland and internationally observed *dropper* is Ostap, which usually downloads the eBanking Trojan TrickBot. This spreads within company networks and places ransomware (e.g. Ryuk, LockerGoga, MegaCortex, etc.) in selected systems.

However, the healthcare sector is by no means the only target. It can affect companies in all sectors. Ransomware attacks can be both targeted and random.[64] Industry, transport, public administration, communication and sports are among the sectors affected. Recently, Ryuk ransomware targeted at least five organisations in the oil and gas industry. In at least one case, the attackers are said to have penetrated the victim's *Active Directory* servers using the *Remote Desktop Protocol* (RDP).[65] In the second half of 2019, there was an increase in the number of ransomware attacks in which the attackers scan the internet in search of *VPN* servers and open *RDP ports*, and attempt to gain access using *brute force* attacks. This access is then used as an initial vector for infiltrating a company network. In Switzerland, for example, Dharma, Phobos and Maze malware were found to be exploiting open or poorly secured RDP access points visible on the internet.

The vulnerabilities of the RDP protocol can be exploited for lateral movement in a system once infected. As early as April 2018, FireEye identified a distribution campaign with fake updates for various browsers (Chrome, Internet Explorer, Opera and Firefox) that spread Dridex,

---

60 https://www.silicon.co.uk/security/cyberwar/french-hospital-ransomware-attack-318031

61 https://www.spiegel.de/netzwelt/web/rheinland-pfalz-und-saarland-hackerangriff-auf-krankenhaeuser-a-1277759.html

62 https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/

63 https://krebsonsecurity.com/2019/11/ransomware-bites-400-veterinary-hospitals/

64 See key topic in the MELANI semi-annual report 2019/1, chapter 3.

65 https://www.darkreading.com/threat-intelligence/ryuk-ransomware-hit-multiple-oil-and-gas-facilities-ics-security-expert-says-/d/d-id/1336865

NetSupport Manager RAT, AZOrult and Chthonic malware.[66] Once this malware has spied on the network, stolen credentials and acquired rights, it acts as a *dropper* for BitPaymer and DoppelPaymer ransomware. The updates appeared on infected sites that reached potential victims, for example through "http://" redirections. In the second half of 2019, MELANI monitored compromised Swiss websites for this purpose.

The ransomware business model was previously based purely on the concept of "data decryption for money". Recently, some groups of attackers[67] have begun to exfiltrate data before launching an encryption attack. By publishing some of the data, they aim to prove their capabilities, increase pressure on the victim or simply blackmail the victim with the threat of publication. This acts a type of fall-back if the blackmailing with the data encryption is unsuccessful due to successful data recovery.[68] In November 2019, for example, the Maze group leaked almost 700MB of data that it had stolen from a security company.[69] This was followed by data from other organisations that the Maze Group had blackmailed: the medical diagnostics laboratory MDLab, the wire and cable manufacturer Southwire and a small town in Florida.[70] The group behind this ransomware is active in Switzerland as well.

A ransomware attack that becomes a data leak if the ransom is not paid seems to be a profitable business model. The operators of the encryption Trojan REvil, also known as Sodinokib, have announced that they will switch to this business model.[71]

Due to this development, every ransomware incident carries the risk of a potential data leak. This risk remains even after the incident has been resolved. Depending on the value of the data and information, it is to be expected that the criminals will likewise use these to their advantage in the future. As a result, companies that process personal data of interest are also likely to become increasingly targeted by hackers.

---

66 https://www.fireeye.com/blog/threat-research/2019/10/head-fake-tackling-disruptive-ransomware-attacks.html

67 For example, Maze, Sodinokibi and Doppel Paymer.

68 https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/; https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/

69 https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

70 https://www.bleepingcomputer.com/tag/maze/

71 https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

Recommendations:

The following internal measures have proven effective for companies: ensure complete data protection practices to increase the certainty that all data can be restored after any ransomware attack. This includes testing the data recovery process. Document your IT infrastructure, install software updates as soon as they are released, and keep your security policies up to date. Create concepts for incident management, communication and business continuity management. Determine the effectiveness of these concepts through regular tests. For effective prevention against cyberattacks, technical security measures should be accompanied by regular employee awareness raising. It is a company management's non-delegable task to monitor the implementation of these measures.

Few companies are in a position to fend off every cyberattack with certainty. You should therefore build response and recovery capabilities to mitigate the impact of an unavoidable incident.

In the second half of 2019, MELANI published updated security measures to protect against the new approach taken by ransomware attacks:

https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

Note: In the case of multi-stage infections, merely restoring data from a backup is not enough! You should have your network cleaned and reinstall the infected systems to remove the dropper successfully.

4.6.2 Emotet remains the greatest threat of infection

Emotet was again very active in Switzerland in the second half of 2019. After slightly easing in June, the group returned with full force in August, spreading malware widely and claiming many victims in Switzerland.

The approach has remained similar during this period: the Trojan continues to harvest content from previous email conversations, generate new messages from them and send these to the recipients listed in the distribution lists. The emails contain a malware attachment, often a Word document, with a macro. As soon as the victim opens the document and switches to edit mode, the malware is executed. If no additional protective measures are taken, Emotet downloads further modules and sets up persistence on the victim's computer.[72]

The group has perfected its approach and resells access to networks and systems to other players. This has made Emotet a key player in organised cybercrime. Even groups close to the state are active in the underground market and are interested in acquiring access to compromised systems, which they can then use for espionage purposes or financial gain.

[72] See MELANI semi-annual report 2019/1, section 3.4.1 and 4.6 and technical annex.

Recommendations:

Caution is called for with regard to emails not only from unknown individuals, but also from known senders, especially when a previous conversation is referenced in an unexpected message. Particularly trustworthy companies are often used as fake sender addresses. In case of any doubt, contact the supposed sender using an already known contact option or one of the ones listed on their website, for instance, and ask about the exact nature of the matter and whether they actually sent the email.

Be particularly careful when you receive Word documents. Normally, companies and organisations send PDF files for business transactions (e.g. invoices, quotations, etc.) and not Word documents.

Companies should block websites that are actively used to distribute Emotet at the network perimeter, such as web proxy or DNS. A list of such websites is provided by abuse.ch, among others.

4.7 Vulnerabilities

Errors in software development lead to vulnerabilities. That is why life cycle and patch management are of key importance. Every company (regardless of whether it is an SME or a large corporation) must keep an inventory of all its systems and applications and define a plan of what needs to be patched and when, and when each piece of software will reach the end of its life cycle. This also applies to hardware-related components such as firmware or management boards. In addition attention should be paid during software development to vulnerabilities of the *frameworks* used and their dependencies.

Vulnerabilities that can be exploited remotely over the network without authentication are particularly sensitive, such as those in *SMB* (EternalBlue[73]), *RDP* (BlueKeep[74], BlueGate[75],[76]), Citrix Netscaler[77] and Oracle Weblogic[78]. As long as a vulnerability is unknown (zero-day exploit), it has a high value and is usually used only for targeted attacks. As soon as the vulnerability becomes public and patches are available, the patches are analysed to determine the vulnerability that still remains on unpatched systems. This information is then used to write exploit codes. As soon as a publicly available exploit code is available, it is added to the toolbox of most criminal and/or state players and widely used. At the latest at this point in time, systems that are accessible remotely and contain the vulnerability are to be considered compromised. Web applications and CMSs with their various plug-ins are attacked particularly frequently and require appropriate security measures (see also "Measures to secure content management

[73] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
[74] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
[75] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0610
[76] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0609
[77] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19781
[78] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2546

systems (CMS)"[79]). While the patching of common IT systems and applications is relatively easy, it is much more difficult for control systems, IoT devices and medical equipment. A vulnerability in VxWorks, a real-time operating system which is very often used in control systems but also in medical equipment, was discovered in September 2019[80] and exposes a large number of devices, some of which are very difficult to update.

Exploiting vulnerabilities can serve various purposes:

1. Data theft for industrial espionage or blackmail
2. Distribution of ransomware
3. Taking over of a system to use it for mining cryptocurrencies
4. Sending of malware or spam
5. Point of attack for further penetration into a network

Recommendations:

In order to maintain consistent security, a company needs good life cycle and patch management across all components in use. This concerns not only the usual office automation systems, but also web applications, mobile devices, IoT devices and control components. Particular attention must additionally be paid to the frameworks and software libraries used.

In the case of critical vulnerabilities that are not resolved immediately, alternative solutions are needed (e.g. a second web browser) or ways to isolate or temporarily eliminate the vulnerability (e.g. a web application firewall for web applications).

Remote access solutions such as *VPN gateways*, *web application gateways*, email web access and exposed terminal services are among the most interesting targets for attackers, as they allow direct access to internal resources. In addition to life cycle and patch management, these always require supplementary security measures, such as two-factor authentication, *hardening* and centralised log analysis.

Those who develop applications, systems, controls and IoT devices themselves also need clearly communicated life cycle and patch management, as well as corresponding information channels to their clients. It is likewise important to provide an easy-to-find contact channel via which *security researchers* can report vulnerabilities. *Bug bounty* programmes are a worthwhile addition and can help to ensure that vulnerabilities are reported early and resolved in a coordinated manner.

79 https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-to-secure-content-management-systems--cms-.html

80 https://go.armis.com/urgent11

4.8 Preventive measures

4.8.1 New minimum standard for food supply

In recent months, the Federal Office for National Economic Supply (FONES) has published some minimum standards for the security of information technology and telecommunications systems (ICT) for various sectors. This is because production and business processes are increasingly dependent on ICT. Any failure of these systems would jeopardise companies' business activities and Switzerland's supply of critical goods and services. In order to protect against ICT-related risks and to ensure the supply of food to the population, the FONES recently published a minimum standard for ICT security in food supply. It is intended to support companies in the food industry in their efforts to avoid ICT disruptions or quickly remedy them.

This recommendation follows on from the previously published minimum standards for ICT security in water supply and the manual for the basic protection of operational technology in power supply. These industry standards are supplemented by the general ICT minimum standard, which resulted from the vulnerability analyses on cyber-risks in various industries that are important for the functioning of Switzerland. These vulnerability analyses were carried out by the FONES as part of the National strategy for the protection of Switzerland against cyber-risks" (NCS).[81]

4.8.2 Swiss police block fictitious online shops

Online shopping is convenient, but not without risk. Buyers run the risk of not receiving items they appear to order and pay for, or of receiving counterfeit goods. In addition to theft, there is also the risk that the data communicated by the buyers will be used for further offences.

Fictitious online shops have likewise spread to Switzerland, as cybercriminals also register fraudulent sites with the domain ending ".ch". At certain times of the year, for example before Christmas, such activity increases exponentially.

The cybercrime division of the Zurich Cantonal Police, in collaboration with SWITCH, the Swiss registry of .ch internet addresses (domains), prosecutes fraudulent online shops with Swiss internet domains. In December 2019, this cooperation led to an action in which 450 fictitious online shops were blocked shortly after they went online. Since the beginning of 2018, the Zurich Cantonal Police have identified and blocked a total of over 6,500 online shops of this kind.

This measure not only reduced the number of these fictitious shops, but also led to a drastic reduction in the number of newly emerging fraudulent shops with Swiss internet domains. Zurich Cantonal Police confirmed this on their website.[82] In addition, the cybercrime division explains on its website which aspects should be considered in order to avoid such traps. These include in particular domain names that have nothing to do with the goods offered, the absence

81 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-75891.html

82 https://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2019_12/1912161f.html

of the lock symbol indicating an encrypted connection to the website and the absence of an imprint as required by law.[83]

4.8.3 International operation dismantles RAT as a Service infrastructure

MELANI has repeatedly highlighted the now widespread practice of offering to perform cyberattacks or the tools to carry them out.[84] Prosecuting such offences is anything but easy. In addition to the difficulty of identifying the cybercriminals, a further obstacle is the fine line between legality and illegality, which is not always clear. This may explain how it was possible for the software developer ShockwaveTM to sell the *remote administration tool* (*RAT*) Imminent Monitor online trouble-free ever from 2012 onwards. This did not come to an end until November 2019, when an international operation by several law enforcement agencies disabled the infrastructure.

On the website where he sold his product, the author distanced himself from those who wanted to use it for illegal purposes and declined any responsibility. At the time of purchase, a declaration had to be made that the service would not be used to distribute malware. However, the product had a number of features that are atypical and superfluous for a legal remote access product. For example, it enabled the deactivation of antivirus software, included features that made detection difficult, provided access to the remote desktop that was concealed from the victim, and even enabled the mining of cryptocurrencies on the victim's computer.

The base product cost only USD 25, making it accessible to everyone. According to authorities, the product was actually purchased by over 14,500 criminals, who used it against tens of thousands of victims in 124 countries.

The operation was carried out jointly by the Australian Federal Police (AFP), Europol, Eurojust, the FBI and numerous other criminal prosecution and police agencies, and resulted in the seizure of 430 devices and the arrest of 13 users who used the product illegally.[85]

4.8.4 Bug bounty programmes – bounty hunting on the internet

To provide incentives and a way for hackers to report vulnerabilities they discover, more and more *bug bounty* programmes have been established. These are platforms that give rewards for verifiable vulnerabilities. Bug bounty programmes can take various forms and commercial platforms mediate between the hacker and the company and set the rules for both sides. Some platforms are also based on a non-commercial approach. These are typically free and community-based, but they do not provide an institutionalised intermediary function between the parties. Such projects provide a platform for security experts to report vulnerabilities in any website. From the companies' perspective, there is the possibility of starting a bug bounty programme for newly introduced software, i.e. only on an occasional basis, or introducing a permanent bug bounty programme. They can use the services of a commercial provider or set

---

83 https://www.cybercrimepolice.ch/de/fall/betruegerische-internetshops-vorsicht-bei-der-online-schnaeppchenjagd/

84 MELANI semi-annual report 2009/2, section 4.7; 2016/2, section 6.1 and 2019/1, section 3.3.

85 https://securityaffairs.co/wordpress/94525/cyber-crime/imminent-monitor-rat-shutdown.html
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

up their own company bug bounty programme for this purpose. Individual countries[86] have also developed regulations for dealing with vulnerabilities.

For years now, there has been a debate about how hackers should deal with discovered vulnerabilities in order to benefit the public and not harm companies. Two approaches have now become established: "full disclosure" and "responsible disclosure". With full disclosure, the hacker informs the company and the public at the same time. This puts the company under pressure because anyone can misuse it once the vulnerability has been revealed. Hence, this is the main point of criticism of this approach. With responsible disclosure, the hacker first informs only the company, which is then given time (usually 60 to 120 days) to fix the problem. Only then does the hacker publish the vulnerability.[87]

The principle of responsible disclosure generally applies when participating in bug bounty programmes. This includes the following elements:

1. The company has sufficient time (usually 60 to 120 days) to verify and fix the vulnerability.
2. Third parties must not be informed about the vulnerability.
3. Tests on the vulnerabilities must not interfere with the company's services, products or regular operations.
4. Data must not be exposed or shared.
5. Demands (e.g. for specific monetary compensation) in connection with the reporting of a vulnerability will not be considered.

This practice will probably be increasingly used by companies in the future, which means that the future looks bright for qualified bounty hunters and internet security researchers.[88] Existing bug bounty programmes such as that of Swisscom are delivering impressive results. The telecommunications company has received and processed 844 vulnerability reports. Of these, 427 reports led to a correction and Swisscom paid out rewards amounting to CHF 350,000. The types of vulnerabilities reported range from low-level *cross-site scripting* (XSS) to highly critical *zero days* in known and widely used products.[89]

Hacktivists have recently launched a new form of bug bounty programme to reward vigilante hackers and hacktivists who perform hacks and leak data in the name of public interest. This programme only has its name in common with traditional programmes, which are designed to make a significant contribution to security and to identify and fix vulnerabilities in security systems before they are exploited.

---

86 Such as the Netherlands: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure

87 https://www.zeit.de/digital/datenschutz/2013-09/bug-bounty-hack/seite-2

88 https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

89 Figures since 2018, https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

The National Cybersecurity Centre (NCSC) is in the process of developing a responsible disclosure policy for Switzerland.

It is already possible to report any information on vulnerabilities to incidents@ncsc.ch

5 Research and development

5.1 Ransomeware: everything stops working, and then what?

The practice by criminals of obtaining money by encrypting the victim's data has already been reported on in several MELANI semi-annual reports[90]. Corresponding technical guidelines on how to protect yourself from ransomware attacks are available on the MELANI website.[91]

Yet, even the best technical precautions cannot provide 100% protection against infection. 2019 saw a certain degree of professionalisation, in particular as regards groups specialising in ransomware as a business model. It is no longer simply a question of your local or currently network-accessible data being encrypted after you click on a spoofed telephone bill or job application. Instead, following the initial infection, the attackers spend a long time inside the targeted network in order to gain access to as many sensitive systems and areas as possible, including online backups. This guarantees maximum damage when the actual encryption software finally goes to work.

In some circumstances, this multi-stage approach allows the ICT to detect and fight off the attackers before serious damage is caused. MELANI receives regular reports from security firms and partner organisations about infections of corporate networks, and forwards them to the affected network operators. By the same token, however, the multi-stage approach can have horrendous consequences when the attackers activate the ransomware itself, bringing key systems in both the primary infected company and even productive sites abroad to an abrupt standstill because their network connections run via the company headquarters.

5.1.1 Successful ransomware is not an ICT problem

Ransomware groups base their business model on exerting the greatest possible pressure on affected companies and organisations, in order to lend weight to their demands. These groups therefore focus on paralysing ICT-supported business processes. Even if ICT is the cause of the problem, often its hands are tied as regards rapidly solving the actual problem, namely how

---

90 MELANI semi-annual reports 2011/2, section 3.5; 2013/2, section 3.1; 2014/2, sections 3.6 and 5.3; 2015/1, section 4.6.1.5; 2015/2, section 4.5.1, 2016/1, sections 4.6.3 and 5.4.3; 2016/2, section 6.1; 2017/1, chapter 3; 2017/2, section 5.4.2; 2018/2, sections 4.5.4 and 5.3.5; 2019/1, chapter 3

91 https://www.melani.admin.ch/melani/en/home/themen/Ransomware.html

to restore critical business processes and activate the business continuity plan which the management has hopefully set up in advance.

Following a successful ransomware attack, unaffected systems and processes, or those that can be operated without ICT support, should be identified as quickly as possible.

The use of legal experts is necessary right from the start because the attackers will, at least briefly, have had access to data. Accordingly, the provisions of the Data Protection Act apply, as well as the EU's General Data Protection Regulation (GDPR) for companies operating in the European Union. In a second step, it should rapidly be ascertained what, if any, ICT systems can be restored using available backups and snapshots. It is generally a good idea to consult an external ICT security service provider as, owing to their experience with ransomware incidents, they can assess the true impact and remaining options for action relatively efficiently.

Once the first two steps have yielded the necessary facts, in the third step the management will have to address the question of whether the impact and the associated costs warrant giving in to the criminals' demands. MELANI strongly advises against paying ransom money, because this merely serves to reinforce and fund the ransomware group's business model. There is also no guarantee that the criminals hold true to the agreement. It is important that the companies concerned contact the cantonal police immediately, file a complaint and discuss the next steps with them.

5.1.2 Prosecution – more than just handcuffs

After the immediate initial internal measures, the incident handling leads to an often underrated but indispensable fourth step, regardless of whether the victim has decided to pay or not: the involvement of the prosecution authorities.

Companies generally do not bother to involve prosecution authorities in ransomware incidents. There is a commonly held view that the police can do nothing against foreign cybercriminal groups. Yet, the prosecution authorities do have experience with such incidents, and carry out cross-border investigations into ransomware groups. However, should a company decide to pay the ransom, the police have officers who are specially trained in making contact with the perpetrators.

So involving the authorities has multiple benefits. It allows them to gather evidence, not just for use in the case at hand but also to support prosecutions that have already been launched in connection with other cases and to tie in investigations with each other. De facto, therefore, the prosecution authorities act as their own competence centre for ransomware incidents. They can provide advice or, depending on the ransomware group, may have knowledge that could prove useful for the staff and external service providers working to restore the systems.

5.1.3 Plan B, as in "business continuity management"

In 2019, Swiss manufacturing was a popular target for ransomware attacks. The logic is simple: If you can't produce anything, you will, quite understandably, be more prepared to pay a high ransom in order to avoid several days of lost production. The initial impact of the news that everything has stopped due to a ransomware attack has been described by one manufacturer as a "near-death experience".

Ransomware attacks the availability of processes and is thus very similar to attacks on the availability of webshops (DDoS attacks). Ideally, the company should be brought to a standstill and rendered willing to pay a ransom in order to get up and running again. Businesses that are heavily dependent on ICT are thus badly affected. Consequently, this kind of attack aims to shut down the ICT systems first.

One of the tasks of any company's or organisation's management is to ensure that critical business processes can also continue to function independently of the ICT unit if necessary. Business continuity management, as this process is called, must be established before a cyberattack takes place.

5.2 Escalating conflicts in the Middle East also threaten business partners in Switzerland

Organisations that have business relations with the Middle East could run the risk of being used as the springboard for attacks against targets connected with the ongoing conflicts in that region.

In addition to the open warfare in Syria and Yemen, the Middle East has also been a risky region as regards information security for some time now. The regional governments' monitoring regime is therefore much more rigorous than that in most European states. Last year, Reuters[92] reported on Project Raven, in which US intelligence service veterans helped the United Arab Emirates to set up their offensive cybercapacity. According to the news agency, Project Raven was later transferred to the company DarkMatter. The Kingdom of Saudi Arabia made headlines with the use of GovWare ahead of the murder of journalist Jamal Khashoggi,[93] and also probably against Jeff Bezos, founder of Amazon and owner of the Washington Post.[94] Elsewhere, the Israeli armed forces carried out an air strike against a building which, according to the Israelis, was being used by the Palestinian Hamas to launch cyberattacks against them.[95]

In this highly charged environment, over recent years the governments and private sector companies concerned, especially operators of critical infrastructures, have regularly invested in their information security arrangements. These battle-hardened organisations present an increasingly impenetrable target, which is why the attackers began to look for opportunities at other points along the supply chain, in Europe[96,97] and North America.[98] In addition to industrial

92 https://www.reuters.com/investigates/special-report/usa-spying-raven/

93 https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/

94 https://techcrunch.com/2020/01/22/bezos-nso-group-hack/

95 https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/

96 MELANI semi-annual report 2018/2, section 5.2.2

97 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/

98 https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

suppliers,[99] ICT service providers[100] present a particularly rewarding intermediate target from which to launch the actual attack against the adversary organisation.

Since no de-escalation is to be expected in the Middle East in the foreseeable future, Swiss organisations with links to the Middle East should look into the risk of cyberattacks originating in the region. It does not matter if they are a supplier, service provider or simply the business partner of an organisation with a peripheral connection to the conflict region: they can find themselves in the attackers' crosshairs. Groups such as APT33,[101] Oilrig,[102] Muddywater,[103] Leafminer[104] or APT39/Chafer[105] spare no effort to find a suitable gateway for their activities.

In the referenced descriptions of the groups in the MITRE ATT&CK[106] knowledge base on attackers' methods and techniques, the attack methods used and appropriate mitigation measures are discussed. Clear implementation and consistent application of multi-factor authentication prevent many attacks of this kind, or at least make them much more difficult.

5.3 New business models for even whiter laundry

Cybercrime is a typical example of sophisticated division of labour. Cybercrime in all its forms can be regarded as a series of clearly defined tasks which often involve specialist players. These people constantly aim for the greatest possible efficiency, thereby contributing to the overall cost-effectiveness of this phenomenon. The laundering of illegally obtained money occupies a special place among these different specialisations. Indeed, the entire criminal activity chain would be pointless if there were no way of laundering the money for legitimate use afterwards. This activity is flourishing: According to a study published by Bromium, between USD 80 billion and USD 200 billion are laundered by cybercriminals every year.[107]

The development of virtual currencies was a revolution for transactions resulting from cybercrime activities. Today, a whole range of criminal activities are funded through virtual currencies like bitcoin. Despite transactional documentation with blockchain, a virtual currency can be processed to make it difficult to trace, for example by using mixers or tumblers.[108] However, the spoils of other cybercrime activities still come in the form of traditional currency, for instance in the case of computer fraud using eBanking Trojans or payments with a stolen credit card. This kind of activity requires more traditional money laundering methods. It has long been documented that private individuals are hired to make their bank accounts available for receiving money and transferring it to another account, in return for a commission. These

---

99 https://www.wired.com/story/iran-apt33-industrial-control-systems/

100 https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain

101 https://attack.mitre.org/groups/G0064/

102 https://attack.mitre.org/groups/G0049/

103 https://attack.mitre.org/groups/G0021/

104 https://attack.mitre.org/groups/G0077/

105 https://attack.mitre.org/groups/G0087/

106 https://attack.mitre.org/

107 https://www.bromium.com/press-release/up-to-200-billion-in-illegal-cybercrime-profits-is-laundered-each-year-comprehensive-research-study-reveals/

108 Service enabling large-value cryptocurrency transactions to be masked by passing them through individual, very active wallets, where they are broken down into many small transactions.

people are called money mules or financial agents. True to their opportunistic approach, criminals are also trying to take advantage of existing platforms. Well known money laundering methods are based on, for example, micropayments via PayPal or overpriced eBay sales.

At the moment, the success of platforms like Airbnb or Uber is attracting criminals' attention. These platforms use new technology to allow service providers to contact their customers directly. A typical example of the new money laundering method is a "ghost ride" with Uber. The criminals predominantly recruit Uber drivers who are likely to look the other way and try to top up their monthly pay. For this purpose, announcements are made on underground forums. The criminal books a ride and pays the driver using the required method. But the journey is completely fictitious: the driver never even leaves home. Drivers refund the money to the criminals, keeping a percentage for themselves as a reward. A very similar pattern has been observed on the Airbnb accommodation platform. In this case, criminals pay for an apartment that they are never going to use. Here, too, the landlord pays the money back and deducts a commission.

The fight against cybercrime aims to break this highly profitable activity chain by attacking one of the links in the chain. These money laundering methods are therefore a frequent focus of police activity. For example, in December 2019, Europol announced that an operation involving 31 countries had resulted in the arrest of 228 money mule recruiters.[109] Already in May of that year, the same authority announced that it had shut down Bestmixer.io in a joint action with the Dutch and Luxembourg authorities. The service had been used to launder around USD 200 million over a one-year period.[110] As the examples of Uber and Airbnb misuse show, there is no lack of ideas and knowledge among criminals when it comes to diversifying their money laundering models. As well as police work and the awareness campaigns against potential money mules, part of the solution undoubtedly lies in the measures introduced by the misused online services themselves, and in their ability to identify misuse for money laundering purposes.

[109] https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering

[110] https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-best-mixerio-taken-down

6 Published MELANI products

6.1 GovCERT.ch blog

6.1.1 Trickbot – An analysis of data collected from the botnet

We are monitoring various threats and in this context we have collected quite a lot of data about the Trickbot botnet in the past few years. This paper is based on an analysis of selected aspects of our Trickbot data collection. Our analysis consists of two main parts. In the first part we consider the PE timestamps of Trickbot droppers (the binaries being distributed by the Trickbot operators) and of the respective payloads (the PE binaries which are unpacked and then executed once a dropper is executed). The analysis is based on approximately 2,100 droppers and corresponding payloads which were collected between July 2016 and February 2019.

https://www.govcert.admin.ch/blog/37/trickbot-an-analysis-of-data-collected-from-the-botnet

6.2 MELANI newsletter

6.2.1 Encryption Trojan update: new approaches

30.07.2019 – In recent weeks, Swiss companies have become the target of a new kind of attack, in which unknown attackers successfully infiltrate corporate networks and encrypt large amounts of their data by means of an encryption Trojan. A number of renowned Swiss companies have been affected by the attacks.

https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

6.2.2 Microsoft discontinues support for older products: danger looming

16.12.2019 – Microsoft announced that support and thus updates for various older products would be discontinued on 14 January 2020. The following products are affected: Windows 7 operating system, Windows Server 2008 and Windows Server 2008 R2.

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/microsoft-end-of-life.html

7 Glossary

Term	Description
APT Advanced persistent threat	Various techniques and tactics are used in this attack. It is specifically targeted at a single organisation or country. Very significant damage can be done in most cases. Therefore, attackers are willing to invest a great deal of time, money and knowledge in the attack and generally have considerable resources at their disposal.
Backdoor	Backdoor refers to an often intentionally incorporated software feature that allows users to gain remote access to a computer or protected function of a computer program by circumventing the usual access controls.
BGP Border Gateway Protocol	Border Gateway Protocol is the routing protocol used on the internet to determine the path of data packets between networks.
Bitcoin	Bitcoin is a decentralised payment system that can be used worldwide, as well as the name of a digital currency unit.
Bot	Comes from the Slavic word "robota" meaning work. Refers to a program that automatically carries out certain actions after receiving a command. Malicious bots can control compromised systems remotely and have them carry out any kind of arbitrary action.
Botnet	Several bots can form a network, which is controlled via a command & control infrastructure.
Brute force	Brute force is a method for solving problems in the fields of computer science, cryptology and game theory, based on trying out all possible cases.
C2 Command and control	Command and control infrastructure of botnets. Most bots can be monitored and receive commands via a communication channel.
CaaS Cybercrime-as-a-Service	Cybercrime as a service that can be purchased enables technically inexperienced criminals to carry out illegal activities on the internet with easy-to-use tools.
CEO fraud	CEO fraud occurs when perpetrators instruct the accounting or finance department in the name of the CEO to make a payment to the (typically foreign) account of the scammers.

CPU / processor	The CPU (central processing unit) is another term for processor, the central unit in a computer, and contains the logic circuits to run a computer program.
Cryptomining	Mining creates new blocks and then adds them to the block chain. The process requires considerable processing power and is therefore remunerated.
DDoS	Distributed denial of service attack. With a DoS attack, the victim's service or system is attacked simultaneously by many different systems, bringing it to a standstill and rendering it unavailable.
Defacement	Unauthorised alteration of websites.
DNS Domain name system	With the help of DNS, the internet and its services can be utilised in a user-friendly way, as users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
Drive-by infection	Infection of a computer with malware simply by visiting a website. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
Dropper / downloader	A dropper or downloader is a program that downloads and installs one or more instances of malware.
Exploit kits	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Financial agent	A financial agent works as a legal money broker and thus engages in financial transfers. Recently, this term has been used in connection with illegal financial transactions.
GPS Global Positioning System	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
Internet of Things	The term "Internet of Things" (IoT) describes the networking and collaboration of physical and virtual objects.
ISP Internet service provider	Internet service providers are providers of services, content or technical services that are required for the use or operation of content and services on the internet.
JavaScript	An object-based scripting language for developing applications. JavaScripts are program components integrated in HTML code enabling specific functions in internet browsers. An example could be checking user

	input in a web form. It is possible to verify that all the characters entered when a telephone number is requested are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the computer of the website visitor. Aside from useful features, unfortunately dangerous functions can also be programmed. Unlike ActiveX, JavaScript is supported by all browsers.
Malspam	Bulk emails with which malware is distributed.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Man-in-the-middle attacks (MITM)	Attacks in which the attacker infiltrates the communication channel between two partners unnoticed and is thereby able to spy on or even modify their data exchanges.
Metadata	"Metadata" and "meta-information" refer to data containing information about other data.
Monitoring and control systems (MCS)	Monitoring and control systems (MCS) consist of one or more devices that control, regulate and/or monitor the behaviour of other devices or systems. In industrial production, the term "industrial control systems (ICS)" is commonly used.
MSP Managed service provider	A managed service provider is an IT service provider that supplies and manages a defined set of services for its clients.
NAS Network-attached storage	Hard disk storage or file server connected directly to a network.
Patch	Software which replaces the faulty part of a program with an error-free part, thereby eliminating a vulnerability, for example.
Peer to peer	Network architecture in which the systems involved can carry out similar functions (in contrast to client-server architecture). P2P is often used for exchanging data.

Phishing	Fraudsters phish in order to obtain confidential data from unsuspecting internet users. For example, this can be account information from online auctioneers (e.g. eBay) or access data for online banking. The fraudsters take advantage of their victims' credulity and helpfulness by sending them emails with false sender addresses.
PowerShell script	PowerShell is a Microsoft cross-platform framework for automating, configuring and administering systems, consisting of a command line interpreter and a scripting language.
Proxy	A proxy is a communication interface in a network. It works as a mediator, receiving queries on the one side and then making a connection on the other side via its own address.
RaaS Ransomware-as-a-Service	Ransomware as a service that can be purchased enables technically inexperienced criminals to carry out attacks with easy-to-use tools.
Ransomware	Malware that typically seeks to persuade its victims to pay a ransom by encrypting data.
RDP Remote Desktop Protocol	A Microsoft network protocol for remote access to Windows computers.
Remote administration tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
Router	Computer network, telecommunication or internet devices used to link or separate several networks. Routers are used in home networks, for instance, establishing the connection between the internal network and the internet.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
SMB protocol	Server message block (SMB) is a network protocol for file, printing and other server services in computer networks.
SMS	Short Message Service for sending text messages (160 characters maximum) to mobile phone users.
Social engineering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order

	to gain access to confidential data or to prompt them to perform certain actions, for example. Phishing is a well-known form of social engineering.
Spam	Spam refers to unsolicited and automated mass advertising, a category into which spam emails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Spear phishing	Targeted phishing attacks. The victims are led to believe that they are communicating via email with someone they know, for example.
Spoofing	Falsification of address elements or signals in order to deceive the recipient person or device.
Supply chain attacks	Attack that attempts to infect the actual target by infecting a company in the supply chain.
Take-down	Term used when a provider takes a website offline due to fraudulent content.
TCP/IP	Transmission Control Protocol/Internet Protocol is a suite of network protocols, also referred to as the internet protocol family because of its great importance for the internet.
TLD Top-level domain	Every name of a domain on the internet consists of a sequence of character strings separated by full stops. The term "top-level domain" refers to the last name in this sequence, constituting the highest level of the name resolution. If the full domain name of a computer or website is de.example.com, for instance, the right-most item in the sequence (com) is the top-level domain of this name.
Two-factor authentication	Two-factor authentication is used to increase security. For this, at least two of the following three authentication factors are required: 1. Something you know (e.g. password, PIN, etc.); 2. Something you have (e.g. a certificate, token, scratch list, etc.); 3. A unique body feature (e.g. fingerprint, retinal scan, voice recognition, etc.).
UDP	The User Datagram Protocol, short UDP, is a minimal, connectionless network protocol that belongs to the transport layer of the internet protocol family.
USB	Universal Serial Bus. Serial communication interface which enables peripheral devices such as a keyboard,

	mouse, external data carrier, printer, etc. to be connected. The computer does not have to be switched off when a USB device is unplugged or plugged in. New devices are usually detected and configured automatically (depending on the operating system).
Vulnerability	A loophole or bug in hardware or software through which attackers can access a system.
Watering hole attacks	Targeted infection with malware using websites which tend to be visited only by a specific user group.
Website infection	Infection of a computer with malware simply by visiting a website. The websites concerned often have reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
WLAN	WLAN stands for Wireless Local Area Network.
Worm	Unlike viruses, worms do not need a host program to spread. Instead, they use vulnerabilities or configuration errors in operating systems or applications to spread independently from one computer to another.
Zero-day vulnerabilities	Vulnerability for which no patch exists yet.
ZIP file	ZIP is an algorithm and file format for data compression to reduce the storage space needed for archiving and transferring files.