Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

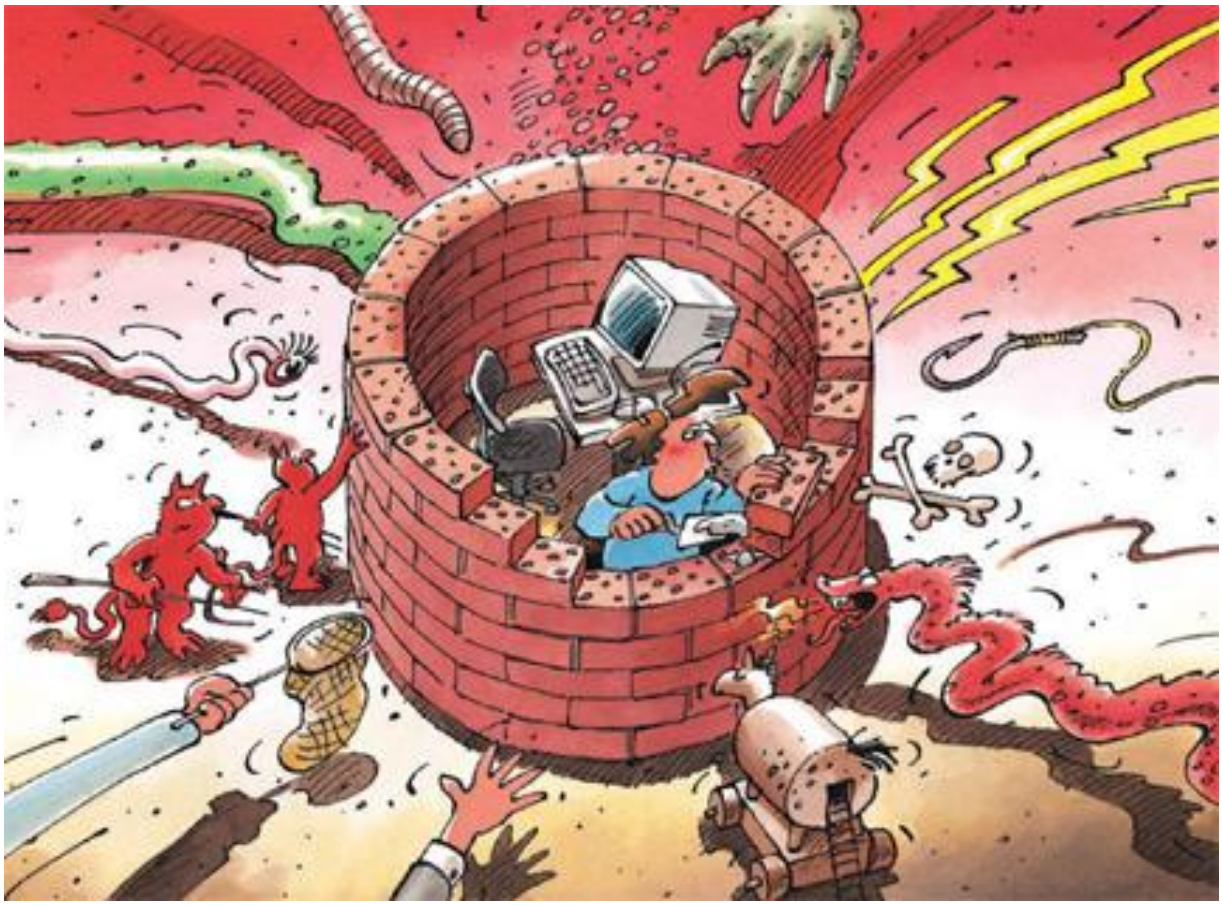
Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

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

Information Assurance

Situation in Switzerland and internationally

Semi-annual report 2013/II (July – December)



Contents

1 Focus areas of issue 2013/II 3

2 Introduction 4

3 Current national ICT infrastructure situation 5

3.1 Extortion via CryptoLocker & Co 5
3.2 Banner ads spread malware 6
3.3 Websites repeatedly compromised 7
3.4 Advance payment fraud goes professional 8
3.5 Bank statements sent to wrong addresses 9
3.6 Switzerland also affected by the theft of Schengen Information System data 9
3.7 NZZ inaccessible – technical problems 10
3.8 Switzerland wins first Cyber Security Alpine Cup 11
3.9 Malware also on Linux systems 12
3.10 NTP amplification attacks – Swiss infrastructure already abused 12

4 Current international ICT infrastructure situation 13

4.1 Further revelations about the NSA and GCHQ 13
4.2 APT - reinventing methods 16
4.3 Details of millions of Adobe customers stolen 17
4.4 Attacks on Target retail chain outlets 18
4.5 Second SIM cards and the consequences 19
4.6 Hacked DES algorithms and the consequences for SIM cards 20
4.7 Industrial and domestic Control Systems 20
4.8 The Syria conflict – war of information 2.0 22
4.9 When DDoS diverts attention from other attacks 22
4.10 Hackers and smugglers in cahoots 23
4.11 EU Parliament adopts more stringent penalties for cybercriminals 23

5 Trends/Outlook 24

5.1 The Internet at a crossroads or business as usual 24
5.2 Bitcoin - success, but at a price 25
5.3 The role of cyberspace in conflicts 27
5.4 Virus detection in the 21st century, what will succeed signature-based anti-virus programs? 28
5.5 Attacks on home routers 31
5.6 Items of parliamentary business related to information assurance issues 33

6 Glossary 34

1 Focus areas of issue 2013/II

- **Further revelations about the NSA and GCHQ**
  The various activities of the US National Security Agency (NSA) and the UK Government Communications Headquarters disclosed on the basis of Edward Snowden's documents continued to generate huge interest in the second half of 2013. The full picture began to emerge in the second half of the year of the extensive, all-encompassing data collection by these intelligence services. These revelations highlight the problems that are inherent in a transnational facility like the internet, which every single individual and state can participate in and use as they choose and as permitted by national legislation, without having to give any thought to the global repercussions.

  ► Current situation internationally: Chapter 4.1
  ► Trends/Outlook: Chapter 5.1

- **Bitcoin: success, but at a price**
  Bitcoin is a decentralised digital currency, which means that it works independently of a central issuer. This is what sets it apart from traditional currencies and also from many other digital currencies. Bitcoin's growing popularity raises many issues, particularly in terms of security, but also with respect to the legal status and regulation of these currencies.

  ► Trends/Outlook: Chapter 5.2

- **Ransomware on the rise**
  A very widespread type of ransomware displays a message on infected computers that appears to be from a police authority. Another more serious issue is a Cryptolocker malware infection, which was observed for the first time in Switzerland in November 2013. Cryptolocker encrypts all of the data on the hard disk and all other data carriers connected to the computer, and making the data inaccessible.

  ► Current situation in Switzerland: Chapter 3.1

- **Theft of large amounts of data**
  Data theft has once again been reported, affecting millions of datasets. According to figures released by Adobe, 38 million of its clients had their details, passwords and credit card details stolen. The Target retail chain has also been affected by data theft. Reports claim that the details of 40 million credit and debit cards as well as the personal details of 70 million customers were stolen.

  ► Current situation internationally: Chapter 4.3, Chapter 4.4

- **Industrial and domestic Control Systems – a growing number of systems on the internet**
  It is now relatively easy and cheap to purchase systems with remote query and control functions or to upgrade an existing system by installing a communications interface. Accordingly, apart from the function and user-friendliness of a remote access solution, special attention must also be paid to protecting against unauthorised manipulation. For this reason, MELANI published a checklist for the protection of industrial control systems in October 2013.

  ► Current situation internationally: Chapter 4.7

2 Introduction

The eighteenth semi-annual report (July-December 2013) of the Reporting and Analysis Centre for Information Assurance (MELANI) presents the most significant trends involving the threats and risks arising from information and communication technologies (ICT). It provides an overview of the events in Switzerland and abroad, sheds light on topics in the area of prevention, and summarises the activities of public and private players. Explanations of jargon and technical terms (*in italics)* can be found in a **glossary (Chapter 6)** at the end of this report. Comments by MELANI are indicated in a shaded box.

Selected topics covered in this semi-annual report are outlined in **Chapter 1.**

Chapters 3 and 4 discuss breakdowns and failures, attacks, crime and terrorism connected with ICT infrastructures. Selected examples are used to illustrate important events of the second half of 2013. Chapter 3 discusses national topics; Chapter 4 international topics.

Chapter 5 contains trends and an outlook on developments to be expected.

Chapter 5 contains for the first time ever selected items of parliamentary business related to topics in the field of information assurance.

3 Current national ICT infrastructure situation

3.1 Extortion via CryptoLocker & Co

Ransomware, or extortionate *malware*, which is used to extort money from the owners of infected computers, has been around for some time now. A very widespread type of ransomware displays a message on infected computers that appears to be from a police authority such as the Federal Crime Office or the Federal Department of Justice and Police (FDJP). The message demands the payment of a fine on the pretext that illegal data was found on the infected computer. If the payment is not made, the computer will remain blocked. However, this type of malware is relatively harmless compared to other ransomware as it does not cause any real harm to files on the computer and the block can be removed by relatively simple means.

In most cases, the pest can be removed by analysing the computer with the most up-to-date *Antivirus Live CD*. A guide on producing and using an Antivirus Live CD can be found on the pages of the Cybercrime Coordination Unit Switzerland (CYCO).[1]

Much more serious is a CryptoLocker malware infection, which was observed for the first time in Switzerland in November 2013. CryptoLocker also encrypts all of the data on the hard disk and all other data carriers connected to the computer, meaning that the victim can no longer access it. We can only assume that this malware is not widespread within Switzerland. Nevertheless, the personal stories behind each of the cases are dramatic: private individuals have lost their entire digital past for instance. In the case of SMEs, important business data is often affected, which could endanger the company's existence if a *backup copy* has not been made of the data or if the backup is defective.

CryptoLocker appears to be spread by infected e-mail attachments and via bogus websites, resulting in what are known as website infections or *drive-by downloads*. In some cases, the device in question was already infected with a different malware, which then downloaded CryptoLocker. There are now copiers who have developed similar malware and are bringing it into circulation.

After the computer has been infected, the victim receives a message containing a demand for money from the criminals. In return for the money, the victim should receive the *decryption key* for recovering the files. Although various antivirus products are able to locate and eliminate the malware, it is too late in most cases because the files on the computer have already been encrypted. Therefore, the real problem is not removing the malware, but recovering the original data. Ransomware with an integrated data encryption developed up until now used a fixed, programmed key which could simply be extracted from the *source code*. This is no longer possible with CryptoLocker: a separate key is generated on a command and control server for every single victim. Therefore, there currently appears to be no method for decrypting the data without the key that only the fraudster knows. Nevertheless, MELANI advises against giving in to the criminals' demands and making a payment. After all, there is no guarantee that the criminals will actually send the victim the key that is needed to decrypt the files and there is every possibility that the extortioners will take advantage of the victim's willingness to pay and demand more money.

---

[1] Guide to producing an Antivirus Live CD from the Cybercrime Coordination Unit Switzerland CYCO: http://www.cybercrime.admin.ch/content/kobik/de/home/dokumentation/informationen/2012-07-06.html

Together with Swiss Internet service providers, MELANI has adopted measures to minimise the CryptoLocker threat.

CryptoLocker clearly illustrates the importance of making regular backup copies and ensuring the quality of these.

What makes matters worse in the case of CryptoLocker is that external hard disks connected to the computer are also affected by the encryption. A particularly tragic case was one where CryptoLocker struck just as a backup copy was being made and destroyed the original and backup data at the same time. Therefore, it is advisable to use two hard disks alternately and to have the data carrier connected to the computer only when making the backup copy.

Network drives are currently not affected by the encryption, provided they have not assigned any network drive letters. However, the malware will most certainly continue to be developed so that it could possibly contain both this and other functions in the future too.

3.2 Banner ads spread malware

Ad servers are used to place advertisements on websites. The advertisements themselves can come from various advertisers and advertising networks. OpenX and Revive Adserver, which is based on this, are examples of well-known ad servers that are frequently used. Ad servers are an extremely interesting target for criminals, as malicious code can very easily be spread in the form of manipulated advertisements via several websites, some of which are visited a lot. A common tactic is to place an *iframe* in addition to the banner ad. An iframe is an *HTML* statement that can be used to embed external content, such as a link to a page with malware.

An aggravating factor is that multiple security vulnerabilities were found in OpenX in the last six months. Combined with the fact that many administrators do not apply updates promptly, this results in a major security risk.

For example, in July 2013, an OpenX security vulnerability was discovered that allows the attacker to inject arbitrary *script code* or HTML script (*cross-site scripting*). In August 2013, it transpired that a *backdoor* had existed in a free version of OpenX for a prolonged period. All those who used this version had also automatically installed the backdoor which attackers incorporated in the software for their purposes and also exploited actively. September saw the detection of a further vulnerability in OpenX and Revive that enabled registered users to execute arbitrary *PHP code* on the server. Finally, in December, a very serious vulnerability affecting both OpenX and Revive was discovered. This vulnerability enabled attackers to access the server's database directly (*SQL injection*) and manipulate the ad server's data without having any access data whatsoever.

In Switzerland, incidents affected various websites, some of which are used very extensively. MELANI generally recommends patching Internet-exposed software regularly and maintaining it in a *lifecycle management* process. Moreover, the corresponding log files should be checked regularly and anomalies investigated. The measures to secure *Content*

Management Systems[2] can also be applied analogously to ad servers. Furthermore, for OpenX and Revive, there are checklists[3] with the most important tasks to be conducted regularly.

3.3 Websites repeatedly compromised

Phishing sites are an everlasting problem. While in the past domains were deliberately registered by fraudsters in order to place phishing sites, today they prefer to check existing websites for weaknesses and then exploit them to place a phishing site (usually in a subdirectory). As described in the last MELANI Semi-annual report 2013/1[4], it takes little effort to find websites with *weaknesses*, as many website operators do not regularly update their *application software* – for example, content management systems.

One of MELANI's aims is to ensure phishing sites are removed from the Internet as quickly as possible. To this end, MELANI writes to the provider's contact point (*abuse unit*) once a phishing site has been discovered and requests that the corresponding website be removed from the Net. It has become established international practice for each web host to have an abuse unit that receives reports on fraudulent sites.

However, the processes and reaction times for the removal of fraudulent sites are not uniformly regulated and differ greatly. While some providers immediately remove the relevant sites themselves, other providers first inform the website owners and ask them to take the necessary measures. Only if the owners do not react within a timeframe set by the provider do the providers take action themselves.

The availability of abuse units also varies considerably. While some web hosts offer a 24-hour service, others work only during office hours. This leads to delays particularly if the host is in another time zone or if the phishing incident occurs at the weekend or during a public holiday.

However, the differences are not limited to speed and availability. Various approaches are also taken for dealing with an incident. For example, if a CMS weakness was exploited to place a phishing site, it is not sufficient simply to delete the phishing site. The website owner must also be made aware of the fact that the applications used are to be fully updated. In the absence of updating, the same websites will attract negative attention time and again with repeatedly placed phishing pages or malware. This is also clearly demonstrated by the following case, which was observed in Switzerland in the second half of 2013. Between October and December 2013, the same Swiss website was abused a total of three times in succession in order to place phishing sites against various financial service providers and credit card companies.

There is no obligation for hosting providers to create an abuse service. However, a network is quickly *blacklisted* if it is not looked after sufficiently. This is particularly the case with spam. If there is a spammer in a network, the *IP range* can quickly be included in a spam

---

[2] MELANI checklists and instructions: measures to secure Content Management Systems (CMS) http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=en (as at 20 February 2014)

[3] https://checkpanel.com/checklist-templates/openx-maintenance (as at 20 February 2014)
https://checkpanel.com/checklist-templates/revive-maintenance (as at 20 February 2014)

[4] MELANI Semi-annual report 2013/1, Chapter 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as of 20 February 2014)

filter unless the provider takes appropriate action, with the result that clients can no longer send e-mails. This principle is not applied consistently in the case of phishing websites, which gives individual providers leeway in the processing of phishing websites.

3.4 Advance payment fraud goes professional

Aside from credit card details, e-mail access data is also increasingly being stolen. But what is e-mail access data actually used for? The type of fraud that uses e-mails claiming that the sender is stuck abroad and is in difficulty is already familiar from previous semi-annual reports.[5] As the perpetrator has access to the e-mail account, he can lead the recipient to believe that the e-mail is genuinely from the person he or she knows. The victim is then urged to pay a sum of money.

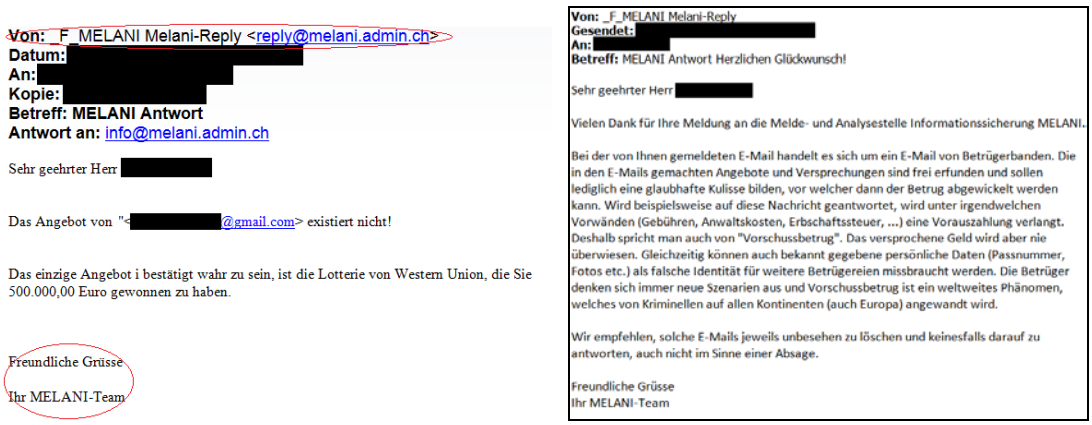
Another variant that continues to be observed is the searching of e-mails for any form of communication with a financial institution. In this case, the fraudster subsequently tries to re-establish this communication with the bank employee and persuade him or her to trigger a payment. This variant is seen primarily abroad, but there are also individual cases in Switzerland.

A far more perfidious variant was observed by MELANI at the end of 2013. It all started with a simple advance payment fraud e-mail. In such a fraudulent e-mail, the victim is given the prospect of winnings or large sums of money from inheritances. Once the victim has taken the bait, requests follow for alleged advance payments that are necessary for profit tax, inheritance tax, transaction tax or something else. However, the victim never sees a penny of the promised money.

In the case described, the victim was sceptical and decided to ask the Reporting and Analysis Centre for Information Assurance (MELANI) if the e-mail was genuine and if he should respond to the offer. As always in such cases, MELANI gave the standard reply saying to stay away from such e-mails, to delete them and not to contact the fraudsters. The victim's reaction was quite astonishing, as he wrote again to enquire whether MELANI really believed that the transaction was above board and he should indeed pay the requested taxes in advance.

Confused, MELANI phoned the person to make it clear that the e-mail was fraudulent and that he should by no means make a payment. During the telephone conversation, it immediately became clear that the fraudsters had manipulated the e-mail from MELANI in the victim's inbox, changing it to encourage the victim to pay. The fraudsters thus had access to the victim's e-mail account in order to carry out the manipulation in question.

[5] MELANI Semi-annual report 2012/1, Chapter 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 20 February 2014)



Von: _F_MELANI Melani-Reply <reply@melani.admin.ch>
Datum: [redacted]
An: [redacted]
Kopie: [redacted]
Betreff: MELANI Antwort
Antwort an: info@melani.admin.ch

Sehr geehrter Herr [redacted]

Das Angebot von "<[redacted]@gmail.com> existiert nicht!

Das einzige Angebot i bestätigt wahr zu sein, ist die Lotterie von Western Union, die Sie 500.000,00 Euro gewonnen zu haben.

Freundliche Grüsse

Ihr MELANI-Team

Von: _F_MELANI Melani-Reply
Gesendet: [redacted]
An: [redacted]
Betreff: MELANI Antwort Herzlichen Glückwunsch!

Sehr geehrter Herr [redacted]

Vielen Dank für Ihre Meldung an die Melde- und Analysestelle Informationssicherung MELANI.

Bei der von Ihnen gemeldeten E-Mail handelt es sich um ein E-Mail von Betrügerbanden. Die in den E-Mails gemachten Angebote und Versprechungen sind frei erfunden und sollen lediglich eine glaubhafte Kulisse bilden, vor welcher dann der Betrug abgewickelt werden kann. Wird beispielsweise auf diese Nachricht geantwortet, wird unter irgendwelchen Vorwänden (Gebühren, Anwaltskosten, Erbschaftssteuer, ...) eine Vorauszahlung verlangt. Deshalb spricht man auch von "Vorschussbetrug". Das versprochene Geld wird aber nie überwiesen. Gleichzeitig können auch bekannt gegebene persönliche Daten (Passnummer, Fotos etc.) als falsche Identität für weitere Betrügereien missbraucht werden. Die Betrüger denken sich immer neue Szenarien aus und Vorschussbetrug ist ein weltweites Phänomen, welches von Kriminellen auf allen Kontinenten (auch Europa) angewandt wird.

Wir empfehlen, solche E-Mails jeweils unbesehen zu löschen und keinesfalls darauf zu antworten, auch nicht im Sinne einer Absage.

Freundliche Grüsse
Ihr MELANI-Team

Figure 1: On the left: counterfeit e-mail from the fraudsters; on the right: original mail from MELANI

3.5 Bank statements sent to wrong addresses

Because of a program error, Bank Coop experienced some incorrect deliveries with its year-end dispatches, causing certain account statements to be sent to incorrect addressees. Bank Coop has since discovered the cause of the incorrect deliveries; it is linked to the introduction of a new point overview for the Supercard customer loyalty programme, in which the bank participates. The recipients of the erroneously dispatched documents were requested to return them to the bank. Bank Coop has promised to take all necessary measures to prevent a similar error from occurring in the future.

In Basel Stadt, where the bank is headquartered, the office of the public prosecutor announced that it was launching police investigation proceedings due to the suspected negligent breach of bank client confidentiality.

This incident is not an singular one. In February 2014 a similar case got public. The auditing company PricewaterhouseCoopers (PWC) has sent some wage statements to the wrong employees.[6] In ICT, there is a clear trend towards the use of increasingly complex programs with more and more functions. It is obvious that the risk of error also increases with this growing number of programming lines. There is a particular problem in the case of applications that can be modified or updated only when they are running. Although numerous tests are always carried out on test systems in advance, it is not possible to test all of the dependencies that abound in such programs.

3.6 Switzerland also affected by the theft of Schengen Information System data

In December, various Swiss media reported the theft of data concerning the Schengen Information System (SIS) database. The SIS is an information system for reporting stolen objects, people who are wanted by the police for the purposes of extradition, as well as missing persons and those who are subject to a ban on entry. The police and customs authorities of the Schengen Area member countries have access to the database.

6 http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/PWCMitarbeiter-erhalten-Lohnausweise-der-Kollegen/story/26934239 (as at 20 February 2014).

The unauthorised access took place via a security breach at the company managing the database for the Danish police in 2012. Because of the transnational nature of the SIS, a breach has the potential to automatically concern the data entered by all of the countries that have access to the system. Switzerland was thus notified of the breach in May 2013. It transpired that 26'478 of the 1.2 million pieces of data stolen were entered by the Swiss authorities. The stolen file contains personal details as well as coded data referring in particular to the reasons for entry in the database. This coded data is not directly interpretable and it is thus impossible, in principle, to link specific acts to people on the list. The breach concerns only the SIS 1 system, which was replaced by SIS 2 in May 2013.

The details of the attack (method used, breach) and the perpetrators' motives are still unclear and will probably not be made public before the end of the investigations being conducted in Denmark. Nevertheless, the Danish authorities have stated that the breach used has been remedied. Different elements were also revealed by the German authorities within the scope of a reply to questions from a member of parliament. They put forward the hypothesis of an untargeted attack that was not specifically aimed at SIS but exploited a breach on a server that also contained other data. Two hackers, one Danish and the other Swedish, were supposedly involved in the attack.

This incident highlights a considerable issue with the specification and implementation of systems for the international exchange of sensitive data. Often, such systems are specified at the political level primarily on the basis of which type of data is to be exchanged. Technical requirements on implementation are either dealt with merely as a matter of secondary importance or are left up to the individual member states. This brings with it the risk that sub-optimal implementation in one member state will also affect the data of other countries. Accordingly, it must always be insisted upon in the future, also in the case of other exchange of information projects, that there is not only a definition of the data to be exchanged, but also a clear, predefined minimum standard that applies to everyone for securing, processing and technically transmitting data.

3.7 NZZ inaccessible – technical problems

On 19 August 2013, some users were no longer able to access the NZZ website. Initially, it was suspected that an attack was responsible for this incident. However, according to Swisscom, this partial outage was due to a mistake of the renewal of the domain registration between the domain name registrar Network Solutions and Swisscom.

Swisscom's domain ip-plus.net was registered with Network Solutions at this time. This company had deactivated the *domain* at 12.40 p.m. on 19 August 2013, with the result that ip-plus.net could no longer be resolved and therefore no longer worked. As *DNS services* of third-party companies such as NZZ were also running under this domain, these websites were inevitably down as well and were no longer accessible. Swisscom had solved the problem already by 3.25 p.m., and the NZZ IT Department immediately deleted all affected servers from the DNS records, replacing them with working servers. However, as resolution errors always remain stored for 24 hours in the name server and *Internet Explorer cache*, it took up to 24 hours for all services to be working smoothly again.[7]

After this incident Swisscom has immediately implemented measures to exclude a further incident of that kind.

[7] http://www.nzz.ch/aktuell/digital/nzz-dns-1.18135806 (as at 20 February 2014)

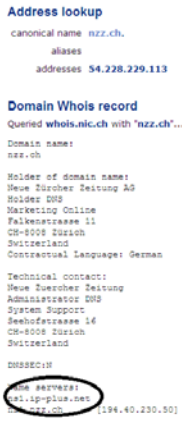


Figure 2: Whois record of NZZ with the DNS server ip-plus.net

The Domain Name System (DNS) makes it easier to use the Internet and its services by allowing web addresses (URLs) to be entered instead of IP addresses. The Internet would still work without DNS servers, but IP numbers would have to be entered instead of URLs. With these, the root servers are found uppermost in the hierarchy, and they serve as the highest authority for information concerning top-level domains (e.g. .com, .net, .ch). The lower authorities (second level domains) are operated by numerous large and small Internet service providers. A malfunction or manipulation can always have far-reaching consequences, particularly if an important DNS server of a large company is involved, like in this case.

3.8 Switzerland wins first Cyber Security Alpine Cup

In order to avoid the problem of a lack of cyber security specialists in the country and at the same time to make it easier for businesses to search for talented people, the Cyber Security Austria (CSA) association initiated the Cyber Security Challenge in 2012. In this competition, which is conducted in cooperation with the Austrian Interior Security Board (KSÖ) and the Counter-Intelligence agency, hundreds of pupils competed for victory in a selection procedure carried out on the Internet.

In 2013, the Swiss Cyber Storm Association adopted this idea under the patronage of the Confederation's Reporting and Analysis Centre for Information Assurance (MELANI) and the Swiss Police ICT.[8] As a result, it was decided to carry out a transnational competition under the leadership of Cyber Security Austria, with the field of participants being extended to include pupils and students. And so it was that the Cyber Security Alpine Cup was born.

As a result, the first Cyber Security Alpine Cup took place in Linz from 5 to 7 November 2013. After the first day of team-building activities and time for getting acquainted, the team competition itself took place on the second day. For more than eleven hours, the two teams from Austria and Switzerland tried to decipher codes, find security vulnerabilities and find possible ways to access mobile phones and tablets. This was not just about the attack; it also concerned measures to prevent unauthorised access. The Swiss team finally won the competition and accepted the winner's trophy at the awards ceremony in the Museum of Military History in Vienna, in the presence of numerous guests from political circles, the armed forces and the business world.

[8] MELANI Semi-annual report 2013/1, Chapter 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

The concept of a cyber security competition as a platform to search for talent and promote junior staff and its successful implementation in the first Cyber Security Alpine Cup did not go by unnoticed: next year Germany will also take part in the competition. Swiss qualification for the international contest will once again take place during the Swiss Cyber Storm IT security conference, which will take place for the fifth time on 22 October 2014 at the Culture and Congress Centre in Luzern. Pupils and students who are interested can pre-register at www.verbotengut.ch.

3.9 Malware also on Linux systems

Windows (Microsoft) and OSX (Apple) systems are not the only ones affected by malware; Unix/Linux systems are as well. A number of compromised Unix/Linux systems in Switzerland were reported to MELANI in the second half of 2013. They had been infected by a sophisticated *root kit* by the name of Ebury. Here criminals were able to gain access by hitherto unknown means to the system of the victim and install the Ebury *root kit*. Normally the *SSH daemon* installed on the victim's system is modified in such a way that the access data of all users who log on via SSH after the system was infected are leaked to the criminals. In addition, the Ebury root kit steals private SSH keys present on the system. The attackers can gain access to the infected system at any time with the stolen access data and can use the system for illegal purposes, such as hosting *command and control (C&C) servers* or sending *spam* e-mail, for example.

Given that Ebury is a form of malware with root kit functionality, it is difficult to detect on infected systems. In addition, Ebury uses a DNS-based protocol as a communication channel between the system infected with Ebury and the criminals. In many cases, this makes it even more difficult to detect the infection.

Further information on Ebury and how this malware can be detected is available on the website of Germany's Computer Emergency Response Team for federal agencies (CERT-Bund).[9]

Open source is often put forward with good reason as a possible alternative for the use of so-called proprietary software solutions. However, the logic that *open source* is comprehensible and thus more secure also falls short of the mark. Open source solutions do allow everybody to check the program code for errors. However, in the event that an error of this nature is not found and therefore is not remedied by the community, an attack vector would still be present even with open source solutions. In this respect, it should be borne in mind with the professional application of open source solutions that an in-house team examines the software used on the basis of the priorities of the company so as not to be dependent on the interests of the open source community. This fact must be taken into account accordingly in economic considerations about the use of open source or *proprietary systems*.

3.10 NTP amplification attacks – Swiss infrastructure already abused

Also in the last few months, so-called *Distributed Denial Of Service* (DDoS) attacks have been a method used frequently by cyber criminals in order to restrict the availability of certain services or websites, or even to stop them operating. Various types of attack can be

[9] https://www.cert-bund.de/ebury-faq (as at 20 February 2014)

distinguished: after the sharp increase in DNS amplification attacks[10] in the last six months, which amplify attacks by a factor of between 20 to 50 (cf. the MELANI Semi-annual report 2013/1[11]), in the second half of 2013 the *NTP protocol* which is used for time synchronisation on the Internet, was also misused in a similar way for DDoS attacks. Here the attackers request data from NTP servers using a forged sender address. The reply, which is considerably larger, is then sent to the presumed sender address, i.e. to the actual target of the attack. Because the replies are legitimate data coming from authorised servers, it is particularly difficult to block these attacks. NTP attacks are far more effective than DNS amplification attacks and can trigger amplification by a factor of 500.[12] Several NTP servers in Switzerland which had been misused for attacks had already come to the attention of MELANI.

NTP attacks are based on exploiting the command "monlist", a feature which is activated by default in older NTP-enabled devices.[13] This command releases a list with the 600 *IP addresses* which most recently connected to the NTP server. If the source address is forged, the entire list is then sent to the victim.

In order to prevent an NTP device from being misused for attacks of this nature, the "monlist" function can be deactivated or updated to the most recent NTP version, which has this function deactivated by default.

In view of the increase in DDoS attacks, it is recommended that every company which depends on its business activities being accessible via a website and/or Internet connectivity should clarify the risks posed by attacks of this nature and plan defensive measures. Along with the company's own technical measures to detect and eliminate problems, these typically include the assessment of the capabilities of the upstream provider and its contractual obligations in the event of an incident.

4 Current international ICT infrastructure situation

4.1 Further revelations about the NSA and GCHQ

The activities of the US National Security Agency (NSA), the UK Government Communications Headquarters and other foreign intelligence agencies which were disclosed by journalists based on Edward Snowden's documents continued to generate huge interest in the second half of 2013. Following the first revelations about Prism, XKeyscore and Tempora, which MELANI had discussed already in the last semi-annual report[14], the full picture of the extensive, all-encompassing data collection by the US and UK intelligence agencies began to emerge in the second half of the year. For example, it was revealed that

[10] In the case of DNS amplification attacks, bogus DNS queries were sent to open DNS servers on the Internet. Since the source IP addresses are bogus, the responses are sent to the IP address of the victim and not to the actual sender of the data packet.

[11] MELANI Semi-annual report 2013/1, Chapter 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

[12] http://www.zdnet.de/88184056/rekord-ddos-angriff-europa-erreicht-400-gbits/?ModPagespeed=noscript (as at 20 February 2014)

[13] https://www.us-cert.gov/ncas/alerts/TA14-013A (as at 20 February 2014)

[14] MELANI Semi-annual report 2013/1, Chapter 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

the NSA, like the UK operation Tempora, runs a programme called Upstream[15] in order to access data on fibre-optic cables. This cooperation with US telecommunications companies should have cost the NSA around USD 278 million in 2013.[16] Moreover, a project with the code name Muscular became public. The aim of this project operated jointly by the NSA and GCHQ is to access data flows among the data centres of Google and Yahoo.[17] The published document quantified the data sets at 181 million in 30 days. Another insight into the magnitude of the data collection was given by a 2012 presentation showing that the NSA had infected 50,000 computer networks worldwide with malware in order to obtain sensitive data.[18] A document published in January 2014 spoke of 100,000 computers hacked by the NSA.[19]

However, it was not only the scale that created controversy, as the targets of the NSA also gave much food for thought. For example, the primary objective of the intelligence gathering was always seen as counter-terrorism. However, the fact that various interceptions also focused on heads of government and diplomats quickly made it clear that there was also a political element. In Latin America, the interception of data from Brazilian leader Dilma Rousseff and Mexico's current and former presidents Peña Nieto and Felipe Calderón caused indignation.[20] At the international level, the alleged electronic spying on the G8/G20 summit in Toronto was in the spotlight[21], while the tapping of German Chancellor Angela Merkel's mobile phone made the most headlines in Europe.[22]

Operation Socialist[23] was also made public. This consisted of an attack on the Belgacom subsidiary Bics, a joint venture with Swisscom and South Africa's MTN. Major customers of this telecommunications firm include the European Commission, the European Council and the European Parliament.

Operation Socialist / attack on Bics

Belgacom ordered an internal investigation following the NSA revelations and determined it had been the subject of an attack, which was initially attributed to the NSA. After a further revelation, suspicions were directed at the GCHQ, which supposedly used technology for the operation that the NSA had developed. The goal of the project conducted under the code name "Operation Socialist" was apparently "to enable better exploitation of Belgacom" and "to improve understanding of the provider's infrastructure". According to the presentation, the computers of Belgacom employees were deliberately infected and it was then attempted to access central *roaming* routers from those computers.

---

15 http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (as at 20 February 2014)

16 http://www.heise.de/newsticker/meldung/Ueberwachungsaffaere-NSA-zahlt-Hunderte-Millionen-Dollar-an-Provider-1945984.html (as at 20 February 2014)

17 http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (as at 20 February 2014)

18 http://www.spiegel.de/netzwelt/netzpolitik/nsa-soll-50-000-netzwerke-weltweit-infiltriert-haben-a-935335.html (as at 20 February 2014)

19 http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0 (as at 20 February 2014)

20 http://www.bbc.co.uk/news/world-latin-america-23938909 (as at 20 February 2014)

21 http://www.spiegel.de/netzwelt/netzpolitik/kanada-erlaubte-nsa-spionage-bei-g-8-gipfel-a-936255.html (as at 20 February 2014)

22 http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html (as at 20 February 2014)

23 http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html (as at 20 February 2014)

This case affects Switzerland both directly and indirectly, as Swisscom has a 24% stake in Bics, and 51% of Swisscom itself is held by the Swiss government and thus Swiss taxpayers.

Corrupted encryption standard?

From an information security viewpoint, one of the most important issues is the extent to which encryption programs and encryption standards are still trustworthy today. The main thing making the headlines here was the Dual_EC_DRBG standard, a random number generator developed by the NSA that does not generate numbers quite as randomly as it should. In December 2013, it was discovered that the NSA had supposedly paid RSA Security USD 10 million to use the controversial random number generator as the default in the widely-used BSafe software.[24] RSA denied these reports, while the NSA did not react to the publication.

The limits of encryption – Bullrun and Edgehill

The details published show how systematically both the GCHQ and NSA intelligence agencies tackle encryption.[25] [26] In recent years, the two intelligence agencies have apparently established a hoard of measures and techniques to break or circumvent encryption. One aspect is the aforementioned weakening of random generators. With such manipulated generators, the encryption appears strong but it can be hacked with relatively little computing power. Even "leaking" keys is a way for encrypted data to be decrypted in real time or at a later date.

Finally, in December 2013, it emerged that the NSA can easily hack the *stream* cipher A5/1, which is the technology used most widely across the world for encryption between mobile phones and transmitter masts.[27] Phone calls and text messages can be decrypted in this way.

There still remains the possibility of breaking into the systems and tapping the data even before it is encrypted. The so-called Tailored Access Operations (TAO) division is responsible for this at the NSA.[28]

Other topics in connection with the Snowden affair that were in the spotlight include the following:

Royal Concierge

In November 2013, Germany's weekly magazine Spiegel published an article on the monitoring program Royal Concierge used by Britain's GCHQ. It can monitor reservations in at least 350 upscale hotels around the world in order to detect the stays of diplomats and senior government officials.[29]

---

[24] http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 (as at 20 February 2014)

[25] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (as at 20 February 2014)

[26] https://www.schneier.com/blog/archives/2013/10/defending_again_1.html (as at 20 February 2014)

[27] http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html (as at 20 February 2014)

[28] http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html (as at 20 February 2014)

[29] http://www.spiegel.de/netzwelt/netzpolitik/royal-concierge-britischer-geheimdienst-ueberwacht-diplomatenhotels-a-933997.html (as at 20 February 2014)

TOR – not crackable directly

According to a presentation likewise published by Snowden, the NSA has also turned its attention to the Internet anonymity tool TOR. While the NSA cannot crack the TOR network directly in order to unmask individual users, it nevertheless appears possible to attack TOR users by exploiting weaknesses in Firefox browsers. However, as the presentation shows, this is possible only in the case of a small fraction of TOR users by means of manual analysis.[30]

Follow the Money – SWIFT

In Switzerland, it was primarily the reports about the NSA spying on the financial service provider SWIFT that caused a stir. One of SWIFT's three data centres is in Diessenhofen in the Canton of Thurgau. Up to 15 million financial transactions are processed here every day. In connection with this revelation, it was also claimed that the NSA has a division called "Follow the Money" and that this is responsible for spying on financial data. SWIFT declared that there was no reason to believe that there had ever been unauthorised access to its network.[31]

NSA's Signals Intelligence (SIGINT) Strategy of February 2012, which was reported on by the New York Times in November 2013, gets right to the heart of the NSA's strategy: "Ensure Signals Intelligence provides THE decisive edge in advancing the full spectrum of US national security interests." In order to fulfil this vision, it is ready to "Defeat adversary cyber security practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere".[32]

The now published documents and details indicate that the statements in this strategy are not merely paying lip service; the NSA and its partners are actually implementing the strategy as well. At the moment, it is still difficult to gauge what repercussions these revelations will have on the development of the Internet.[33] It is already being prophesied extensively that this is the end of the Internet as we know it. Private and business users of the Internet will increasingly have to deal with the impact of the information revealed by Snowden and also with the subsequent risk assessment.

4.2 APT - reinventing methods

"NetTraveler" is an *APT (advanced persistent threat)* that was uncovered by Kaspersky in June 2013. Its targets were companies active in industry, energy production, telecommunications and new technologies, and also government entities. The following September, Kaspersky produced proof of the renewed activity of this APT, which now incorporated new attack vectors. While NetTraveler largely used *spear phishing* in the past to disseminate malicious code, this is the first time that it has been seen to be using a *watering*

30 http://www.zdnet.de/88171545/nsa-arbeitet-sich-an-anonymisierungsdienst-tor-ab/?ModPagespeed=noscript (as at 20 February 2014)

31 http://www.nzz.ch/aktuell/schweiz/swift-bestreitet-nsa-spionage-1.18151215 (as at 20 February 2014)

32 http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?pagewanted=all (as at 20 February 2014)

33 For this discussion see chapter 5.1 of this report.

hole method.[34] Another new development reported by FireEye researchers is the exploitation of a security vulnerability in *Java*.

Operation "Molerats" was uncovered by the FireEye firm in October 2012. It had its sights set on government targets both in Israel and in Palestine and was allegedly launched from the Middle East. This group appeared to rely heavily on XtremeRAT, a widespread malware tool that is often associated with attackers based in that region. New revelations by FireEye in August 2013 showed that the same group was using Poison Ivy at that time in its attacks on the USA and the Middle East. Poison Ivy is another malware tool that is widely used and has often been associated with Chinese attackers. Its use by attackers based in a different geographic area is an entirely new development.

These two examples are proof of the huge adaptability and opportunism that can be shown by groups launching APT attacks. The methods and tools used by these groups are not set in stone and can develop and be redefined depending on the circumstances or the target. This ability to reinvent themselves must be included in every single analysis.

This has an impact on how an attack is to be attributed in particular. A wide range of elements needs to be taken into consideration before venturing to make a judgement. An overly mechanical approach, based solely on the modus operandi and tools used, generally entails substantial risk. When attributing an attack, non-technical information should also be used to support the argument and the actual intentions, motives, victims and consequences should always be considered.

4.3 Details of millions of Adobe customers stolen

One of the largest password thefts came to light at the start of October. The victim was Adobe. After it was initially reported that the details, passwords and credit card details of 2.9 million customers had been stolen, Adobe put this figure at 38 million some weeks later.[35]A 3.8 GB file which also materialised apparently contains 150 million usernames and hashed passwords. While Adobe has not yet confirmed this officially, it has stated that encrypted credit card details and passwords were stolen. To decrypt the data, what is needed is a security key (3DES) that the attackers were more than likely unable to steal. The password reminders, however, had not been encrypted and some of these made it very easy to obtain the passwords. For instance, a password hint like "1-6" would mean the password is "123456". Because the same 3DES key was always used, all of the identical passwords looked the same even after encryption and it was then possible to group identical passwords together. These hints were enough to draw up a list of the 100 most frequently used passwords and disclose them publicly.[36] It became apparent in this case that many of the users had chosen very easy passwords. While this may be due to a lack of awareness, it is also possible that clients consider certain accounts to be "of no value" as they had only intended to use the account for making purchases, for instance, or they think that no information worth protecting is contained in the account.

After the attack had come to light, Adobe reset all passwords. The 38 million customers that Adobe claims were directly affected received an e-mail informing them of the theft and urging them to reset their password.

---

[34] MELANI semi-annual report 2013/1, Chapter 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

[35] http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ (as at 20 February 2014)

[36] http://stricture-group.com/files/adobe-top100.txt (as at 20 February 2014)

In addition to users' details, it would appear that the attackers were also able to steal the source codes for Adobe's ColdFusion, Acrobat and Photoshop products. The attack allegedly occurred in August 2013.

Apart from all the inconvenience that a case like this causes a company, communication with customers is a key element for minimising the damages as much as possible. Adobe reset all of the passwords, informed the affected customers about the attack by e-mail and asked them to reset their password.

However, a lot of consideration must be given to sending e-mails like these because they serve as the perfect template for further (phishing) attacks. Furthermore, Internet user awareness is so high nowadays that these kinds of e-mails urging users to change their passwords are quickly labelled as fraudulent. MELANI received numerous messages from citizens who were sceptical that this information e-mail from Adobe had actually been sent by Adobe. Careless client communication by a company may also have a negative impact on client behaviour regarding fraudulent e-mails.[37]

A problem that should not be underestimated in cases like these is that users use the same password for several services. The theft of a password with the associated e-mail address makes it possible for other Internet services to be accessed too.

4.4 Attacks on Target retail chain outlets

In December, several articles backed up by a press release from Target publicly disclosed this very large-scale attack on the retail chain. According to the news reports, the details of 40 million credit and debit cards as well as the personal details of 70 million customers were stolen.

The attack took place during the extremely busy sales period just before the festive season, between 27 November and 15 December. Initially, the statements and information released by Target about the incident were extremely brief and it has only been possible to gradually gain insight into the circumstances of the attack and the methods used through the investigations and disclosures made by various sources. At the time of writing this text, however, some aspects remained vague.

The first analyses, which were confirmed by Target, explained that the breach was carried out through a malware that had infected the point-of-sale terminals.[38] The malware BlackPOS or one of its variants is suspected of having been used in this incident and was most likely implemented by criminal gangs from Eastern Europe. This malware manages to copy the data stored on the card's magnetic strip in the instant after it has been swiped at the point-of-sale terminal and is still in the system's random-access memory (RAM). Warnings about this method, known as RAM scraping, had already been issued, particularly in press releases from VISA during the summer.[39] The key questions of how the data was taken and how the system was compromised to begin with (e.g. what was the entry point) were only partly answered several weeks later and after various disclosures and announcements had

[37] MELANI Semi-annual report 2012/1, Chapter 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 20 February 2014)

[38] The topic of vulnerabilities in POS terminals was covered in the MELANI Semi-annual report 2012/II. MELANI Semi-annual report 2012/II, Chapter 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=en (as at 20 February 2014)

[39] http://usa.visa.com/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf (Stand: 20. Februar 2014).

been made. Target initially said that the breach was attributable to the theft of network access data at one of its suppliers. Subsequent discoveries then pointed to one supplier in particular: a company that was managing the heating and air conditioning system. The access data had apparently been obtained after e-mails had been sent that contained malware specialised in password theft. This supplier's authorisation then gave the criminals access to the payment system, where they installed malware that intercepted the data.

This attack was followed by a report in January of a similar attack launched on the Neiman Marcus retail chain. Again, the data stored on the magnetic strip of the credit cards had been recorded immediately after they had been used for payment. While the same methods appear to have been employed in these two cases, it is not possible to say with any certainty for the time being that the same criminals are responsible for both cases. Finally, various sources claim that several other retail chains have fallen victim to the same attack, but these chains have not yet been identified.

The hacking of Target and other such cases underscore the risks entailed in using credit cards that are operable by their magnetic strip alone. This system, still widely used in the USA, has a much lower level of security than chip and PIN card systems. It is relatively easy to intercept the credit card details. Most of the time, card details recorded in this way are resold on specialist sites and forums, the ultimate aim being to create cloned copies of cards.

This incident also highlights the issue of service providers performing their services via the company network and enjoying extensive rights. As has been shown by this case, these service providers are also potential entry points for an attack.

4.5 Second SIM cards and the consequences

Attacks on smartphones which aim to attack e-banking systems with *mTANs* were already discussed in the last semi-annual report[40]. It was demonstrated at the end of October 2013 that attacks which take advantage of organisational weaknesses and not just technical ones are also possible. At the time, there were initial reports of scammers in Germany successfully compromising e-banking applications secured with mTANs by means of a second SIM (Subscriber Identity Module) card. To do this, the scammers simply had a second SIM card delivered to a second address and were able to snoop on the incoming mTANs with the help of this card.

A SIM card guarantees the user's authorisation. If a person has this card in their possession, it is possible, in principle, to connect to the mobile network in the name of the user. Depending on the policy of the mobile network operator, parallel operation of several SIM cards is possible. However, if only one card is accepted by the telecommunications provider, usually the two SIM cards disrupt each other.

Aside from this technical restriction, there is, however, the organisational issue of what security measures are used by telecommunications providers when issuing SIM cards. As critical services are being transacted via mobile phones more and more frequently, the security of these mobile phones and also that of the mobile operators is increasingly attracting attention.

[40] MELANI Semi-annual report 2013/1, Chapter 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

4.6 Hacked DES algorithms and the consequences for SIM cards

In July 2013, the German crypto specialist Karsten Nohl published initial results of his research on the security of SIM cards. According to these results, several million SIM cards around the world are inadequately protected and could be compromised. This allows, for example, an attack on the user's identity, electronic eavesdropping or even manipulation of payments which are carried out via the mobile phone infrastructure.[41]

The networks of mobile providers regularly communicate with SIM cards without their owners even noticing this. A technology is used which allows access to be gained to a SIM card's data from a distance (*over-the-air* technology). In this way, updates are installed for example, and a wide range of information is exchanged. The security of communication between the SIM card and the network operator is ensured by means of encryption. It is precisely this encryption that Karsten Nohl is calling into question. Specifically, with the issue of the Data Encryption Standard (DES), which was developed back in the 1970s but is still used in certain applications. DES algorithms have been regarded as insecure for a long time, particularly due to the insufficient length of the key used, i.e. 56 bits. According to Nohl, it is possible to find out the cryptographic key of certain SIM cards with DES encryption.

Once the hacker has this key, it is also possible to launch various attacks on the SIM card and its owner. Based on this security vulnerability, Nohl successfully hacked a quarter of the SIM cards tested. It is assumed that about 500 million SIM cards worldwide remain exposed to this risk. Newer SIM cards, which use the successors to DES, are not vulnerable in this way.

The published security vulnerability has significant potential for damage for users with SIM cards protected with DES. However, there is no danger for the Swiss market. According to the information MELANI received from Swiss telecommunications firms, the DES standard is no longer used in Switzerland.

4.7 Industrial and domestic Control Systems

Networked industrial facilities and remote-controlled domestic installations

MELANI has already repeatedly drawn attention to the risks involved in the increasingly networked nature of control devices of physical processes in the industrial and domestic sectors.[42] As a result of technical developments, there is an ever-increasing choice of ways to access systems remotely, to retrieve data and finally also to control the underlying devices. Meanwhile, it is relatively easy and cheap to purchase systems with remote query and control functions or to upgrade an existing system by installing a communications interface. This is often in line with the wishes of the customer: it is practical and convenient to be able to switch on the heating and the boiler via tablet or smartphone on the way to one's holiday home or to check if the cooker was switched off at home. This also applies to people in charge of property, whereby home automation systems can be controlled and monitored remotely. Even operators of small hydroelectric plants or other facilities which do not have to

[41] https://srlabs.de/rooting-sim-cards/ (as at 20 February 2014)
http://www.heise.de/security/artikel/DES-Hack-exponiert-Millionen-SIM-Karten-1920898.html (as at 20 February 2014)

[42] For example: MELANI Semi-annual report 2013/1, Chapter 4.5:
http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

be manned round the clock appreciate being able to monitor operation and carry out certain settings from the living-room sofa.

In principle, unauthorised access can also be gained to any system which legitimately allows *remote access*, whether this is directly or by infiltrating a device which has right of access. The simple rule that "everything which is accessible via the Internet can be hacked" still applies.[43] The interconnectedness of industrial control systems and ICT control of home automation are increasingly arousing the interest of security experts. This is how, in recent years, various security vulnerabilities were identified in such products or in their use.[44]

The various remote-controlled systems fulfil various tasks and any manipulation has diverse consequences for those concerned. If a boiler is switched off, the occupants of a house can only shower in cold water; switching on the floodlights in a stadium costs money and uses energy; if an industrial production line is stopped, perhaps the whole company will come to a standstill, which can have far-reaching consequences for the company and its employees.

Finally a scenario where many consumer devices are switched off or on in a coordinated way, thereby threatening the stability of the electricity grid, is also conceivable. Accordingly, apart from the function and user-friendliness of a remote access solution, special attention must also be paid to protecting against unauthorised manipulation.

ICT should primarily support operational processes. However, the use of ICT always has a physical and procedural impact as well, and this must be taken into account.

MELANI published a checklist for the protection of industrial control systems in October 2013.[45]

OSCE good practices to reduce cyber risks in the energy sector

The Organisation for Security and Co-operation in Europe (OSCE) has published a guide for countries and private energy companies on how they can protect their infrastructure against possible cyber terrorist attacks.[46] Although the title of the document suggests a relatively narrow focus, it introduces the topic from a broad scope and recommends general measures which can be applied to other industry sectors and which have a preventive impact and improve resilience in general, not just against terrorist attacks. The OSCE advocates increased awareness by means of training, greater cooperation by all those involved and the exchange of information. These measures are advocated by many quarters and are now highlighted by the OSCE especially for the non-nuclear energy sector. Nuclear energy was probably excluded so as not to provoke any conflict of responsibilities with the respective regulators. However, the OSCE recommendations are noteworthy even for operators of nuclear facilities.

It is the joint responsibility of all of those involved to ensure the security of supply for Europe's highly fragmented but increasingly interconnected energy supply. Many other sectors are dependent on the supply of energy and particularly electricity. This indicates that the supply of electricity is particularly critical. Added to this is the move towards intelligent power networks, which further increases the risks involved. In addition to new, convenient

---

43 "If you can ping it, you own it!" Kyle Wilhoit, The SCADA That Didn't Cry Wolf, 2013

44 http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities (as at 20 February 2014)

45 http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=en (as at 20 February 2014)

46 Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace", http://www.osce.org/atu/103500 (as at 20 February 2014)

possibilities for providers, the additional measurement and regulating stations controlled by ICT provide new attack points for malicious players, who can interfere with the electricity supply via these. The security of "intelligent" components in the supply of energy must thus be duly taken into account.

4.8 The Syria conflict – war of information 2.0

The Syrian Electronic Army (SEA) is a group of hackers which supports the regime of Syria's President Bashar al-Asad. However, the connections between the SEA and the Syrian leadership are not clear. According to its own information, the SEA is not part of the government and is not supported by it as such. It is made up of patriotic hackers who are, in their view, fighting against misreporting on the Syrian civil war.
In the last half year, the SEA mainly attacked news websites (New York Times, BBC News, Al-Jazeera, etc.) and was even able to compromise the Twitter accounts of news agencies such as Reuters and the Associated Press (AP) with the objective of spreading its own propaganda and deliberate misreporting.[47]

More than two thousand years ago, the Greek poet Aeschylus noted that "in war, truth is the first victim". With the rise of the Internet and in particular social media, information warfare has been "democratised". State intervention is no longer needed to spread information (correct or incorrect); all that is needed is an Internet connection and a story which can be spread virally.

Social media accounts and other information channels which authenticate access and subsequent information dissemination only via user names and passwords are relatively simple to infiltrate using methods such as *spear phishing*. Important information channels and platforms should therefore be protected by *two-factor authentication* insofar as possible.

Aside from technical measures, it should also be considered and defined in advance how and via which channels a bogus message can be denied as efficiently as possible, or corrected, so that even greater confusion and other consequences can be avoided.

4.9 When DDoS diverts attention from other attacks

A trend which appeared last year was that of low-intensity distributed denial of service (*DDoS*) *attacks* used as a diversionary tactic for other attacks. Various experts and articles reported on this phenomenon, which is based in particular on cases affecting US banks. Whilst those in charge of security were dealing with the DDoS attack on the company's website or e-banking portal, a more serious attack was simultaneously being carried out. In actual fact, the attacks targeted the bank's transfer system and not the accounts of individuals. In addition, the large amount of log data complicates analysis of the incident.

While a DDoS attack must be treated as such, it should also prompt people to be more aware of the potential for other attacks. This is particularly true if the attack is one of relatively low intensity.

[47] See Chapter 4.4 of the last MELANI Semi-annual report 1/ 2013 http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

4.10 Hackers and smugglers in cahoots

Between 2011 and 2013, several ship containers "disappeared" from the port of Antwerp. Investigations by the prosecuting authorities revealed that the legal containers had been misused by criminals for drug smuggling. To do this, the perpetrators infiltrated the ICT systems of the container companies so as to discover the locations of the containers concerned and then to steal them before their rightful owners could collect them.

Original access to the information systems was achieved by using simple *social engineering* e-mails, whereby company employees were misled into opening *attachments* and thereby installing espionage programs. After these incidents were discovered, the ICT security measures in the container companies were strengthened. The perpetrators then gained physical access to the offices and installed manipulated hardware in order to continue to have access to the information required, i.e. the security codes which permit drivers to access the premises and collect specific containers.

The IT infrastructure which supports the planning and execution of business activities has become indispensable in many sectors. Without IT systems, demanding logistical tasks in particular are unlikely to be performed. Moreover, many logistics companies want to be able to know the current location of deliveries and transport vehicles at all times. This information, which allows for more efficient use of resources and service provision, simultaneously provides the opportunity for targeted criminal acts to be committed. It should also be considered that manipulation of this information can adversely affect the normal course of business. Nevertheless, ICT systems are primarily another means to support specific operating procedures. Understanding of the physical and procedural impact of such systems is thus crucial primarily at company management level.

The same as in every market, increasing specialisation and professionalism can be seen also on the Internet underground market. This trend has been observed now for several years. Hackers are no longer curious youngsters who just want to test what is technically possible; increasingly they are experienced technicians who provide their skills at a price. Even in this case, the hackers were apparently recruited by the smugglers on the Internet. There is scarcely a service which cannot be obtained on the Internet underground market.

4.11 EU Parliament adopts more stringent penalties for cybercriminals

In the future, cybercriminals will face higher penalties in the European Union. With the approval of Directive 2013/40/EU on 12 August 2013, the European Parliament adopted more severe penalties in the case of attacks on information systems. One of the objectives is to harmonise laws and penalties amongst the member states, as attacks and scams often take place transnationally and these actions are penalised differently in the EU states. Harmonisation of the penalty framework will create the necessary basis for cooperation in terms of prosecution.

The Directive makes provision for imprisonment of at least two years. For example, constructing *botnets* will be punishable by at least three years' imprisonment. Criminals who are responsible for attacks on critical infrastructure such as power plants, transport systems or government networks face the threat of at least five years' imprisonment. The same applies to an attack if it is carried out by a criminal association rather than an individual or if serious damage is caused.

The Directive also contains requirements for the police and judicial authorities. In this way, EU member states should be able to exchange information on cyber attacks in order to ensure operation of the networks. In order to additionally improve the exchange of information, the responsible bodies should react to urgent requests within eight hours.

This new course primarily underlies the objective of tentatively harmonising the law in the area of cyber crime in the EU states. Practice has shown that prosecution in cross-border cyber crime is regularly stretched to the limit, which is due to the member states' different approaches to prosecution. Whether or not the more severe punishments will be implemented in future will depend to a large extent on how this joint framework can be anchored in the national laws of the member states.

5 Trends/Outlook

5.1 The Internet at a crossroads or business as usual

With the continued release of documents about the practices of the NSA and other intelligence services, many people have voiced their opinion in recent months on the future of the internet. As can be expected, these views are extremely diverse: in one of his articles, the security expert Bruce Schneier laments the fundamental betrayal of the Internet and the basic values it stands for.[48] He also highlights the paradox of the actions of the USA – the leader of the free world – currently supporting the intentions of totalitarian states that have always sought nationalisation of the internet. This fear of a growing "balkanisation of the Internet" has led Google Vice President Vinton Cerf, for instance, to evoke the demise of the Internet as we know it today.[49] With a growing national partitioning and the accompanying diversification of the market, it will no longer be of interest to companies economically to participate in the internet. Criticism is also coming from its supporters, who welcomed the Internet as the ultimate discovery in terms of basic democracy and emancipation. They now regard the Internet as the perfect surveillance platform and blame their own naivety for ever having seen it as anything else.

At the same time, however, the Internet appears to have remained very active and it is likely than nothing will change in this state of affairs, at least in the short term. However, the activities of some intelligence services, revealed by the Snowden documents, would at least suggest that people have definitively lost their trust in the Internet on several levels.

They also highlight the enormous problems inherent in a transnational facility like the internet, which every single individual and state can participate in and do as they choose and as permitted by national legislation, without having to give any thought to the global repercussions. If, at a technical level, a country changes global security standards as it sees fit, or if the companies themselves are instructed by way of classified, coercive measures to surrender vast amounts of information so that, in the interest of national security, data can be accessed as easily and extensively as possible, the principle of good faith would appear to have been violated and with it, a large body of other national laws. However, it does make it substantially easier and more enjoyable for state employees to achieve their objectives. The fact that reliance on greed and laziness in the state's procurement of information and

[48] http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying (as at 20 February 2014)

[49] http://www.tagesanzeiger.ch/digital/internet/GoogleVize-warnt-vor-Untergang-des-Internets/story/12499111 (as at 20 February 2014)

personal data has always been considered a borderline approach from a liberal democratic viewpoint would appear to have been forgotten.

What this means for companies in the IT sector is that although they are operating in a global environment, ultimately they are subject to national legal foundations which differ from each other and do not always correspond. And this is not only true for companies in the IT sector. It is therefore imperative to address this lack of consensus on basic principles for the Internet and participating stakeholders.

The restoration of trust in the IT security community in particular is also linked to this issue, i.e. trust and international exchange between IT security bodies whose primary aim is to protect networks, products and applications. However, the matter becomes complicated when you consider, for example, the fact that the body managing security standards in the USA, the Information Assurance Directorate, has to report to the head of the NSA, whose remit presumably stipulates that the focus probably not solely lies on secure IT products and robust standards. Furthermore, the establishment of CERTs responsible for the international information exchange and protection of networks within offensive Signal Intelligence units will probably support the trust with other government CERTs only to a limited extent. Nevertheless, it is precisely this technical community and its international system for the exchange of information that has to assume the lion's share of whipping the internet, or rather the security of its components, back into shape so that further partitioning can be avoided and basic trust in the Internet can be restored.

Proclaiming the death of the Internet in its more or less twenty-fifth year of existence is perhaps going too far. However, rebuilding basic trust in the Internet and trust among the security stakeholders in the ICT domain is quite a significant task. Similarly, there will be no easy answers to the fundamental question of how to ensure that the application of national law to a transnational system such as the Internet also results in the law being applied in practice with an extraterritorial effect. This question will have to be discussed at all levels, from a security policy viewpoint, right up to the multi-stakeholder committees that deal with standards and requirements and in which the economy is also the main concern.

In any case, what is needed is to take stock of the situation and to return to the basic idea that the Internet stood for: first and foremost, a highly resistant, decentralised system, through which information is conveyed. The security and confidentiality of this information was only ever on the fringes and never at the centre of this vision. Security and confidentiality have always been and will continue to be the responsibility of those who upload this information and data on to the Internet in the first place.

5.2 Bitcoin - success, but at a price

How it works

Bitcoin is a decentralised digital currency, which means that it works independently of a central issuer. This is what sets it apart from traditional currencies and also from many other digital currencies.

There are two types of main stakeholders in bitcoin. Users are represented by their wallets, which consist of a pair of cryptographic keys – one public, one private. The public key can be considered by analogy to be the account number to which money can be transferred. The private key enables the user to sign a transaction, i.e. make a payment.

For the payment to be completed, it has to be validated. This is where the network of miners, the system's second group of main stakeholders, comes into play. In concrete terms, miners

take part in maintaining the "block chain", which is at the heart of the bitcoin system. This is a type of ledger that groups together all of the confirmed transactions and can be consulted by all users. The validation process, called mining, aims to confirm transactions that are pending by including them in a block. The validation of a block requires the miner to produce a proof of work. This process requires immense computing power and is remunerated in bitcoins, thus leading to a rise in the money supply in circulation. The integrity of the block chain is of crucial importance because in order for a new transaction to be authorised, it must be possible to match it to previous revenue recorded by the payer. Without this tracking method, a user could sign a completely unrealistic transaction.

There are three main ways to obtain bitcoins: participating in mining, accepting bitcoins as payment for a service or by purchasing them from an exchange which allows bitcoins to be exchanged for "classic" currency. Bitcoins can then be used in shops that accept this method of payment. The anonymity of bitcoin transactions is a recurrent discussion point and needs to be clarified. In reality, users are anonymous theoretically as they are only identified by the *cryptographic key* they hold. On the contrary, unlike the classic banking system, transactions are in actual fact public.

Security risks

Bitcoin's growing popularity raises many issues, particularly in terms of security, but also with respect to the legal status and regulation of these currencies.

Several recent events clearly show that bitcoins and their users have become interesting targets for criminals and that the methods used for fraudulently obtaining bitcoins vary. A range of attacks and security incidents of varying levels of complexity and with different targets have been identified in recent months.

The private key, and through it the wallet owner, is generally the most attractive target for attackers. In reality, the wallet's confidentiality is guaranteed entirely by this key, and storing it securely is of utmost importance. Many users have fallen victim to attacks targeting this element. Furthermore, web services also offer to store their customers' keys. Given this centralisation of wallets and the large sums they can represent, these sites have become the main targets for attack. For instance, one such service, input.io, had USD 1.2 million worth of bitcoins stolen in July 2013.

Exchanges are another potential target. In December, the exchange market Swiss bitcoin announced that it had fallen victim to an attack. The attack had been very successful despite the modus operandi that was extremely unrefined and related mainly to social engineering. This incident saw hackers contact the exchange's e-mail account provider in the guise of Swiss bitcoin. They requested that its e-mail account passwords has to be changed, which the account provider granted. The head of Swiss bitcoin has since changed its e-mail account provider, but has not specified if the hackers used the stolen data to commit criminal activities. Other types of attacks also have been observed, with a strong tendency in particular for distributed denial-of-service (DDoS) attacks. In certain cases, the attackers demanded the payment of a ransom, based on the known modus operandi. Other attacks appear to have other aims. For instance, certain manoeuvres have been observed that seemed to aim at destabilising the market, pushing the bitcoin exchange rate down with a view to subsequently buying it at a better price. The volatility of the bitcoin exchange rate and the implicit possible speculative manoeuvres have become a major concern here.

A final line of attack consists in targeting the returns generated by mining. At the start of 2014, malware spread by ads featured on various websites belonging to the Yahoo group was detected. A special feature of the malware was its ability to use the computing power of the infected computers to mine, without the owners' knowledge, and thus generate bitcoins.

In addition to these attacks, bitcoin has often been the subject of discussions regarding its use in illegal transactions. Bitcoin is widely used in particular for performing transactions on platforms offering illegal products, such as Silk Road, an e-commerce platform used for black-market activities.

All of these security risks underscore once more the huge opportunism of criminals operating on the internet. As a general rule, a successful service is quickly preyed upon by tailor-made attacks. As a user, it is advisable to be aware of this risk and of the value of bitcoins, and therefore of the need to protect them. This protection begins with secure storage. It is recommended that the private cryptographic key be stored on a digital medium, that is not connected to the internet or on paper (Paper Wallet). The general security of the computer, and particularly protecting it from infection, is also of crucial importance here.

The framework and regulation of the use of bitcoins are aspects that should be developed much further. This currency's popularity coupled with concerns about the scope for abuse or its extreme volatility have triggered the interest of the US, particularly in drawing up regulations. Similarly, Germany has also granted bitcoin the official status of "private money". In Switzerland, the last two months of the year saw bitcoin involved in three parliamentary proceedings, specifically in relation to its risks and a possible legal status.

5.3 The role of cyberspace in conflicts

The cyber component now plays a role in many conflicts, as shown by the example of the Syrian Electronic Army in the Syria conflict, for instance.[50] Primarily propaganda and disinformation are observed here, but direct attacks on infrastructure are also seen. Commonly cited examples include the DDoS attack on Estonia, DDoS attacks on US banks and attacks in North and South Korea. However, the terms cyber war and cyber terror are used extensively, which appears inappropriate given the damage actually caused. Terrorist attacks and war inevitably make people think of panic, fear, injuries and deaths, but cyber attacks to date have caused something very different, i.e. system failures, inconvenience and loss of money.

Use of cyber attacks particularly below the conflict threshold

History has shown that cyber attacks are launched when targeted operations below the conflict threshold are to be conducted. If these were carried out conventionally, they would lead to major discord between states. A typical example is the use of the malware Stuxnet in a bid to disrupt the centrifuges in Iran's uranium enrichment plants. Such an attack conducted with conventional means would probably have led to a serious conflict in the region.

Many players and motives

The great number of players and motives makes assessments even more difficult. A DDoS attack on a bank can have either a criminal background (extortion) or an ideological background, as shown by the various Anonymous attacks on banks in recent years, for example. But a state background is also perfectly feasible, for example if it were attempted to weaken an entire financial system with an attack.

[50] Current MELANI Semi-annual report 2013/2, Chapter 4.8
and MELANI Semi-annual report 2013/1, Chapter 4.4:
http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 20 February 2014)

The problem of attribution may become more difficult in the future, as the huge potential of people with cyber skills – including those in criminal circles – will be recognised by various states and used for their purposes. Therefore, actions can be commissioned and carried out without the state having to expose itself to the risk of attribution.

Future attacks

So is there little risk of cyber attacks with significant potential for damage? It is of course possible that there could be attacks on particularly critical systems whose failure would have major repercussions. However, such attacks usually require in-depth specialist and insider knowledge, as well as a considerable amount of effort. Moreover, the attention paid to security is particularly high in the case of critical systems. Therefore, it is not only the risks of cyber attacks that should provide food for thought, but also the fact that systems are becoming increasingly complex and interconnected. As a result, it is no longer easy to grasp links and dependencies. A problem or disruption can thus have unforeseeable effects. This does not even have to be an attack, as breakdowns can also have a major impact, and troubleshooting in a complex system frequently takes quite some time.

5.4 Virus detection in the 21st century, what will succeed signature-based anti-virus programs?

The history of virus detection

The first *virus* was observed in 1971. This was the Creeper which spread through the Advanced Research Projects Agency Network (*ARPANET*), the predecessor to today's Internet. Creeper in turn was combated using a code called "The Reaper". Even though the term "virus" was not used at that time, "The Reaper" can be seen as the first anti-virus program in history. In the meantime, there have been commercial anti-virus solutions for more than 20 years and a huge anti-virus industry has developed. But where is this industry now and what defensive capacities do current anti-virus products really have?

In a test report published by AV Comparatives.org in 2012, the percentage of successfully blocked malware and successfully blocked malicious websites is surprisingly high. The detection rate here is over 90%:

Whole Product Dynamic "Real-World" Protection Test – (March-June) 2012 www.av-comparatives.org

Summary Results (March-June)

Test period: March – June 2012 (2159 Test cases)

	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][4]	Cluster[5]
BitDefender	2150	-	9	99,6%	1
G DATA	2147	1	11	99,5%	1
Kaspersky	2146	2	11	99,4%	1
Qihoo	2143	6	10	99,4%	1
BullGuard	2131	21	7	99,2%	1
F-Secure	2135	10	14	99,1%	1
Avast	2110	28	21	98,4%	2
ESET	2117	1	41	98,1%	2
AVIRA	2107	13	39	97,9%	2
Sophos	2112	-	47	97,8%	2
Trend Micro	2108	-	51	97,6%	2
AVG	2103	6	50	97,5%	2
GFI	2102	-	57	97,4%	2
Panda	2097	-	62	97,1%	2
eScan	2094	-	65	97,0%	2
PC Tools	2024	126	9	96,7%	2
Tencent	2052	32	75	95,8%	3
Fortinet	2046	-	113	94,8%	3
McAfee	2041	6	112	94,7%	3
AhnLab	1999	-	160	92,6%	4
Webroot	1963	1	195	90,9%	4

Figure 3: Test report from AV-Comparatives.org

Judging by these statistics, anti-virus programs seem to detect and eliminate most viruses. However, the conditions for the test were specially selected. Under the pretext that a real situation should be simulated, it was assumed that 40% to 50% of the Internet addresses included for analysis led directly to malware, the remaining 50% to 60% in contrast led to a so-called *exploit pack*. Unlike malware, which reaches computers directly, exploit packs can be relatively easily monitored and detected by anti-virus products. This explains the high success rate.

By contrast, in a similar test with static conditions conducted by the CRDF Threat Center[51], a non-commercial, French web agency, and in which the malicious codes were analysed solely on the basis of their digital signature, a more differentiated picture emerges. While there were anti-virus programs which detected that over 70% of the codes under scrutiny were malicious, other products recognised the malware in only 1% to 3% of cases. According to this study, the average detection rate was 33%.

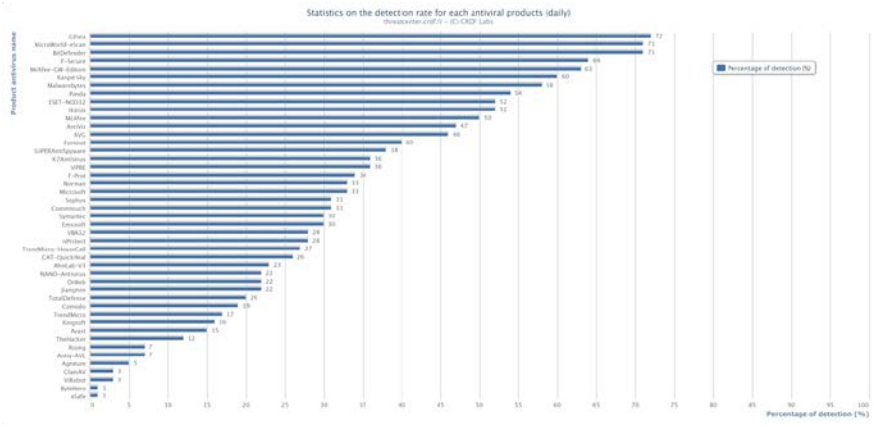


Figure 4: Test report from the CRDF Threat Center.

What is the true reality now in the criminal world and particularly in the area of white-collar crime?

In order to avoid detection by anti-virus programs, criminals often repackage malware several times a day. In the case of this packaging process, the underlying code remains identical but it is compiled in such a way that outwardly it looks new in order for it not to be detected by anti-virus software. To this end, criminals even use special platforms which examine how many and which anti-virus programs are able to detect the repackaged malware. In contrast to the offerings from security providers[52], the platforms used by criminals pay scrupulous attention to ensure that no information whatsoever on these new viruses reaches anti-virus manufacturers.

---

51 https://threatcenter.crdf.fr/?Stats (as at 20 February 2014)

52 For example, Virustotal: http://www.virustotal.com (as at 20 February 2014)

Figure 5: example of an anti-virus check tool used by criminals. If "ok" appears on an anti-virus check tool, this means that the malicious code is not recognised as a virus. If an anti-virus product classified the code as malicious, the criminal would repackage the malware.

Faced with so many virus variations and packaging programs, it is becoming increasingly difficult for anti-virus manufacturers to identify malware only with the aid of the signature. Even if the minimum requirements for basic security (updated system, *firewall*, anti-virus software) remain applicable, these measures are no longer sufficient to guarantee complete protection.

Efficiency only in the case of widespread malware

The efficiency of anti-virus products is restricted in particular to common, widespread malware. In the case of targeted attacks which only affect a fraction of clients, detection is problematic and practically impossible. Mikko Hypponen, Head of Research at F-Secure, said with reference to Duqu, Flame, Gauss and Co: "all of us had missed detecting this malware for two years or more. That's a failure for our company, and for the anti-virus industry in general".[53]

Even if targeted attacks are generally not directed at the common user, it was seen in the case of Stuxnet that even machines which have nothing to do with the actual target or the potential victim can be infected with operations of this nature. However, there are also trends in the area of white-collar crime to carry out smaller attacks by exploiting unknown vulnerabilities or with malware specially packaged for a specific target so as to remain under the radar of anti-virus products.

New measures are in demand

It therefore has to be asked what other measures are required to increase the level of security so that smaller and more targeted attacks can be recognised. Many companies, above all bigger ones, already use the most diverse additional systems to detect and block anomalies and suspicious Internet traffic. Intelligent detection systems which analyse company network traffic and deviations from the norm are sought after here. Firewalls and anti-virus software are joined by systems to detect attacks (*Intrusion Detection System*, IDS), white and *black lists* to filter network traffic, monitoring of network traffic or even monitoring of the behaviour of individual computers.

---

[53] http://www.f-secure.com/weblog/archives/00002376.html (as of 20 February 2014)

Another aspect is comprehensibility. Should (targeted) malware nevertheless have found its way into the company network, it is very important to be able to understand how it reached the company network and what other computers and servers are also involved. This is the only way to eliminate the malware completely from the network. As past attacks have shown, several months or even years can elapse between when the malware gains access to the network and when this malware is discovered.[54] A discussion must also take place on the length of time *log data* is stored.

Another finding from the last few years is that technical measures on their own are insufficient. In the end, it is always the employee who has the most efficient means to detect an attack and react to it correctly. Regular employee training and awareness-raising are of crucial importance in this regard. Also important is the creation of a body to which employees can report suspicious incidents and moreover be taken seriously.

Action needed in the case of small companies

Action is still needed regarding additional cyber defensive measures particularly in the case of small companies. These are frequently inadequately protected against such targeted attacks. Very often these are niche companies which have invested considerable capital in the area of research and development and can therefore become a target for possible specific espionage activities. It is precisely these firms that have to introduce security systems which are not exclusively based on anti-virus software. It is frequently forgotten that the costs for implementing security measures must be contrasted with the risk of considerable losses in the event of a successful attack.

Difficult implementation in home usage

The measures mentioned above cannot be transferred to private individuals. Extended and appropriate security solutions are too costly in such cases. In addition, there usually is a lack of time and/or technical know-how. How in that case should the normal computer user behave and what measures can he/she take?

In the future, it will be a case of private users having to request the provision of a "clean" Internet connection from their own provider even if there is a cost involved. In the process, the provider could implement the aforementioned additional security measures centrally for all of its clients and thereby provide them with additional protection. The security aspect is scarcely in demand from clients at present. Conversely, providers are also not promoting security. The main criterion when choosing an Internet connection, along with the cost, is usually speed. This will (have to) change in the future.

5.5 Attacks on home routers

Time and again, *home routers* have insecure configurations or vulnerabilities. Whereas modern devices can be automatically updated by providers, this is not always the case with older devices.

---

[54] Verizon: Data Breach Investigations Report 2012, figure 40
available at http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf
(as at 20 February 2014)

Insecure default configurations (standard or factory settings)

Services which are misused for DDoS attacks in the case of home routers are currently a very serious problem. Here the focus is on *DNS* and *NTP*, both of which are *UDP* based. If a service of this nature is incorrectly configured and accepts requests from the entire Internet, attackers can use these for DDoS attacks. They frequently exploit the fact that a huge reply can be generated (amplification) with a relatively small request. Some of these old devices were delivered with insecure default configurations and cannot be equipped remotely with current *firmware* and/or a secure configuration. Many users are totally unaware of the misconfiguration of their device and the associated risks posed by this. However, these devices' potential for damage is huge. Removal of these misconfigurations takes a lot of time and effort. MELANI is in contact with the big telecom providers, which have to carry out updates of the vulnerable devices.

Security vulnerabilities also in routers

Time and again, vulnerabilities are revealed in firmware versions used on *ADSL* terminals. There is practically no manufacturer which has not had to eliminate vulnerabilities. In June and July 2013, several serious security vulnerabilities were revealed in Asus devices[55] and also a vulnerability in the *UPnP* service of D-Link devices.[56] In October 2013, a vulnerability was published whereby it was sufficient to simply change the "user agent" in the browser to gain access to the Internet web server in the case of certain Netgear devices.[57] Also in the case of other Netgear[58] and Draytek[59] devices, there are vulnerabilities which allow an attacker to gain access to the router or to execute malicious code. Vulnerabilities of this nature are exploited by worms such as Linux.Darlioz[60] on the one hand but can also be used by criminals on the other for redirecting online banking sessions.

MELANI recommends restricting access to the maintenance interfaces of routers insofar as possible. Many devices support a restriction to an *IP address* from the internal network. If devices which are not maintained by a provider are used, the user must then carry out regular updates independently. In addition, only services which are actually required should be activated. Green provides full instruction on how to eliminate the OpenResolver problem also on home devices.[61]

[55] Bugtraq: http://seclists.org/bugtraq/2013/Jul/87 (as at 20 February 2014)

[56] Heise: http://www.heise.de/security/meldung/D-Link-Router-mit-schwerwiegender-UPnP-Luecke-1914510.html (as at 20 February 2014)

[57] Devttys0.com: http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/ (as at 20 February 2014)

[58] The Shadow File: http://shadow-file.blogspot.ch/2013/10/complete-persistent-compromise-of.html (as at 20 February 2014)

[59] CERT.org: http://www.kb.cert.org/vuls/id/101462 (as at 20 February 2014)

[60] Symantec: http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices (as at 20 February 2014)

[61] Green: http://www.green.ch/Portals/0/Support/pdf/Anleitung_OpenResolver_DE.pdf (as at 20 February 2014)

5.6 Items of parliamentary business related to information assurance issues

Selected items of parliamentary business from the second half of 2013 are shown below.

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Fra	13.5284	Contact with Edward Snowden to obtain further information on US espionage activity in Switzerland	Glättli Balthasar	09.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135284
Fra	13.5283	Insufficient Federal Council reaction to breaches of the privacy of Swiss citizens and Swiss companies	Glättli Balthasar	09.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135283
Fra	13.5338	Extensive introduction of electronic voting	Markwalder Christa	11.09.2013	NC	FCh	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135338
Fra	13.5334	Blurring of aerial photos of sensitive areas in documents accessible to the public	van Singer Christian	11.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135334
Fra	13.5328	Electronic voting	Sommaruga Carlo	11.09.2013	NC	FCh	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135328
Fra	13.5319	What measures could be taken to prevent violations of data protection by the NSA	Schwaab Jean Christophe	11.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135319
Ip	13.3677	Are the NSA and other intelligence agencies snooping in Switzerland too?	Social Democratic Group / Tschümperlin Andy	11.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133677
Ip	13.3692	Telecommunications market:. Are the current legislation and regulatory measures still up to date?	Hurter Thomas	12.09.2013	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133692
Fra	13.5321	NSA economic espionage also in Switzerland?	Leutenegger Oberholzer Susanne / SP Group	16.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135321
Po	13.3707	Holistic, forward-looking cyberspace strategy	BD Group / Guhl Bernhard	17.09.2013	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133707
Fra	13.5382	Export controls on surveillance software from Switzerland	Glättli Balthasar / Green Group	18.09.2013	NC	EAER	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135382
Fra	13.5380	Insufficiency of instruments for fighting cybercrime	Reinmann Maximilian	18.09.2013	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135380
Po	13.3736	Switzerland's Wi-Fi strategy	Buttet Yannick	18.09.2013	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133736
Ip	13.3726	Identity theft: a gap in criminal law that needs to be filled?	Schwaab Jean Christophe	18.09.2013	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133726
Fra	13.1060	Domain name abuse	Fehr Jacqueline	18.09.2013	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20131060
Pa.Iv.	13.445	Making malicious identity theft using digital means of communication punishable	Golay Roger	18.09.2013	NC		http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20130445
Ip	13.3773	Forward-looking Telecommunications Act; for a comprehensive cyberspace strategy	Wasserfallen Christian	24.09.2013	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133773
Mo	13.3808	No rush with the extension of electronic voting	Schwaab Jean Christophe	25.09.2013	NC	FCh	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133808
Ip	13.3799	IT security in the Federal Administration: what is the cost-benefit ratio?	Cassis Ignazio	25.09.2013	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133799
Mo	13.3812	No insecure e-voting; only permit systems with verifiability and open source code	Glättli Balthasar	26.09.2013	NC	FCh	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133812
Mo	13.3841	Expert commission for the future of data processing and data security	Rechsteiner Paul	26.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133841
Mo	13.3930	Banning the exportation of surveillance and espionage software to lawless states	Glättli Balthasar	27.09.2013	NC	EAER	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133930
Ip	13.3927	Protection for Switzerland as a data storage bunker	Reimann Lukas	27.09.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133927
Po	13.3989	Violation of personal rights due to progress in information and communication technologies	Recordon Luc	27.09.2013	CS	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133989
Mo	13.4009	Implementation of the National Strategy for the Protection of Switzerland against Cyber Risks	National Council Security Policy Committee	05.11.2013	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134009
Ip	13.4023	The Confederation's IT plans	CVP, EVP Group	27.11.2013	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134023
Po	13.4069	Espionage by the NSA and other foreign intelligence services	Schwaab Jean Christophe	04.12.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134069
Ip	13.4077	Data espionage and Internet security	Swiss People's Party Group	05.12.2013	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134077
Mo	13.4086	National research programme on data protection in the information society suitable for everyday use	Green Group / Glättli Balthasar	05.12.2013	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134086
Mo	13.4091	Banning the use of facilities for political, military or economic espionage on Switzerland or foreign countries	Green Group / van Singer Christian	05.12.2013	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134091
Mo	13.4165	NSA affair. "No spy" agreement with the United States	Allemann Evi	12.12.2013	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134165
Po	13.4308	Improving the security and independence of Swiss IT	Graf-Litscher Edith	13.12.2013	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134308

6 Glossary

3DES	The Data Encryption Standard (DES) is a widely-used symmetric encryption algorithm.
Abuse unit	A provider's unit where reports concerning suspicious incidents in the provider's network area can be submitted.
AdServer	Ad servers are employed for the placement and success measurement of Internet advertising. Both the physical server itself on which the ad server software runs as well as the software may be called ad servers.
ADSL	Asymmetric Digital Subscriber Line A technology enabling a high-speed and permanent Internet access via telephone lines.
Advanced Persistent Threat (APT)	This threat results in very great damage impacting a single organisation or a country. The attacker is willing to invest a large amount of time, money and knowledge in the attack and generally has substantial resources.
Anonymity service	A service such as TOR that enables users to hide their identity by using a third-party IP address.
Antivirus Live CD	CD from an anti-virus software manufacturer that checks the computer for malware even before the operating system loads.
App	"App" (an abbreviation of "application") generally refers to any type of application programme. In common parlance, the term now generally refers to applications for modern smartphones and tablet computers.
Application	A computer programme that performs a given task. Word processing and internet browsers are examples of applications.
ARPANET	ARPANET (Advanced Research Projects Agency Network) was originally commissioned by the US Air Force and developed from 1962 by a small research group headed by the Massachusetts Institute of Technology and the US Department of Defense. It is the predecessor of today's Internet.
Attachment	An attachment is a file sent along with an e-mail.
Backdoor	"Backdoor" refers to a software feature that allows users to circumvent the usual access control of a computer or of a protected function of a computer

	programme.
Backup	"Backup" means the copying of data with the intent of copying them back in the event of data loss.
Black- / White-List	Blacklist: A list of entities, e.g. websites, which are to be denied a particular privilege or service. For example, this may result in the website in question being blocked. Whitelist: A list of elements that the author considers to be trustworthy.
Botnet	A collection of computers infected with malicious bots. These can be fully remotely controlled by the attacker (the owner of the botnet). Depending on its size, a botnet may consist of several hundred to millions of compromised computers.
Command & control server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called command & control server.
Content Management Systemen (CMS)	A content management system (CMS) is a system that makes possible and organizes the joint preparation and processing of content, consisting of text and multimedia documents, generally for the World Wide Web. An author may operate such a system even without programming or HTML knowledge. The information to be displayed is referred to as "content".
Cross Site Scripting	Cross Site Scripting (XSS) is a type of computer security vulnerability typically found in Web applications.
Distributed denial of service attacks (DDoS)	A DoS attack where the victim is simultaneously attacked by many different systems.
Domain Name System	Domain Name System. With the help of DNS the internet and its services can be utilised in a user-friendly way, because users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
Domains	The domain name (e.g. www.example.com) can be resolved by the DNS (Domain Name System) into an IP address, which may then be used to establish network connections to that computer.
Drive letters	Microsoft operating systems use capital letters to refer to drives (or more precisely, partitions on a disk, so that they appear to users as individual drives).
Drive-By Downloads	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain 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.
Exploit pack	An exploit pack is a kit with which malware can easily be produced to exploit weaknesses.
Firmware	Instructions stored in a chip to control a device (e.g. a scanner, graphics card, etc.). Firmware, as a rule, may be modified by upgrades.
Hash function	Algorithm converting any text into a numeric sequence. Hash functions are used in three areas: - Cryptography. - Database systems. Database systems use hash functions to search efficiently within large databases. - Checksums. A hash value can be assigned to every file. An altered hash value indicates a manipulation.
Hosting	Hosting is the business of housing Internet projects that in general can also be accessed publicly via the Internet.
HTML	HyperText Markup Language Pages for the World Wide Web are written in HTML. This allows to determine the properties of the web page (e.g. page representation, links to other sites, etc.). Because HTML is made up of ASCII characters, a HTML page can be edited using a normal word processing programme.
IFrame	An IFrame (also inline frame) is an HTML element used to structure websites. It is used to integrate external web contents into one's own website.
Internet Explorer cache	In the world of computers, a cache is a quick buffer memory that helps to prevent the slow loading of a background medium or lengthy new requests when pages are (re)accessed.
IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
Java	An object-based scripting language for developing applications.
Key/encryption key	In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher.

Lifecycle management	Lifecycle management is a business administration concept that describes the process from the time a marketable product is released on the market or completed to the time it is withdrawn from the market.
Log file	A log file contains the automatically maintained log of all or specific actions of processes on a computer system
Malicious Code	Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses. See also Malware.
mTAN	The mobile TAN (mTAN) variant or smsTAN includes text messages as a transmission channel. The transaction number (TAN) is sent in the form of a text message.
Network drives	If a permanent connection is set up on a file share on the network, a network drive is created which, as a virtual drive, displays the folders and files of a server to the client as usual.
NTP protocol	Network Time Protocol (NTP) is a standard for clock synchronization between computer systems over packet-switched communication networks.
Open source	Open source is a range of licences for software whose source code is publically available. Further developments are encouraged by the licence.
Over-the-air technology	Over-the-air (OTA) refers to the transfer of data through the air via electromagnetic waves.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with false sender addresses.
PHP Code	PHP is a scripting language mainly used to create dynamic websites or web applications.
PIN	A personal identification number (PIN) is a number for authenticating oneself to a machine.
Point of sale (POS)	A POS terminal (in Switzerland: EFT/POS terminal) is an online terminal for cashless payments at points of sale.
Proprietary	This adjective means held as the property of an owner. When referring to hardware and software, it

	is used to differentiate proprietary items from open source or free software and hardware.
Random-access memory (RAM)	Random-access memory (RAM) is a type of computer data storage that is usually in the form of memory modules.
Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts or deletes data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
Remote Administration Tool (Remote Access)	A remote administration tool is used for the remote administration of any number of computers or computing systems.
Roaming	The term "roaming" originated in the area of GSM telephony. Conventional GSM roaming refers to the ability of a mobile phone customer to automatically make and receive calls, send and receive data, or access other services using a visited network rather than his home network.
Rootkit	A collection of programs and technologies which allow unnoticed access to and control of a computer to occur.
Router	Computer network, telecommunication, or also Internet devices used to link or separate several networks. Routers are used, for instance, in home networks, establishing the connection between the internal network and the Internet.
Scriptcode / Javascript	An object-based scripting language for developing applications. JavaScripts are programme components integrated in HTML code enabling specific functions in internet browsers. For example, while checking user input on an internet form, a JavaScript can verify that all the characters entered of a telephone number are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the client's computer. Unfortunately dangerous functions can also be programmed with Javascripts. In contrast to ActiveX, JavaScript is supported by all browsers.
SIM card	A SIM card (subscriber identity module) is a chip card inserted into mobile phones and used to identify the user on the network
SMS	Short Message Service Service to send 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.
Source text	In computer science, source text (or source code) refers to the text of a computer programme written in a programming language that humans can read.
Sourcecode	Computer program written in a human-readable programming language.
Spam	Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails 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 victim is made to believe that he/she is communicating via e-mail with a person they are acquainted with.
SQL Injection	SQL injection refers to the exploitation of a vulnerability in connection with SQL databases, resulting from insufficient verification of the variables to be transmitted. The attacker attempts to inject his own database commands, in order to change the data as desired or to gain control over the server.
SSH daemon	Secure shell protocol with which, thanks to data encryption, it is possible to securely log in to a computer system that is accessible via a network (e.g. the Internet). A daemon is a program that runs as a background process.
Stream	In computing, the term "data streams" refers to a continuous sequence of data elements with an unforeseeable end.
Two-factor authentication	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, list of codes, etc.) 3. Something you are (e.g. finger print, retina scan, voice recognition, etc.)
UPnP	Universal Plug and Play (UPnP) permits direct access and control of appliances or devices (audio devices, routers, printers, building controls) over an IP network with or without central control via a residential gateway.

User Agents	A user agent is a client programme for accessing a network service.
User Datagram Protocol (UDP)	UDP is a minimal, connectionless network protocol belonging to the transport layer of the Internet protocol family. UDP's job is to assign data transferred via the Internet to the proper application.
Vulnerabilities	A loophole or bug in hardware or software through which attackers can access a system.
Watering-Hole Attack	Targeted infection with malware using websites preferentially used only by a specific user group.