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 2015/I (January – June)

29 OCTOBER 2015

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

1 Overview/Content

2 Editorial

Pascal Lamia, 48, has been the head of the Reporting and Analysis Centre for Information Assurance MELANI since 2008

Dear reader,

The Reporting and Analysis Centre for Information Assurance (MELANI) celebrated its tenth anniversary on 1 October 2014. Innumerable cases have been reported to us over the past decade. MELANI has gained a broad range of experience in the meantime, ranging from run-of-the-mill attempted fraud to espionage attacks. Since 2004, many operators of critical infrastructure have been able to benefit from our support in the areas of preventing and resolving cyberattacks.

MELANI owes its success primarily to the private sector. Without the smooth functioning public-private partnership, i.e. the successful cooperation between the Confederation and the private sector, MELANI would never have achieved its current status. I would like to express my heartfelt thanks to all of those people in the administration and the private sector who over the past decade have made MELANI what it is today.

We have used the advent of MELANI's second decade as an opportunity to have a new emblem created. On the one hand, the emblem symbolises global digital data flows and on the other, it depicts international networking. Without the personal network of partner organisations throughout the world, it would not be possible today to successfully tackle cyber threats.

This semi-annual report is also a step into MELANI's second decade: it has been structurally completely revised and is meant to make it easier and more pleasant for you to read.

I hope you enjoy reading this report,

Pascal Lamia

3 Key topic: website security

In the last 15 years, the internet has grown significantly. Thousands of new websites go online every day. According to Netcraft[1], there are currently more than 850 million active websites. One of the reasons why the number of websites has grown so significantly is due to the use of *content management systems (CMS)*, such as WordPress, Typo3, Joomla! and Drupal. By using a CMS, internet users can publish content on the internet very simply without an in-depth understanding of ICT. In addition, there are a number of *plugins* which are available and which allow the website to be adapted according to one's own wishes. Due to their easy operation, CMSs are often used not just by amateur webmasters but also by small and medium-sized enterprises (SMEs) to publish their information on the internet.

Whereas a CMS is very practical on the one hand, on the other it also acts as a valuable target for hackers. The majority of *phishing* pages and *drive-by infections* are placed on websites operated using CMSs that are not up to date. As with many programs, security vulnerabilities also regularly occur in CMSs, for which the respective manufacturer as a rule promptly makes corresponding security updates available. For example, in 2014, 14 vulnerabilities were discovered and fixed in the CMS software Drupal, nine in Joomla! and 29 in WordPress.[2] Websites which have been created with a vulnerable CMS version can be found and attacked automatically on the internet using tools. It is thus relatively easy for criminals to detect and manipulate a large number of vulnerable websites in this way. It is therefore essential that all website operators update their CMS software regularly (patches). Nevertheless, too little attention is being given to this very area in many cases. By using outdated (and insecure) CMSs, website operators are not only endangering other internet users but themselves as well. Several cases were reported to MELANI In the first half of 2015 in which outdated CMSs had been compromised. The data in the CMS was copied and subsequently used to blackmail the owner. There is a particular danger here for SMEs in that client data is also stored in many CMSs.

As a rule, CMS security updates are quickly made available by the manufacturer. However, in contrast to the majority of operating systems, this does not occur automatically but very often has to be manually initiated by the operator. It is unfortunately the case that the majority of website operators who use a CMS for their website install it once and over a number of years run the website on the same (and thus, as a rule, outdated and insecure) version of the CMS. The following examples of vulnerabilities in WordPress, which can be extended to all other CMSs, highlight this behaviour.

70% of Swiss WordPress installations are vulnerable

In April 2015, it became known that a vulnerability in WordPress allowed attackers to carry out a *cross-site scripting attack* (XSS) against every vulnerable website whereby the attacker writes a comment with specially prepared *JavaScript* on the vulnerable website (CVE-2015-3429). On the same day, WordPress published a security update to eliminate the vulnerability. However, on 6 May 2015, the next WordPress security vulnerability was made public which allowed an attacker to carry out a further cross-site scripting attack (XSS) against WordPress (CVE-2015-3440). Here again, WordPress published a security update the following day.

---

1 http://news.netcraft.com/archives/2015/08/13/august-2015-web-server-survey.html (as at 31 August 2015)

2 https://cve.mitre.org (as at 31 August 2015)

However, the speed at which the operators concerned reacted was alarmingly slow. In Switzerland for example, approximately 6% of websites are operated using WordPress. Although the security updates were available, over 70% of the websites remained vulnerable.[3]

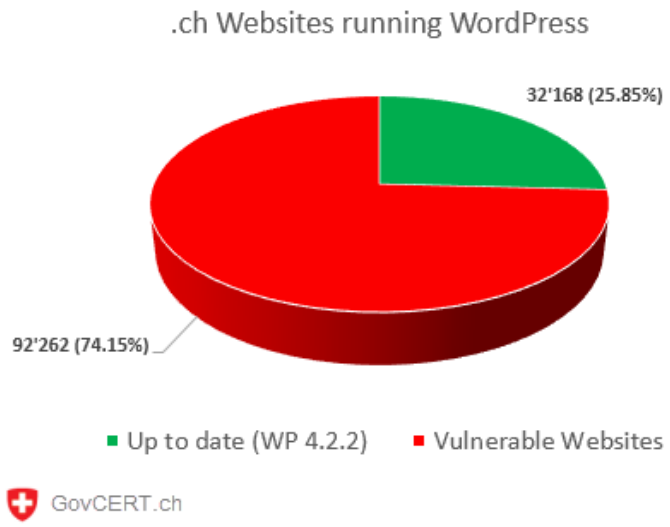


Figure 1: WordPress users still vulnerable to CVE-2015-3440 and CVE-2015-3429 (red) two months after the patch was made public.

Regular updates – necessary but not sufficient

The findings from the analysis drawn up by MELANI are alarming and raise the question of why so many website operators use vulnerable CMS versions. Alongside a lack of awareness and time, the answer is likely to include a certain degree of laziness. Many do not see the necessity of installing patches on their CMS or are not aware of the impact vulnerable CMS installations can have. However, operating a CMS also involves a certain amount of responsibility, which must be taken seriously. In addition to *prompt patch management*, there are also other measures which can improve the security of CMS systems:

- **Two-factor authentication**

  Besides the normal authentication (username and password) which is needed to access the administration area of a CMS, MELANI recommends the use of a two-factor authentication. Such an additional *one time password* (OTP) can be generated for example with the software Google Authenticator. It installs an app on your Mobile Phone (Android, iOS, Blackberry), which generates every 60 seconds a new OTP. Google Authenticator can be installed on the webserver (CMS) with an appropriate plug-in, which already exists for numerous different Content Management Systems like Wordpress or Typo3.

[3] GovCERT.ch blog post: "Outdate WordPress: Thousands of websites in Switzerland are vulnerable" http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable (as at 31 August 2015)

- **Restriction of administrator access to certain IP addresses**

  Such a restriction can be extended to IP-address, IP-range or on the geolocation of an IP-address. Such plugins already exist for a number of Content Management Systems.

- **Restriction of administrator access using a .htaccess file**

  The advantage of this measure is that it not only restricts the IP-range, but it is also possible to implement an additional authentication, such as (Username / Password) (Basic Authentication).

- **Securing the computer of the webmaster**

  It is often the case that websites and CMS are being compromised through stolen FTP credentials. Normally, this is done by means of a Trojan on the webmaster's computer. It is therefore imperative that the webmaster makes sure that the computer he is using is not only free from malware, but also is also protected by an up-to-date antivirus software. In addition, the FTP-connections (sFTP) should be encrypted if possible.

- **Web Application Firewall**

  With a Web Application Firewall (WAF) it is possible to block attacks before they reach the application. There are many different WAF-solutions. The most famous open-source solution is ModSecurity.

- **Early recognition of vulnerabilities.**

  The ultimate goal is to be able to identify potential security gaps before the criminals do. Here too, there are many different solutions to be found on the Internet. Some of which are even free.

The complete instructions and checklist can be found on the www.melani.admin.ch website:

Measures to secure content management systems (CMS)

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

In addition you will find instructions and a checklist here on what to do when an attack has already occurred:

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/instructions-for-cleaning-up-websites.html

4 Situation in Switzerland

4.1 Espionage

In the first half of 2015, there were two espionage cases in particular which aroused public interest and in which Switzerland was directly or indirectly involved. But a distinction must be made in each case as to whether or not the attack was aimed at a specific target in Switzerland or whether or not Swiss infrastructure was used as a base for espionage against third parties. It is evident that not all cases in the area of espionage become public. When it involves industrial espionage, past experience shows that companies are very cautious because they fear their reputation will be damaged. Generally speaking, there is continuous interest and accordingly continuous pressure on sensitive data. A case which attracted huge attention in the first half of 2015 was the discovery and publication of the Duqu2 malware which was reputedly active above all in the nuclear talks with Iran.

4.1.1 Duqu reloaded: sophisticated espionage software used against the participants in the nuclear talks with Iran

In March 2015, the Wall Street Journal reported, based on White House sources, that confidential US internal talks on the nuclear agreement with Iran had allegedly been bugged. Israel was suspected by the USA as the possible culprit in this case.[4] [5] Israeli politicians, however, categorically denied any Israeli involvement immediately. On 10 June 2015, the Kaspersky security company announced in a report that both it and various venues, where the talks in the nuclear negotiations with Iran took place, had been affected by a spying incident that used malware. Parts of the malware contained "very similar to almost identical"[6] software passages to the malware Duqu which surfaced in 2011 and was similar to the malware Stuxnet. This is why Kaspersky dubbed this malware Duqu2. As in almost all espionage incidents, the attack patterns which emerge from the technical analyses don't allow any clear conclusions to be made about possible perpetrators.

In the cases which have now been detected, the targets were the commemoration of the 70th anniversary of the liberation of the Auschwitz-Birkenau concentration camp and the P5+1 talks on Iran's nuclear programme. Computer experts discovered the malware in three places where the P5+1 talks took place. The last rounds of talks took place in Lausanne, Montreux, Geneva, Munich and Vienna.[7]

Based on information from the Federal Intelligence Service (FIS), on 6 May 2015, the Federal Council authorised[8] the Office of the Attorney General of Switzerland (OAG) to open criminal proceedings against persons unknown in this case. In mid-May, various appliances were seized in a house search in Geneva.[9] The authorities in Austria also began investigations into suspected espionage in this case. The focus here was on the Palais Coburg hotel in Vienna where several meetings on nuclear negotiations had taken place.[10]

---

4 http://www.wsj.com/articles/israel-spied-on-iran-talks-1427164201 (as at 31 August 2015)

5 http://www.theguardian.com/world/2015/mar/24/israel-spied-on-us-over-iran-nuclear-talks (as at 31 August 2015)

6 http://www.zeit.de/digital/internet/2015-06/duqu-2-kaspersky-labs (as at 31 August 2015)

7 http://www.kaspersky.com/about/news/virus/2015/Duqu-is-back (as at 31 August 2015)

8 http://www.heise.de/newsticker/meldung/Kaspersky-Trojaner-hatte-auch-Atomverhandlungen-im-Visier-2689929.html (as at 31 August 2015)

9 http://www.srf.ch/news/international/cyber-spionage-bei-atomkonferenz-in-genf (as at 31 August 2015)

10 http://www.tagesschau.de/ausland/duqu-103.html (as at 31 August 2015)

The espionage software was not only aiming at the final targets, but the security firm Kaspersky was also directly attacked. Apparently the attackers trawled through the company network to gain access to data which would facilitate an attack on the targets. IT-Security companies represent a fundamental pillar according to the base confidence in the internet. Attacks with the aim to misuse these companies for further attacks, affect the efforts to develop the internet as a trustworthy medium for example for business activities. Guidelines in this area must be discussed in the future.

For further information see MELANI semi-annual report 2013/2 chapter 5.1:

https://www.melani.admin.ch/melani/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html

4.1.2 Swisscom lines apparently bugged by NSA and BND

According to statements by the Austrian member of parliament Peter Pilz, the German Federal Intelligence Service (BND) and the US National Security Agency (NSA) has allegedly trawled through internet transit data at the Frankfurt internet exchange point for specific search terms in the context of operation Eikonal[11]. The objective of the search was to obtain information concerning terror suspects and arms smugglers. The search terms were transmitted to the BND by the NSA. However, in the course of time, strange, irrelevant search terms should have observed time and again which could only be indirectly linked to this operation.

The operation focused on 250 transit lines. According to Mr Pilz's list, there were also nine lines among these whose endpoints were operated by Swisscom in Switzerland and which led to Prague, Sydney, Tokyo, Seoul, Luxembourg, Warsaw and Moscow. Switzerland was thus one of 64 countries affected by the BND/NSA surveillance measures. The statements made are based on a contract between the BND and German Telecom from 2004 which was published by Mr Pilz. However, according to a statement made by Swisscom, these lines are currently not any more in its possession.[12]

[11] http://www.zeit.de/politik/deutschland/2015-04/bnd-nsa-kooperation-verantwortliche (as at 31 August 2015)

[12] http://www.nzz.ch/schweiz/bnd-und-nsa-sollen-swisscom-kunden-ausspioniert-haben-1.18549890 (as at 31 August 2015)

The Swiss Federal Intelligence Service (FIS) published the brochure "Prophylax" on the topic of industrial espionage. This brochure is part of a prevention and awareness enhancement campaign on non-proliferation and industrial espionage. It serves to raise the awareness of companies and educational establishments and provides information on how dangers and illegal activities can be recognised and prevented and what the authorities are doing to prevent and counter such activities.

http://www.vbs.admin.ch/internet/vbs/en/home/documentation/publication/snd_publ.html

4.2 Data leaks

The theft of data stored electronically can occur as a result of a variety of motivations: countries will be interested in the data itself if it provides them with a strategic or economic advantage for example. For cybercriminals, the theft of data can provide them with quick financial gain. To this end, blackmail is currently one of the most common modi operandi, and this problem has already been extensively covered in the preceding semi-annual report.[13] To be able to extract money from their victims, criminals must have a means of exerting pressure; this is where the stolen data is useful to them.

4.2.1 Rex Mundi

Rex Mundi is an attacker specialised in this type of modus operandi. It acquired a certain notoriety after claiming a number of victims primarily in Belgium in 2014. In January 2015, Switzerland was also affected when an attack was carried out on a company in the French-speaking part of Switzerland. This event was identical to what had been observed up to that point. As a first step, an *SQL injection* attack was used to gain access to a database that contained information entered on a contact form used by the public available on the company's website. This was personal data (addresses, telephone numbers, etc.) and communications transmitted via this form. Afterwards the criminals demanded payment in return for not divulging this information. Rex Mundi is well aware of the potential reputational damage in which might be generated by the response to this attack and relies on this in an attempt to extract payment. To place further pressure on the company, Rex Mundi used Twitter, as always, to publicise the incident, its demands and the reaction of the company. The firm did not give in to the blackmail and the data was released. Anticipating the expected outcome, the company had already started to contact its clients to inform them of the leak and how this data could possibly be used.

In addition to the damage to the company's image, the nature and value of the information divulged can in itself pose problems. This is particularly applicable if this information includes confidential matters on the company and its operations. But in the case of Rex Mundi, the problem was rather the use which could be made of the personal client data, such as subsequent fraud attempts using social engineering. Moreover, the value of this information can serve as an opportunity to obtain financial advantage from the attack if no payment is made by the company. What comes to mind here is the possible resale of the data on underground markets. More generally, this type of case once again raises the issue of the security of public websites which are very often vectors for different types of attack.

[13] MELANI semi-annual report 2014/2, chapter 5.3: https://www.melani.admin.ch/melani/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (as at 31 August 2015)

This issue has frequently been addressed by MELANI (see the semi-annual report 2014/II, chapter 3.5 "CMS – vulnerabilities and a lack of awareness among web administrators") and is the subject of the following document:

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

4.3 Industrial control systems

The topic of industrial control systems is becoming more important now that more and more processes are controlled by ICT. This subject area also includes what is called *Industrie 4.0*, the fourth industrial revolution. However, the term "industrial control systems" is very broad and can cover virtually everything from controlling a nuclear power plant to building management. This may in certain circumstances lead to various problems getting mixed up. In the following chapters, we will mainly examine critical systems. Systems with high criticality certainly include those which contribute to the supply of electricity.

4.3.1 Hydroelectric power plants as a honeypot – 31 attacks

One way to find out how real the risk of an attack is, is to use so-called *honeypots*. In this case, systems which imitate the authentic target systems are placed on the internet in a controlled manner to attract attacks without any damage being caused.

In February 2015, the Sonntagzeitung[14] featured a study of this nature which dealt with hydroelectric power plants. To this end a system was set up which for three weeks masqueraded as a hydroelectric power plant. The result was 31 attacks including three attacks by hackers who attempted to cause an error in the system or make the system crash. Even though this was a model experiment and certainly cannot be fully applied to systems in use, it does, however, illustrate how interested attackers are in systems such as these. This is not the first time that a model experiment has shown whether and how control systems can be infiltrated, in particular those of small hydroelectric power plants. Two years ago a similar report made the headlines: it took just 15 minutes to assume control of a power plant in the Canton of Glarus.[15] Even if hacking a small power plant does not necessarily have an impact on the electricity grid, an orchestrated attack on several smaller systems could, however, lead to sudden current fluctuations and thereby to possible chain reactions or even to a widespread power cut.

[14] http://www.sonntagszeitung.ch/read/sz_08_02_2015/nachrichten/Angriff-auf-die-Stromversorgung-27051 (as at 31 August 2015)

[15] http://www.srf.ch/sendungen/10vor10/spur-von-snowden-entlastung-fuer-sachs-angriffe-via-internet (as at 31 August 2015)

The fundamental question arises as to why, in spite of known vulnerabilities and apparently in spite of the interest shown by the attackers (at least in the honeypot system), more extensive cuts or breakdowns have not occurred. The answer to this question is not a simple one. One possibility is the lack of a business model by the hackers: given that in addition to virtual access to the systems, physical access is also usually available, a system can easily be cut off from the internet in the event of an attack (autonomy requirements of subordinate fallback levels). Another possible reason is that the attackers, whose primary motivation is financial, may feel constrained to a certain extent by not knowing exactly what impact (e.g. on human life) an attack on a system of this nature might have.

4.3.2 Open system control of water supply systems

It is not always easy for the Reporting and Analysis Centre for Information Assurance (MELANI) to assess how critically open systems should be categorised and if and how any sensitive systems are affected[16]. This was shown by an incident two years ago when hackers published numerous screenshots at the Chaos Communication Congress (CCC) of systems which hackers had apparently penetrated. Amongst these screenshots was the water supply system of a small Swiss commune. Further analysis and enquiries at the commune revealed, however, that this access had not been published indeed but interested citizens were able to look at this data. It could be seen on the charts how much water flows into the reservoir from the individual sources. However, no critical data had been visible and it had also not been possible for any harmful action to be taken via remote access.

Things can also take a very different turn as a similar case from the current reporting period shows. This situation also concerned a Swiss water supply system and the readings of figures relating to individual sources and reservoirs. Upon closer analysis, however, MELANI detected that pre-programmed passwords had been used on the website to retrieve the data from the control appliances and thus to be able to access the control components. A password which is so easily accessible again provides a dangerous, additional point of attack.

[16] http://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (at 31 August 2015)

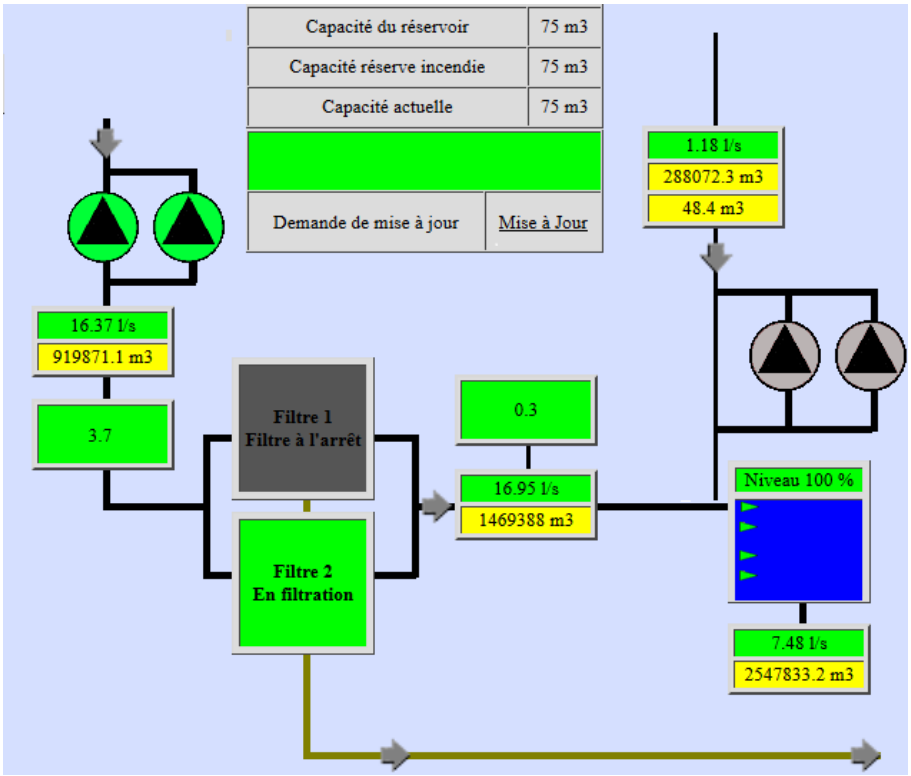


Figure 2: Diagram showing a publicly accessible platform of a water supply plant in Switzerland

MELANI provides a checklist of measures for the protection of industrial control systems. The mentioned measures should be embedded in an overarching security process, ensuring that the measures are applied, regularly verified, and continuously improved. Moreover, it is important for operators of installations to know the current threat situation, to monitor that situation regularly, and to incorporate the findings into the implementation and improvement of the security measures. For this purpose, close cooperation between risk management, engineering, and operations is of the utmost importance.

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

In February 2015, the European Union Agency for Network and Information Security (ENISA) published a new study. This provides information on the challenges and recommendations for developing systems to certify the skills of cyber experts who work with industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems in Europe.

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

4.4 Attacks (DDoS, defacements)

Swiss companies and the public in Switzerland continue to be the targets of different types of attack. Their websites are a primary target for these attacks. The importance of maintaining a

reliable online presence especially for companies makes denial of service attacks and website defacements particularly problematic.

4.4.1 DDoS and extortion: wave of attacks by DD4BC

Extortion is currently one of the methods most favoured by cybercriminals seeking rapid financial gain. Different types of attack can be used as leverage to extract money from a target, which include *denial of service* (DoS) attacks. DD4BC is an attacker that has been specialising in this type of attack since July 2014. It is characterised most notably by its immense flexibility in terms of target selection. DD4BC has in effect been active both in Europe and the United States, Asia and Oceania and targets specific sectors in successive phases. After focusing on the Bitcoin industry then online casinos, DD4BC claimed numerous victims amongst banks and companies in the finance sector.

This group was particularly active in Switzerland during the first half of 2015. MELANI was informed of about ten cases which affected different companies, in particular in the finance sector. The information gathered ties in with what has been observed in other countries, which shows the modus operandi of this player. The attack generally starts with an initial, low-intensity DDoS (as a rule 10-15 Gbps). After this attack that show the possibilities of what is possible, the attacker sends an e-mail to blackmail the victim. If the latter wishes to avoid a more severe attack, the victim is asked to pay a sum of 30 to 40 Bitcoins (which at that time was equivalent to CHF 7,500 to 10,000). DD4BC claims to have the capacity to strike with an attack of 400 to 500 Gbps. However, this player has never been able to prove this capacity. In the event of non-payment, attacks of up to 30 Gbps[17] were sometimes observed, whereas in other cases, the attacker did not carry out the attack at all.

An inaccessible website may represent a huge loss for its owner, particularly if the services attacked are commercial. The attacker thereby hopes that the target will choose to pay in order to protect itself from the negative impact of an attack of this nature.

MELANI recommends the targets of attacks of this nature not to give in to blackmail. They should immediately contact the host of the website and the upstream provider to take protective measures. Furthermore, the victims can report a criminal complaint with the cantonal police. MELANI has published a document on the topic of DDoS attacks and how to handle them:

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

4.4.2 Defacement of sites in French-speaking Switzerland

A surge of website *defacements* again made the headlines during the first six months of the year, in particular in French-speaking Switzerland. Firstly, a large number of French websites were defaced following the terrorist attack on the editorial staff of Charlie Hebdo, as were websites in western Switzerland, albeit to a lesser extent. At the time, different groups sent out messages containing Islamist propaganda and justifying the attacks. In France, the authorities recorded 1,300 attacks which lead to 25,000 websites being hacked (see chapter 5.4.3). The Swiss sites targeted were hit because of they form part of the French-speaking

[17] External reports confirm the occurrence of attacks up to 60 Gbps. See: http://pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf (as at 31 August 2015)

community. It is to be assumed, that the attackers didn't selectively attack Swiss sites, but more likely confused them with French targets.

In April, a number of other cases of website defacement in western Switzerland were also reported to MELANI and were mentioned in press articles. In these cases, the hacked web pages were also used for Islamist propaganda purposes by a group claiming to be close to the Islamic State. In these instances, however, it would be an exaggeration to talk about a wave of defacements. After analysing the different cases brought to the attention of MELANI, it transpired that they were all the work of one attacker. According to the zone-h.org site which keeps a record of cases like these, a hacker known as "cwne" hacked 180 web pages between 24 and 26 April. All of the sites were hosted by the same provider. In all likelihood, "cwne" exploited a security flaw on the server which hosted a large number of sites (practice of mass defacement). This example shows that it is sometimes possible to achieve a large number of high-profile defacements and a publicity with a single attack, especially if the affected sites are those of companies or organisations located in a geographically restricted area. What is sometimes perceived by the media or the public as a large-scale campaign is in reality the result of a hacker exploiting a single security vulnerability.

Sometimes a link is sought between the hacked websites and the messages disseminated. Generally speaking, this link does not exist as the attackers mostly operate opportunistically and unspecific target vulnerable websites, regardless of their content.

Basic security rules such as updating the programs used on the website and web server provide considerable protection from this type of attack. MELANI has published the following document on this topic:

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

4.5 Social engineering, phishing

Apart from all of the technical attacks, it is also the attacks that exploit human weaknesses which are popular with attackers. The possibilities offered by social engineering are amply demonstrated by a case in the US: a manager in the US company Scoular successively transferred USD 17.2 million to fraudsters via a Chinese bank account in the belief that he was acting directly on behalf of his boss. A study of the auditing company KPMG backs up this observation and shows that companies still place too much emphasis on technology and neglect the human factor in protection against cyberattacks. Basically, an integrated and balanced approach should be pursued which, in addition to technology, also takes account of people and processes.[18]

4.5.1 Phishing – attacks on cantonal banks, credit card data, advances in phishing e-mails

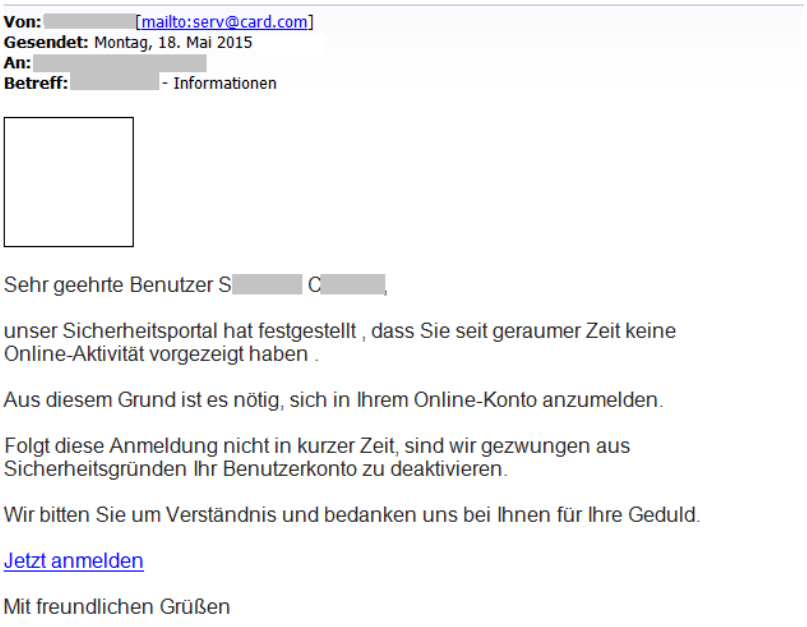
Phishing is still a big, if not the biggest, topic area in social engineering. Most of the attacks observed nowadays are standard attacks. To start with, a financial institution is selected

[18] http://www.kpmg.com/CH/en/topics/cyber-security/Pages/default.aspx?utm_source=mediarelease&utm_medium=email&utm_content=medien-de&utm_campaign=cybersecurity (as at 31 August 2015)

whose costumers will be subjected to the phishing attack. Then the webpage layout and the e-mail layout is copied and drafted, a credible story for the victim is invented and the same attacks are launched over a period of days and months. At the same time, there are phishing waves where websites are stored each time with the same provider. After the phishing pages have been deactivated by the provider, it does not take long before the same web page is online again in a different location.

This is what happened in the phishing attacks observed on Swiss cantonal banks which were recorded repeatedly in the first half of 2015. A feature of this surge of attacks was that it was not the cantonal bank of a specific canton which was the target, but in general the customers of cantonal banks in the entire German-speaking part of Switzerland. This implicitly increased the potential number of victims. Only in a second stage did the victim have to specify the cantonal bank where the e-banking account was held and then of course provide personal data.

However, thanks to the increasing awareness of e-banking customers, attackers have to constantly come up with newer and better attack methods. This includes a personal form of address using first and last names which is designed to gain the trust of potential victims. Up to now, this method had not been widely used, as it probably still required too much work to correlate the first and last names with the corresponding e-mail addresses. However, this was precisely the approach selected in a wave of phishing attacks in the second half of 2015. It is difficult to say where the attackers obtain this data from. It could come for example from compromised e-mail accounts which were accessed by the criminals.



Von: [mailto:serv@card.com]
Gesendet: Montag, 18. Mai 2015
An:
Betreff: - Informationen

Sehr geehrte Benutzer S C,

unser Sicherheitsportal hat festgestellt , dass Sie seit geraumer Zeit keine Online-Aktivität vorgezeigt haben .

Aus diesem Grund ist es nötig, sich in Ihrem Online-Konto anzumelden.

Folgt diese Anmeldung nicht in kurzer Zeit, sind wir gezwungen aus Sicherheitsgründen Ihr Benutzerkonto zu deaktivieren.

Wir bitten Sie um Verständnis und bedanken uns bei Ihnen für Ihre Geduld.

Jetzt anmelden

Mit freundlichen Grüßen

Figure 3: Example of a phishing e-mail with the use of the first and last name as the form of address

The important role played by the targeted form of address, a plausible story and thus professional social engineering is shown by cases where the client database of a company was hacked and copied in the run-up to an attack. This occurs mostly via *SQL injections*. This is followed by a targeted e-mail on behalf of the company referring the recipient to a website which has been perfectly imitated and on which the credit card number must be entered for some reason. Given that the victim was probably in contact with the legitimate company and the pretext sounds plausible, there is a good chance that the victim will

succumb to it. All the affected company can do is inform its clients immediately about the attempted fraud.

4.5.2 Phishing after defacements and sometimes vice versa

In recent times, MELANI has increasingly become aware of a connection between defacements and phishing attempts. So that the fraudsters can set up phishing pages, they firstly have to purchase a domain or compromise an existing website by exploiting security vulnerabilities. In the case of defacements, security vulnerabilities on websites are also exploited to subsequently change content and post personal, religious or political statements. Furthermore, defaced websites are often published on publicly accessible websites such as zone-h.org[19]. This makes it easy for phishers to find websites with known vulnerabilities and also to exploit them and place their phishing sites here. By contrast, the reverse situation, i.e. the defacement of an existing phishing site is much less likely. This is primarily because there is no official list of phishing sites, and secondly, because when these sites are discovered, they are removed from the internet as quickly as possible.

In May 2015, MELANI noticed precisely this kind of approach for the first time. Firstly, a normal phishing attack on a Swiss financial institution was reported. As is usual in such cases, the site was examined and then brought to the attention of the respective provider so that it could deactivate the site. But before the provider could react and remove the fraudulent site, the phishing attack was thwarted by a hacktivist, who placed on the website a message against xenophobia. As a result, the hacktivist – probably unintentionally – prevented potential victims from exposing their data on the phishing site.

4.5.3 Bogus tax forms

Numerous companies in the Geneva area received an e-mail in the first half of 2015 with a form which supposedly came from the Geneva tax authorities. The form on which gains from real estate and other company details had to be declared subsequently had to be sent together with the last rent bill to an e-mail address. The form to be sent back actually exists but the return address indicated had nothing to do with the Geneva tax authorities and belonged to a fraudster.

A similar case was also found in the Canton of Vaud[20].

But for what purpose can data such as this be exploited when it is in the hands of fraudsters? This would seem to primarily be preparatory action for so-called president scams. In the preliminary stages, information on the company is obtained by the attacker to form a precise picture of the organisation and the target's environment. This information is gathered in part by active research as described here. Then the actual attack starts. As a rule, an e-mail that appears to have come from one of the members of senior management is sent to an employee in the finance division. The e-mail sent deals mostly with current, confidential financial transactions. The fraudsters emphasise the unique nature and the confidentiality of this order, but also the urgency that the situation requires. In many cases, the fraudsters attempt to add even more credibility to the scenario using parallel telephone calls.

The Canton of Geneva has published a warning message on its website.[21]

---

[19] Zone-h.org is an archive of defaced websites

[20] http://www.24heures.ch/vaud-regions/arnaqueurs-utilisent-adresse-fisc-vaudois/story/10817017 (as at 31 August 2015)

The main rules of conduct for dealing with e-mails help you to protect yourself from phishing and other types of fraud:

Be wary of any unsolicited e-mails you receive: caution is called for not only with regard to e-mails from unknown persons, but also from known senders. Particularly trustworthy companies are often used as false sender addresses.

- Be sceptical if you receive e-mails that require action on your part and that carry a threat of consequences (loss of money, criminal charges or criminal proceedings, blocking of account or card, missed chance, misfortune) if the action is not performed.
- Do not open any attachments or click on any links in suspicious e-mails, otherwise you risk infecting your computer with malicious software. In case of any doubt, check with the supposed sender about the contact information indicated on the website, what the e-mail is about is exactly and whether or not it actually comes from the sender.
- The basic rule of not disclosing any internal information or complying with any requests when confronted with questionable or unusual contacts is more relevant than ever in view of the recent cases.

Especially for companies:

- All processes which concern payment transactions should be clearly defined internally and complied with by employees in all cases.
- In particular, MELANI recommends raising employees' awareness of these incidents, especially employees in key positions.
- When confronted with unusual contacts and requests, it is recommended to telephone those concerned within the company to verify the accuracy of the order.
- A fact sheet for SMEs concerning ICT security is available on the MELANI website at: https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html (not available in English)

4.6 Crimeware

Crimeware is a form of malware further developed by cybercriminals which, in criminological terms, ranks as computer crime and legally comes under internet fraud. In terms of crimeware, e-banking Trojans are still very common as the figure below shows. The majority of infected systems in Switzerland which were reported to MELANI involved e-banking Trojans such as Torpig, Dyre, Tinba, Gozi and ZeuS.

[21] http://ge.ch/impots/courrier-lectronique-frauduleux (as at 31 August 2015)

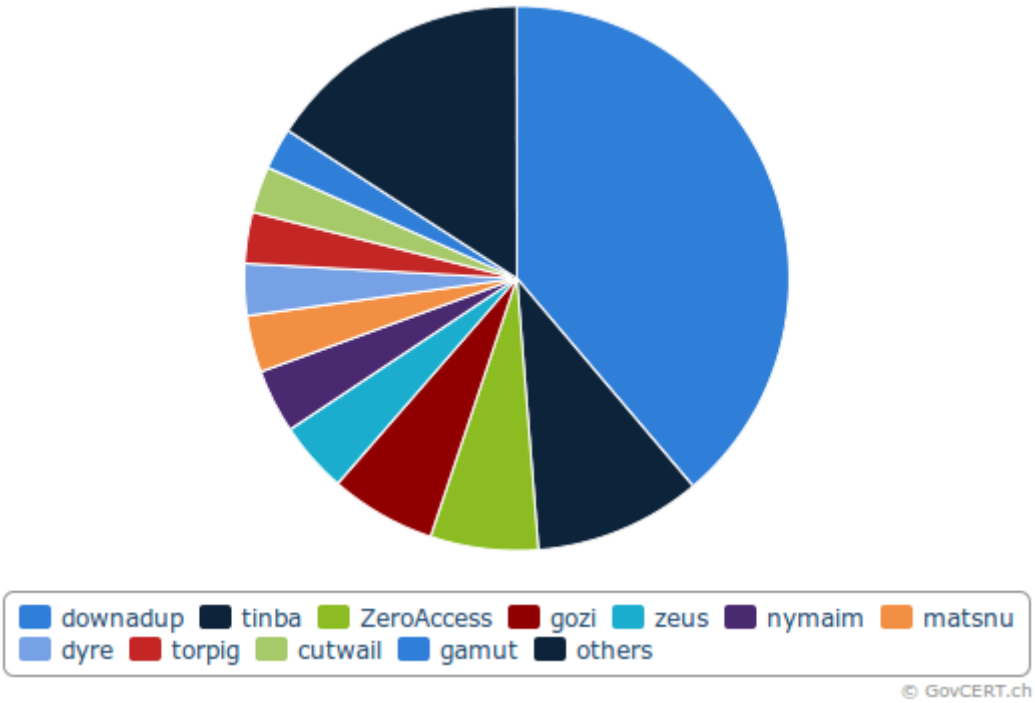


Figure 4: Breakdown of malware in Switzerland which is known to MELANI. The reference date is 30 June 2015. For current data see: http://www.govcert.admin.ch/statistics/dronemap/

In the case of geographic distribution, both the cantons of Zurich and Wallis in particular have a higher rate of infection than other cantons (taking into account the number of inhabitants).

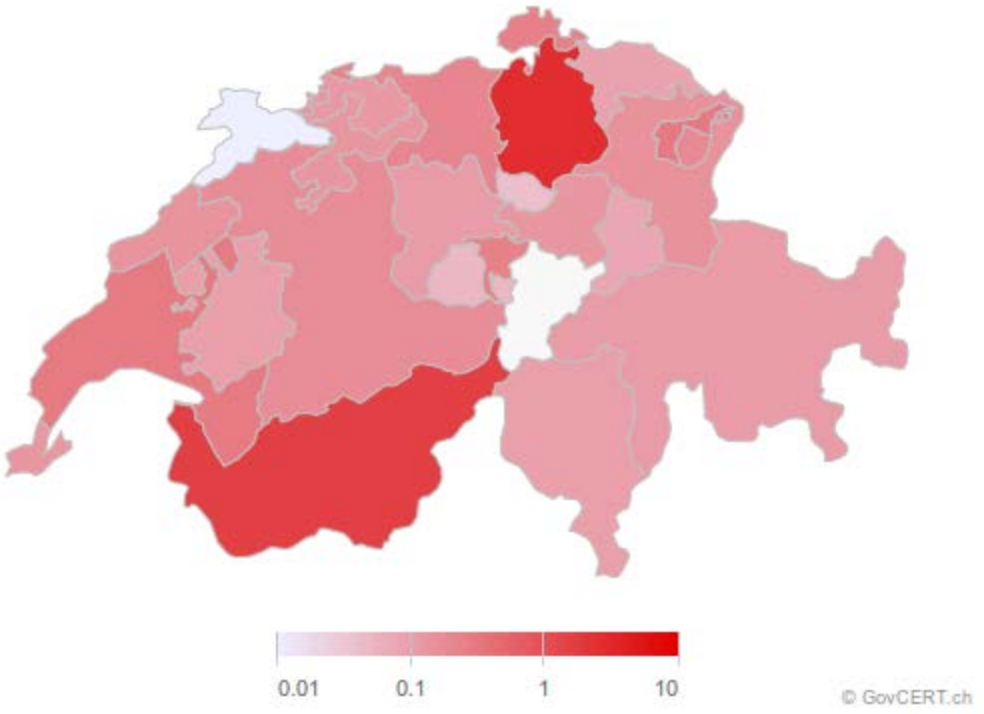


Figure 5: Number of infections per canton taking into account the number of inhabitants. The reference date is 30 June 2015. For current data see: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1.1 Downadup

What is worrying about Downadup infections (also known as Conficker) is that this worm has been in existence for more than 8 years and is obviously still widespread. Downadup is spread via a security vulnerability found in the Windows operating systems in 2008 which can be exploited via the internet. The persistently high number of infections can possibly be explained by the fact that many internet users in Switzerland are still using an older version of Windows (Windows XP) and do not regularly install patches on their operating system. Another possible explanation would be that there are still internet service providers (ISPs) in Switzerland which do not process the reports on infected clients (e.g. due to a lack of resources, technical means or know-how).

4.6.1.2 Dyre

In the first half of 2015, it was mainly the malware Dyre (also known as Dyreza) which spread throughout Switzerland. This is an e-banking Trojan which is spread via e-mail. For this, internet criminals prepare e-mails which generally masquerade as fax messages, bills or the like and have malware in the attachments (usually an executable file – .exe – in a Zip folder). Whereas Dyre set its sights mainly on Swiss SMEs[22] in the first few months of the year, and in the case of a company in Fribourg a seven-figure sum was stolen, since May 2015, it has increasingly been attacking private users[23]. At peak times, as many as 2,000 Dyre infections were reported to MELANI on a daily basis.

If you have already received e-mails such as these and have opened the attachment, we recommend that you scan your system with a virus scanner or malware removal tool. You can find more instructions here:
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/instructions-for-removing-malware.html

MELANI has prepared a fact sheet which is intended to assist SMEs in increasing ICT security in the corporate network. The fact sheet can found at:
https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html (not available in English)

Furthermore, you will find a ten-point programme to increase ICT security on the SME portal of the Confederation:
http://www.kmu.admin.ch/kmu-betreiben/03710/03712/03715/index.html?lang=de (not available in English)

4.6.1.3 Retefe

The Retefe malware continues to be active in Switzerland. MELANI reported on Retefe for the first time two years ago. It is spread exclusively via e-mail, normally via a bogus invoice from well-known online shops such as Zalando or Ricardo.

[22] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking-trojaner-hat-schweizer-kmus-im-visier.html (as at 31 August 2015)

[23] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/information_dyre_2.html (as at 31 August 2015)

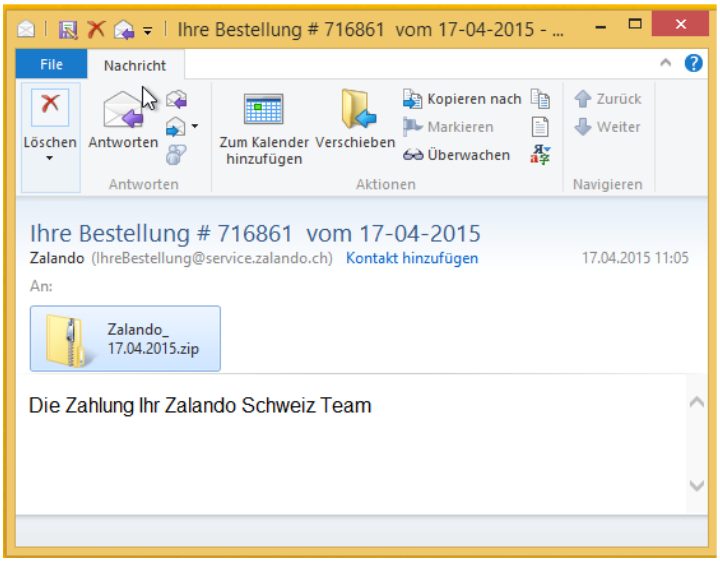


Figure 6: Example of a bogus e-mail which spreads the Retefe malware

If the recipient runs the executable file in the attachment, then the recipient's computer will be infected with Retefe. After successful infection, Retefe alters the settings in Internet Explorer in such a way that certain websites (i.e. the e-banking sites of several Swiss financial institutions) are redirected via a proxy server abroad. In addition, Retefe installs a harmful *certificate authority (CA)* in the Windows certificate store. As a result, Retefe is able to issue certificates for arbitrary financial institutions and thereby pass itself off as one.

If a victim logs on to the supposed e-banking site via a computer infected with Retefe, a *QR code* is displayed. This QR code leads to a harmful URL via which the victim is asked to download and install an App “to improve the security”, which is in reality an Android malware (a so-called SMS Trojan). If the victim installs the recommended Android app, all text messages for two-factor authentication from the bank will be forwarded to a web server abroad to the hackers. In this way, the hackers are then in a position to log in to the victim's e-banking account and also to make payments.

If you use an Android smartphone or tablet, make sure that you only install apps from the official Google Play Store. Never install apps from third-party sources, even if you are requested to do so. Also ensure that the following settings have been selected on your Android appliance:

Settings -> Security -> unknown sources -> DEACTIVATED

Google settings -> Security -> Search appliance for security threats -> ACTIVATED

Further information on Retefe can be found in the GovCERT.ch blog:

http://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

4.6.1.4 Tinba

Tinba (also known as Tiny Banker) also kept internet users in Switzerland busy in the first half of 2015 and was for a time, along with Downadup, the infection most frequently reported to MELANI in Switzerland. Tinba is another e-banking Trojan which also targets several Swiss financial institutions. However, in contrast to Dyre or Retefe, Tinba is a toolkit which

can be purchased in relevant forums on the internet for a few thousand francs. Internet criminals purchase the software and can then use this as they wish. Alongside the Tinba campaigns known in Switzerland, there are several dozen other Tinba campaigns globally which target financial institutions around the world.

4.6.1.5 Encryption Trojans – Cryptowall 3.0, TeslaCrypt and an author overcome with remorse

Numerous cases were once again reported in the first half of 2015 where data was encrypted by a cryptotrojan. These were mostly Cryptowall 3.0, but also cases involving the TeslaCrypt ransomware have increasingly been reported to MELANI. This mainly affects individuals but cases involving companies are also known. Whoever does not have an updated backup will lose all or at least some data. The case of Locker ransomware was remarkable. The malware had spread to various computers beforehand and was waiting to strike and to encrypt data, which then occurred at the beginning of June 2015. Shortly thereafter, the author spoke up and not only apologised, but gave the malware the command to decrypt and simultaneously published the key.[24]

A *backup* copy of data saved on the computer should regularly be made on external storage devices. The devices should be connected to the computer only during the backup procedure.

4.7 Preventive measures

To find a remedy for the multitude of threats, preventive measures are essential. These measures could be technical, organisational or also relate to criminal law. In addition, awareness-raising among the public is an important pillar in combating cyberattacks. The majority of attacks take advantage of the innocence and helpfulness of victims and try to catch them off their guard. Another important measure in combating cyber-related incidents is to establish a reporting culture, both in companies and also in general among the public. Only if employees feel that they are being taken seriously when reporting an incident they also continue to do so. It is for this reason that MELANI set up the "Antiphishing.ch" website, to which e-mails and websites suspected of stealing access data or credit card data can be reported.

4.7.1 Antiphishing.ch

In the summer of 2015, MELANI launched the antiphishing.ch website to be better able to channel and more efficiently analyse reports about phishing pages. Reports on phishing websites can be submitted via the internet form. In addition, the reporting website also provides an e-mail address to which phishing e-mails can be forwarded. You can access the website using https://www.antiphishing.ch.

[24] http://www.heise.de/security/meldung/Krypto-Trojaner-ueberlegt-es-sich-anders-und-entschluesselt-alles-wieder-2678669.html (as at 31 August 2015)

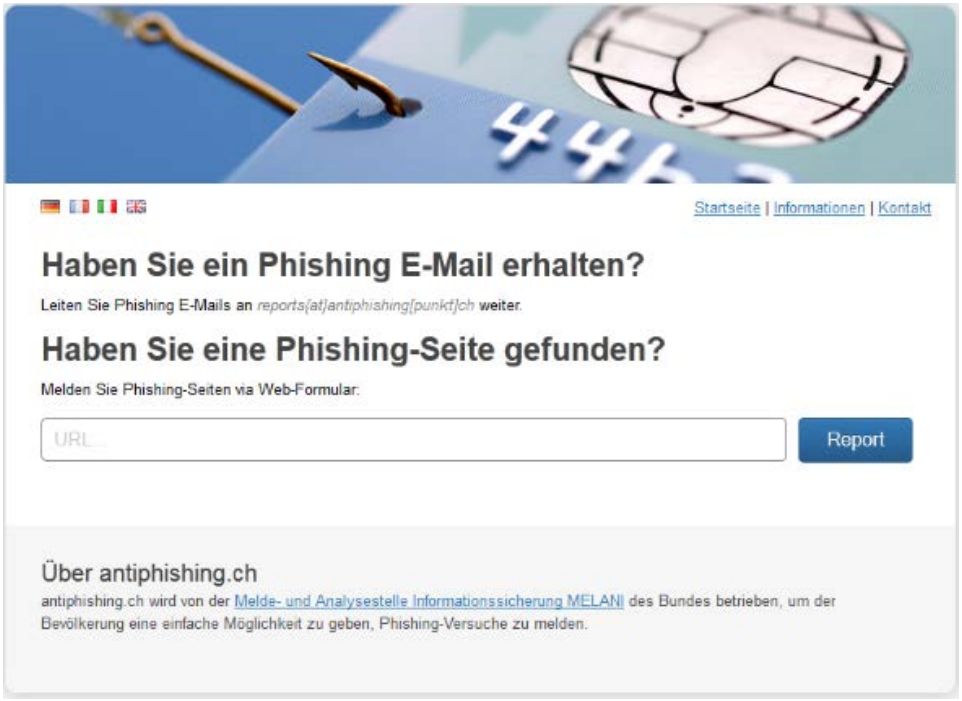


Figure 7: Screenshot of the new antiphishing.ch website to which citizens can report phishing pages.

The incoming phishing reports will be subject to an automatic preliminary examination. Based on the results of this, the phishing reports will be carefully examined manually before they are then reported to interested parties such as manufacturers of ICT security software, web browsers and hosting providers, as well as on request to the financial institutions and Internet Service Providers concerned, so that a maximum protective impact is achieved.

5 Situation internationally

5.1 Espionage

5.1.1 Hacker attack on the German Bundestag

On 15 May 2015, news broke that there had been a targeted attack on the Bundestag's "Parlakom" network and that the attackers had copied 16 gigabytes of data.[25] The attackers had apparently been looking for system passwords, Word documents and locally saved e-mails. According to the newspaper *Die Welt*, the initial infection was carried out with targeted e-mails containing a prepared link, as is so often the case.[26] [27] A protocol of a Bundestag's Commission that was unintentionally made public[28] stated that "unusual communication" between server systems had drawn attention on 8 May 2015. An unusual amount of data has

[25] http://www.spiegel.de/politik/deutschland/cyberangriff-auf-bundestag-abgeordneten-e-mails-erbeutet-a-1039388.html (as at 31 August 2015)

[26] http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html (as at 31 August 2015)

[27] https://www.tagesschau.de/inland/bundestag-cyberattacke-105.html (as at 31 August 2015)

[28] http://www.bild.de/politik/inland/bundestag/spielte-cyber-angriff-laut-geheimprotokoll-herunter-41314062.bild.html (as at 31 August 2015)

apparently been observed on a server of the Bundestag administration. Furthermore, there had been unscheduled connections between this server and an office of parliament members. Four days later, another analysis revealed that two computers had had contact with potentially dangerous servers, known as *command and control servers*. These were apparently the same systems that had already appeared conspicuous a few days earlier. Despite the fact that apparently only a small number of terminals had been affected, the attackers should have penetrated deep into the system, where they could move about freely and could become active again at any time.

As events progressed, it had apparently been difficult to remove the attackers from the network and the measure taken involved rebuilding parts of the network. As a result, the Bundestag's internal network was shut down for four days on 20. August 2015 in order to remedy the consequences of the cyber-intrusion. While this drastic measure shows the scale of this incident, it is certainly no guarantee against future infections.

The Federal Office of the Prosecutor General is checking whether an initial suspicion exists in this case for a criminal offence that comes under its jurisdiction. The espionage program used for the attack has allegedly been identified and it has been speculated that it was carried out by the malware group "Sofacy/APT28".[29] The program structure apparently resembles a piece of malware that had already been observed in a 2014 cyberattack on a German data network.

5.1.2 Carbanak – the electronic bank robbery

Until now, electronic bank robberies had been limited to end clients. In these cases, e-banking *malware* was used to infect the client's computer and take control of the e-banking session. A new type of electronic bank robbery became known in February 2015. An operation by the name of "Carbanak" had been manipulating banking systems on a large scale for two years. The resources used for this attack are similar to the targeted espionage attacks that are seen only in state operations. The first step in this process was to try to infect the computers of bank employees. For this, the classic method of sending a harmful attachment in a targeted e-mail was used. Then the attackers searched for the workstations of employees through which transfers were administered as well as ATMs connected to the network. The bank robbers spent between two and four months in the network in order to find out how they could exploit internal bank processes for their own purposes.[30] After the attackers had gathered this information, they posed as the bank employees and transferred money to themselves or manipulated ATMs so that they dispensed cash at a specific point in time. An accomplice was lying in wait at the ATM in question and collected the cash. To prevent the transfers from being noticed, the balances of the accounts that were to be robbed were first increased before subsequently being reduced again by this exact amount. The total amount in the victim's account remained unchanged, which meant that the victim did not notice the fraud so quickly.

According to Kaspersky, the attackers infiltrated at least 100 banks in 30 countries, most of which were in Russia. The money obtained justified the period of almost two years that the attackers spent on the scam: up to USD 10 million was stolen from each bank.

---

29 http://www.focus.de/politik/deutschland/bundestag-cyber-angriff-auf-bundestag-dauert-schon-laenger-als-bekannt_id_4761526.html (as at 31 August 2015)

30 http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide (as at 31 August 2015)

5.1.3 SIM cards allegedly targeted by NSA and GCHQ

In the first half of 2015, new revelations came to light that were based on Snowden documents. The focus of these were *SIM cards*, i.e. the cards that are inserted into mobile phones and used to identify users in the network. According to the newspaper *The Intercept*, a joint unit of the British Government Communications Headquarters (GCHQ) and the NSA known as the "Mobile Handset Exploitation Team (MHET)" apparently compromised the internal networks of large SIM card makers, major device manufacturers and many network operators. The spotlight was on the SIM card manufacturer Gemalto in particular, which also announced that it had observed or identified sophisticated attacks in its network in 2010 and 2011 which could point to NSA and GCHQ activities. In July 2010, targeted e-mails had apparently also been sent to employees.[31] The attacks centred on the exchange of encryption keys between mobile phone operators and their providers. In most cases, this exchange had already been encrypted by 2010. All attacks are alleged to have happened only on the office networks and not on production networks. It is not clear whether the NSA was really behind these attacks. Gemalto ruled out a massive theft of SIM encryption keys, which would be the worst-case scenario for an encryption specialist.

5.1.4 Espionage in professional sport

It is not at all surprising that cyber espionage also reaches the world of professional sport given the large sums of money involved here. This is also particularly true for the US baseball league. The St Louis Cardinals and the Houston Astros have been playing-field rivals for years. However, it would seem that Cardinals employees decided to no longer limit the game to the playing field and brought it to cyberspace. They collected not only points but also information, such as player training statistics, match statistics, contractual provisions and information on possible future player transfers, strategies, etc., which may certainly be just as valuable.

At the root of all this is the transfer of the Cardinals' general manager, Jeff Luhnow, to the Astros in 2011. Luhnow is known for focusing on statistical analyses. While at the Cardinals, he scouted for young talent, which he found using a database and a type of electronic player screening and thus contributed to the team's success. After he took up his position at the Astros, he proposed the same methods and again found success with them. The Cardinals publicly expressed their fears that Luhnow had made information about them available to their opponents.

In an increasingly connected and digital world, sport too comes under pressure to modernise. Analyses and statistics are being used to an increasing degree and also require the use of large amounts of data, which make them interesting espionage targets. Analysis is very common in baseball because they are player-specific, lower number of variables makes it easier to make predictions and readings. Such methods are less common in football and ice hockey, because it is not individuals but two teams competing against each other and there are more variables. Despite this, the football club Manchester City launched a competition in 2012 to encourage young analysts to develop methods for this area.

[31] http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx (as at 31 August 2015)

5.2 Data leaks

5.2.1 Over 21 million data sets stolen from the US Office of Personnel Management

In April 2015, the US Office of Personnel Management (OPM, the approximate equivalent of the Federal Office of Personnel in Switzerland) discovered that the personal data of 4.2 million current and former federal employees had been copied. The data included details such as names, dates of birth, addresses and social security numbers. While this case was being investigated, the OPM discovered another, even more substantial data theft which also involved background information on current, former and future federal employees and contracting parties. This recent incident more than likely involves 21.5 million individual data sets and pieces of information that were gathered as part of security screenings.[32] Of these, 19.7 million data sets are believed to stem from people who had applied for a job and some 1.8 million data sets from people who had a connection with job seekers, such as spouses or household members. Parts of the stolen data sets contain information such as mental health details, financial history and findings from interviews which were gathered by the screeners. 1.1 million fingerprints were also copied. In 2014, the OPM's internal Office of Audits had recommended shutting down 11 of its 47 ICT systems because they did not have valid security authorisation. The OPM did not follow this recommendation. It is unclear whether one of these ICT systems was affected by the hack. This largest-ever attack on a US government computer network cost OPM Director her job.

US investigators believe that a Chinese group was behind the attacks on the US federal administration. As expected, China immediately denied any involvement in the attacks.

Personnel offices are of particular interest to data collectors, especially if all of the information on the employees of an administration or group is collated and administered in one place. As a large number of documents from various sources must be processed here, this also results in an additional potential danger in the form of malware, which can be sneaked in from any of the various sources.

5.2.2 AdultFriendFinder, British Airways and health insurance – data leaks in a wide range of sectors

In recent years, a large part of mate-finding has moved online. The triumphs of the internet and the possibilities of social media also influence this area and simplify the search for the right acquaintances. However, if the website used falls victim to cybercriminals and the user data, including sexual preferences, is exposed online, then the anonymity that is so cherished is gone. A blunder of this kind happened to the dating website AdultFriendFinder[33] in May this year. Almost 4 million sets of user data that the individuals behind the aliases used to find each other with minimal effort ended up on a related forum, visible for all to see. This incident was topped by the attack on the infidelity website Ashley Madison[34] last July when the login details of 32 million users were published.

---

32 https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/ (as at 31 August 2015)

33 http://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web (as at 31 August 2015)

34 http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (as at 31 August 2015)

In the first half of 2015, also leaks of more critical data were reported. Customer data was stolen from the British Airways frequent flyer programme[35], providing access to information such as the movement profiles of the individuals affected.

It is an even more sensitive matter if detailed tax data ends up in the wrong hands, as happened in May to the US Internal Revenue Service (IRS).[36] The attackers managed to hack an IRS authentication process using social engineering enquiries and thus obtain taxpayers' details.

Patient data also belongs to the most sensitive type of data. Nobody wants details of their doctor's visits and illnesses to be made public. Unfortunately, this kind of particularly sensitive personal data is not always secure from prying eyes. Anthem[37], the second-largest US health insurance company, confessed in February that its database of 80 million customers had been broken into. Another health insurer by the name of Premera Health Care[38] also fell victim to this type of data theft in March.

For operators, this means motivated attackers do not stop at anyone. It is therefore strongly recommended that you take all possible precautions to avoid becoming a victim of data theft. Our leaflet on ICT security for SMEs provides a good overview:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html (not available in English)

5.3 Industrial control systems

After their discovery in recent years of *industrial control and SCADA systems* as a research and test field, ICT security experts are now also increasingly dedicated to the components that are installed in cars, trains, ships and aircraft. It is clear that the networking of all sorts of devices and the trend of being constantly connected to the internet does not stop at means of transport. Airlines, rail operators and shipping lines want to offer their passengers internet access on board, and more and more cars have connectivity too.

There are two different aspects here: access to information and entertainment offered online on the one hand, and the use of electronic and information technology to control the operation of the transport vehicle or to support its operator on the other.

While access to the World Wide Web is inherent in the first, another distinction can be made in the second between applications that must obtain information externally (e.g. *GPS data*, weather and traffic reports) and purely internal systems, such as the fuel gauge, tyre pressure gauge or the rear-view camera in cars, but also driver assistance systems that use sensors and actuators to keep the distance between the vehicle in front constant, brake and accelerate on their own in bumper-to-bumper traffic and park automatically.

35 http://www.theregister.co.uk/2015/03/29/british_airways_frequent_flyers_hacked/ (as at 31 August 2015)

36 http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application (as at 31 August 2015)

37 http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (as at 31 August 2015)

38 http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (as at 31 August 2015).

5.3.1 Security in the automotive industry

Cars were electronically contactable even before being connected to the internet via a mobile communications network. Hackers already knew how to take advantage of the introduction of electronic door locks by either copying the signal sent by the key, enabling them to open the door themselves (this risk has since been identified and eliminated by most manufacturers) or blocking the signal so that the door does not receive the lock command in the first place.

In the meantime cars are becoming increasingly like travelling computers: often, a diagnosis laptop is first connected up at the garage to find out from the car itself how it is doing. The car electronics can be fully accessed through this sort of interface – this is not a bug, but a feature. However, interfaces like these could be used as vectors of attack, although they do typically require physical access to the car. In contrast, various systems communicate with each other wirelessly too: for example, tyre pressure sensors can transmit their readings and the mobile phone is connected by *Bluetooth* to the car electronics so that the integrated hands-free system can be used. A mobile connection is also installed in various vehicles so that information can be sent and received via the internet. This is not only for infotainment purposes, but should also enable the manufacturer to locate the vehicle as needed, to unlock the doors by remote access (if the driver has left the key in the car) or to also activate the immobiliser if the car has been reported as stolen. These functions require a connection between the ICT system and the car electronics, which consequently can also be attacked in this way.

It seems only natural that a vehicle's infotainment system is kept completely separate from its operational electronics, which must be safeguarded to the extent that they cannot be manipulated directly by external agents or compromised infotainment devices. However, manufacturers do not necessarily observe this, as recently shown by researchers on various occasions and in different makes of car.

In many cases, the various components are not sufficiently isolated from each other, which leads to risky hacks such as manipulation of the driver assistance system using malware that has been infiltrated beforehand via a CD in the car radio or even over the VHF *Radio Data System (RDS)*.[39] If commands can be given to the driver assistance system, through malware or via a direct wireless connection, it is very possible to make the vehicle accelerate or brake or to steer it. The manipulation of sensor readings can also cause disproportionate reactions of the driver assistance systems.

All wireless communication in a vehicle must be encrypted to prevent it from being read and recorded easily. The various components should also authenticate each other. These measures make it much more difficult to enter malicious commands or false sensor readings. Furthermore, it must be guaranteed that components that communicate via the internet cannot be used as a gateway into the car electronics.

5.3.2 Reboot for Boeing 787 Dreamliner

It would seem that the cure-all remedy for when an office application is not responding as intended also occasionally works for airplanes. A reboot is helpful not just for business or private computers, but even sometimes for the Boeing Dreamliner.[40]

[39] http://www.bbc.com/news/technology-33622298 (as at 31 August 2015).

[40] https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-10066.pdf (as at 31 August 2015).

A lot of software is used in the Dreamliner. During Boeing laboratory testing, checks on the control software of the generators that produce electrical power found that they go into failsafe mode after 248 days due to a counter overflow. This means the airplane would lose all electrical power. The simple solution is a reboot of the Dreamliner's control software.

As a passenger, we can rest at ease as a reboot is performed during every routine maintenance session, which successfully stops the counter from overflowing.

5.3.3 Airplane infotainment systems

The American ICT security researcher, Chris Roberts, claimed he had identified vulnerabilities in the in-flight entertainment (IFE) systems of the aircraft types Boeing 757-200, Boeing 737-800, Boeing 737-900 and Airbus A320 which give access to critical *on-board electronics* systems. On 13 February 2015, he voluntarily informed the US Federal Bureau of Investigation (FBI) of his findings in the hope that the security vulnerabilities would be eliminated. On 15 April, he was arrested by the FBI after alluding to being able to manipulate control of the oxygen masks, and the equipment found in his possession was seized.

The application for a search warrant[41] of 17 April 2015 in the Roberts case reveals that he had been carrying several devices which would enable penetration tests to be conducted in a wide range of network environments. In addition, wiring schematics and other specialised documentation on flight control and information systems were also found in Roberts's possession. Avionics specialists confirmed that the control commands published by Roberts in reports do in actual fact exist. After his arrest at Syracuse airport, an examination of the seat on the plane where Roberts had sat found that attempts had been made to remove the covers of the seat electronic boxes of the two seats in front. Roberts claimed that he had gained access to the IFE system in this way using an Ethernet cable with a modified connector and that he had then used penetration-testing methods to gain access to other on-board systems.

We can assume from this isolated case described by Roberts that he had at least attempted to penetrate the IFE system and other parts of the network. Had the security precautions been inadequate, he would have had the right equipment and the specialist knowledge required to perform such an action. The success of this methodology cannot be completely ruled out. However, it is also possible that he exaggerated the incidents to market himself.

5.3.4 Power failures – cyber background suspected but not confirmed

We only notice how dependent we are on something when it no longer works. Many people in the Netherlands were reminded of this simple truth on 27 March 2015. Traffic lights, public transport and even mobile communications antennas stopped working after a large-scale power failure. Supermarkets had to close because their electronic cash points and also anti-theft systems were no longer working. Lifts had to be evacuated and schools were closed.[42] Flights were cancelled at Schiphol airport. Airplanes could also no longer land and had to be redirected to other airports. Although some suspected a hacker attack, the power cut had actually been caused by overloading at a substation in a suburb of Amsterdam. Past events

[41] http://www.wired.com/wp-content/uploads/2015/05/Chris-Roberts-Application-for-Search-Warrant.pdf (as at 31 August 2015)

[42] http://nos.nl/artikel/2027141-noord-holland-heeft-weer-stroom.html (as at 31 August 2015)

have shown how a fault at a central site of the electric power supply can cause a chain reaction.

Speculation about a hacker attack was fuelled further when, shortly after the event in Amsterdam, a power failure brought extensive parts of Turkey to a standstill on 31 March 2015: the cities of Istanbul, Ankara and Izmir were left without power. In total, 30 of the country's 81 provinces were apparently affected. Other sources claimed that 80 provinces had been hit. Ten hours passed before the energy ministry was able to announce that the power had been restored across the country. Private companies in the cities of Ankara and Istanbul had previously acquired emergency generators and were prepared for this kind of incident. This helped to contain the effects in those locations. However, the power cut had a major impact on public transport, paralysing, for instance, the Marmara underground system. It was not possible to confirm the speculation about a hacker attack in this case either. The power failure was put down to blackouts at several plants and the voltage fluctuations associated with this.

5.3.5 US filling stations open to online attack

A drive along Route 66 certainly calls for regular fuel stops, so the small filling station in every remote village brings hope. But the filling pump is empty. This is indeed a very unpleasant experience. How could something like that happen? Security problems were detected with the automated tank gauges at US filling stations managed by remote access[43]: 3% of the some 150,000 tank gauges accessible online were exposed to the internet without protection and were freely configurable. By changing the settings, it would be possible to manipulate the filling station so that it interpreted that it had sufficient stock even though the pump was actually empty, which would mean that it would not be replenished. The filling pumps could easily be shut down too through specific commands.

Remote access, whenever it is absolutely necessary, must be subject to an adequate security procedure. The following document by MELANI provides various recommendations on this topic:

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

5.4 Attacks (DDoS, defacements)

5.4.1 Black screen at TV5 Monde

Among the numerous attacks carried out during the first six months of 2015, the attack on the French-language television channel TV5 Monde on 8 April undeniably left a deep impression. This was the first time that a television channel had been so severely affected, not only in its online presence, but also through the immobilisation of its production facility, which is an unprecedented incident.

[43] https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges (as at 31 August 2015)

5.4.1.1 Details of the attack

On 8 April 2015, the channel suffered a multifaceted attack that affected several facilities and platforms. The most remarkable aspect was the way in which the broadcasting infrastructure was affected, leaving the channel unable to broadcast after 10pm. Three hours passed before it was able to restore its broadcasting, initially with pre-recorded programmes. In parallel, the channel lost control of its Facebook and Twitter accounts, which were hijacked to broadcast pro-jihad messages. The channel's website was also defaced. According to information available from open sources, the attack was also able to penetrate and disable e-mail communication within the company. The attack was quickly claimed by a group calling itself "Cyber Caliphate" that confirmed its allegiance to Islamic State. However, the exact identity of the perpetrator and of the party that had ordered the attack appeared less clear as events progressed, which is a reminder of how risky the process of attributing an attack is (see below).

5.4.1.2 Vulnerability of the production facility?

Taking control of social media accounts is an incident that has often been observed, particularly as part of attacks intent on circulating a pro-jihad message. However, the ability to affect a large channel's production facility is a new occurrence. Specifically, what was affected was the infrastructure for transmitting programmes to the antenna (encoders and multiplexers). The attack naturally raises questions regarding the exposure of this type of infrastructure. Unless the equipment is accessed physically, for example with an infection to be spread by USB for instance, the attack would imply remote access. Based on information available from open sources, various systems of the TV5 Monde were visible online, thus increasing the scope of attack. Another question that arises with this type of attack concerns the separation of the office automation system from the production system. Details are not known on this point, but some experts assume there were shortcomings at this level. It is true that in some cases, the office automation system is attacked first, which means that the production system can be reached if the two systems are not effectively compartmentalised. Irrespective of the measures that were in place before the attack, the TV5 Monde incident is a reminder of the extent to which industrial control systems need to be protected.

Remote access, whenever it is absolutely necessary, must be subject to an adequate security procedure. The following document by MELANI provides various recommendations on this topic:

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

5.4.1.3 Difficult attribution

Immediately after the attacks, nobody doubted the attribution of the attack to a group belonging to a Islamic nexus operating online. Only the implication of Islamic State was disputed. It was not until June that new findings led the comments on attribution in a different direction. Firstly, it transpired that somebody had already penetrated the network at the start of the year. In this way, they were free to explore and move about laterally to locate systems of interest. This initial information indicates the relatively high level of professionalization of the attackers. However, revelations made by journalists based on the analyses by the security companies Trend Micro and FireEye provide a new clue concerning a link between

the attack and an alleged Russian cyber espionage campaign of state origin by the name of Sofacy (also known as Pawn Storm and APT28). These parallels are based on various indicators found on the TV5 Monde networks and which are part of Sofacy's infrastructure. Although it has apparently been established that Sofacy was present on the TV5 Monde networks, there are still varying interpretations of the link between this campaign and the attack of April 2015 that disrupted the channel's programmes. An initial hypothesis is that the attack was indeed carried out by the group around Sofacy, which tried to have it attributed to Islamic fundamentalism (false flag). The main weakness of this interpretation is that this type of attack does not tally with the methods and objectives of the extremely stealthy espionage campaign Sofacy. Similarly, it appears odd that a perpetrator allegedly linked to the Russian government would be potentially interested in this type of operation, even if there was clearly tension between France and Russia at the diplomatic level at this time.[44] A second hypothesis points to Sofacy having been implemented by pro-jihad groups. However, there is nothing concrete to support this theory, which would need to explain how these groups acquired the software. The third hypothesis, which we find the most plausible, is that of two parallel, but unlinked operations. It is most certainly possible that a Russian perpetrator with government ties would be interested in media groups such as TV5. True to form, however, the aim of the campaign's operator in this case would be to penetrate the network over time in order to obtain sensitive information. In parallel, a cyber operation led by another group whose main objective was to spread a pro-jihad message would then result in the visible damage observed in April.

5.4.1.4 The media: a popular target

In its semi-annual report 1/2014[45], MELANI already highlighted how the media were particularly interesting, and vulnerable, targets for IT attacks. The TV5 attack confirms this trend, which does not concern the print media only. The media are interesting because they process a huge amount of information, some of which is sensitive, but also because they can provide a strong sounding board for groups intent on spreading propaganda or circulating false information. It is also difficult to match certain aspects that are inherent to a media organisation's activity with security requirements that should be particularly stringent. A good example of this is the need to be able to quickly receive, process and publish a piece of information. Furthermore, it can sometimes be difficult to put certain secure communication protocols in place when working with a large number of correspondents, some of whom are independent, mobile and are located in many different places. Finally, it is important to highlight that those interested in these types of targets very often have a lot more resources for their attack than the media have for their defence.

Given the wide range of risks for the media (such as DDoS, espionage and sabotage), it is advisable that they incorporate security procedures that are both preventive and reactive. Media organisations must be able to detect intrusions or other abnormal events and implement emergency measures that are adapted to the various scenarios.

---

[44] The tensions are based on the sale of two French warships Mistral to Russia, and the annulation afterwards.

[45] MELANI semi annual report 2014/1, chapter 5.2: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-1.html (as at 31 August 2015)

5.4.2 Cyberattack: Polish Airlines flights cancelled

While cyberattacks on means of transport such as trains or airplanes attract a lot of interest, they also cause fear. A report of this kind hit the headlines on 21 June 2015 and initially pointed to a major attack: a hacker attack on the computer system of Polish Airlines LOT forced it to cancel several flights because the system affected was no longer able to generate flight plans. Some 1,400 passengers in total were apparently affected. Flight plans contain details about the airports of departure and destination as well as the flight route. These details are used by air traffic controllers to keep airplanes on safe flight routes. If they cannot be sent or printed, then the airplanes cannot take off. No details have been given on who was behind the attack.[46]

The next day, the media spokesperson said the incident had been caused by a network overload, which had resulted from an attack on its capacity, but did not specify if it was a targeted or non-targeted attack. The type and scale of the attack were also unclear. Critical systems that must be connected to the internet should normally be protected from *DDoS attacks* in particular. LOT CEO Sebastian Mikosz explained that this was an industry problem on a much wider scale and that he expected it could happen to anyone at any time.

According to Ruben Santamarta, a security consultant with IOActive, this might be a turning point for the airline industry, which could also appeal to cybercriminals now. Greater interest has in actual fact been detected in recent months in aviation security systems. This is also shown by the attempt to get into the critical aircraft control area via the infotainment system outlined in section 5.3.3.

Recently a greater focus on security topics in the field of transport has been observed. However is this also connected to an interest of cyber criminals? In general, a distinction needs to be made between systems that have to be connected to the internet and systems that are not connected to the internet for security reasons. The first category covers booking systems and any systems containing an exchange between different points. Here, the conventional types of activities such as *DDoS* extortion or theft of user data with subsequent extortion work exactly as they do in any other field. In this regard, we can assume that cybercriminals will also target these systems (just like those in all other sectors) in the future. In the case at hand, it would appear somewhat exaggerated to talk of a turning point in the aviation sector.

5.4.3 Cyberattacks in the wake of Charlie Hebdo

The assassination of the Paris-based editorial staff of Charlie Hebdo in January 2015 also had an impact online, one which is of course in no way comparable with the physical attacks themselves. The figure of 25,000 that has been given for the amount of virtual attacks in the meantime may be impressive, but the quality of these attacks is not. Most of the attacks involved *defacements*, where website security vulnerabilities are exploited to post political or religious slogans on them. Phrases such as "Death to France" or "Death to Charlie Hebdo" were displayed. Most of the attacks were launched by the groups with names like "Middle East Cyber Army", "Fallaga Team" and "Cyber Caliphate". The attacks were more randomly than consciously selected, which is the usual approach in attacks like these. Those affected included schools, universities, churches and companies. In such attacks, the victims are also

[46] http://www.reuters.com/article/2015/06/22/us-poland-lot-cybercrime-idUSKBN0P21DC20150622 (as at 31 August 2015)

not selected in a targeted manner. Very often, vulnerable systems are searched and their security flaws are then exploited. This is precisely the procedure favoured by religious motivated hackers. In a normal situation, the attacks are spread out all over the world, but should an incident occur, the perpetrators join forces and target the one that have caused the rage. The impact of these attacks was also observed in French-speaking Switzerland (see section 4.4.2).

Also a Belgian branch of Anonymous joined this fight and announced a counteraction in which it would pursue all jihadist online activities and block their Twitter, YouTube and Facebook accounts.

5.4.4 Hackers disable US Army websites

In June 2015, the US Army was confronted with an attack on its web infrastructure. The public website www.army.mil was defaced with propaganda and had to be taken down temporarily. Data could not be stolen given that the website did not contain any confidential or personal information. The Syrian Electronic Army claimed the attack on Twitter and had drawn attention on several occasions in the past for its attacks on several media organisations.[47] The purpose of the attack did not appear to be data theft, but disinformation and the posting of political statements. The Pentagon also stressed that it was just a case of cyber-vandalism.

In January, the Twitter and YouTube accounts of the US Army's Central Command (CENTCOM) were hijacked briefly by alleged Islamic State (IS) sympathisers. During the 30-minute defacement, "Cyber Caliphate" was displayed and propaganda images were spread over the Twitter account. This too was a simple attack and the attackers probably used targeted phishing e-mails (known as *spear phishing*) to obtain the access details. Nowadays, YouTube and Twitter offer two-factor authentication methods to make these attacks more difficult. It would seem, however, that these methods had not yet applied to the accounts in question.

5.4.5 Superfish/Lenovo

The computer and laptop manufacturer Lenovo used to supply laptops with a preinstalled software called Superfish by default. According to ICT security service providers, this was a piece of *adware* which integrated third-party advertisement inserts whenever the Google search engine was used.

In February 2015, it was discovered that Superfish installs its own certificate authority (CA) in the Windows certificate store. This enables Superfish to pass itself off as any website (for example Google) and integrate advertisement even with HTTPS-encrypted connections. As the secret key of the CA installed by Superfish is programmed into the software, it can be extracted from Superfish by applying the relevant techniques. This enables hackers to issue certificates for any websites that are then categorised as trustworthy by Lenovo devices.

---

[47] MELANI Semi-annual report 2013/I, chapter 4.4: https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2013-1.html (as at: 31 August 2015)
MELANI Semi-annual report 2013/II, chapter 4.8: https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2013-2.html (as at: 31 August 2015)

Superfish thus makes devices on which it is preinstalled vulnerable to attacks such as man-in-the-middle attacks. It would theoretically be possible in this way for hackers to pass themselves off as banks and thus steal victims' login details (username, password and token) in order to commit e-banking fraud.

Lenovo's official statement on the Superfish issue can be found on its website.[48]

MELANI recommends that Lenovo device users check if Superfish is installed on the device and, if so, to uninstall the software. The following website can be used to check whether the device in use is affected by the Superfish issue.

Superfish, Komodia, PrivDog vulnerability test

https://filippo.io/Badfish/

In addition, Lenovo has provided a tool for removing Superfish (uninstall):

https://support.lenovo.com/us/en/product_security/superfish_uninstall

For computers with a sensible purpose of use, MELANI recommends formatting computers and notebooks before their first-ever start-up and installing the operating system afresh. This can prevent unnecessary, and possibly undesired, preinstalled software (such as adware) from disrupting the device's operation or from passing sensitive information on to third parties without the user's knowledge.

5.4.6 Exploit kits

An *exploit kit* is a tool for attackers to exploit vulnerabilities on terminal devices, either directly in the browser or applications such as Flash, Acrobat Reader or Java.

With exploit kits it is possible for criminal groups to be divided up to a large extent because they are generally designed in such a way that they can be used by people with no ICT expertise. An exploit kit is generally a web-based interface that provides the necessary functionalities, such as the choice of exploits, statistics on infected devices and other configuration options.

The various attacker groups generally have an almost identical modus operandi:

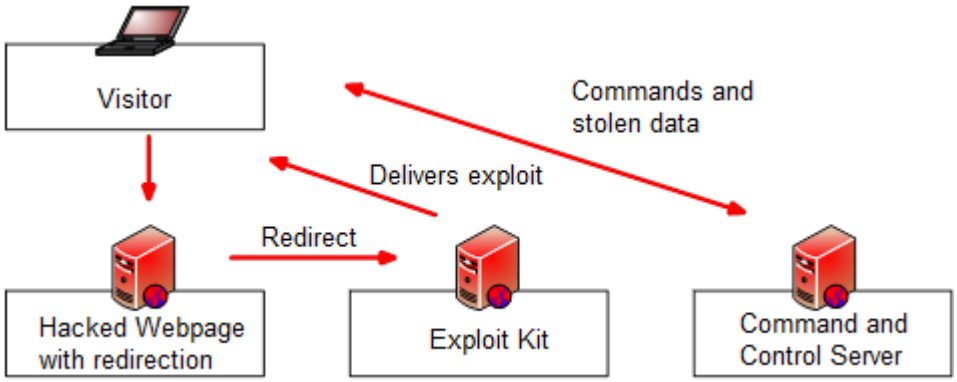


Figure 8: Diagram of how an exploit kit works

[48] http://forums.lenovo.com/t5/Lenovo-P-Y-and-Z-series/Removal-Instructions-for-VisualDiscovery-Superfish-application/ta-p/2029206 (as at 31 August 2015)

Attackers redirect as many potential victims as possible to their exploit kit. There are various ways for them to do this, such as by:

- taking over websites that have a vulnerable CMS and placing a hidden redirection function to the server with the exploit kit. It is therefore essential that all website operators protect their CMS and keep it up to date at all times.[49] [50]
- placing an advertisement that leads the visitors there. This can be achieved by purchasing relevant banners or by taking over vulnerable ad servers.
- purchasing the corresponding traffic from corresponding service providers. This type of system is called a *traffic distribution system (TDS)*. Not all operators of these kinds of systems are criminals: visitor flows are often directed in a legal context too.

The exploit kit often checks the target device itself using *JavaScript* on the installed plugins and their versions in order to find the most suitable vulnerability and attack using an exploit. There are a large number of exploit kits that have various abilities. The best-known exploit kits are Angler, Neutrino, Rig, Nuclear and Magnitude. It is interesting to observe just how quickly exploit kits find suitable exploits when new vulnerabilities appear. Not all exploit kits have the same exploits and there is a relatively large degree of variation.[51] Furthermore, it is increasingly common to find exploit kits with *0-day exploits*.[52]

Exploit kits are not only used by everyday criminal attackers, however; they are also employed by some government attackers as part of espionage activities.

5.4.7 Logjam and FREAK vulnerabilities

During the period under review, two major vulnerabilities were discovered that could threaten the security of encrypted connections: FREAK and Logjam. The background to both of these vulnerabilities lay in the fact that there had previously been export restrictions on cryptographic products in the USA. In the source code of some cryptography libraries the *fallback functions* needed for these are still available and can be exploited for this type of attack.

FREAK (Factoring Attack on RSA-EXPORT Keys) allows weak keys that are possible to decrypt to be accepted on certain browsers. However, this requires a vulnerable browser to connect to a server with weak ciphers. A large number of browsers and client programs were affected by this.[53]

Logjam is a FREAK-related attack on encrypted connections where the encryption strength of the connection can be downgraded to the point that the connection can be deciphered. In this process, the prime numbers used in the *Diffie Hellman* key exchange are reduced in such a way that decryption is possible.[54]

---

[49] See also the MELANI checklists: Security Measures for Content Management Systems (CMS): https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-to-secure-content-management-systems--cms-.html

[50] See also chapter 2 of the current semi-annual report.

[51] http://contagiodump.blogspot.ch/2010/06/overview-of-exploit-packs-update.html (as at 31 August 2015)

[52] http://malware.dontneedcoffee.com/ (as at 31 August 2015)

[53] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204 (as at 31 August 2015)

[54] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000 (as at 31 August 2015)

5.5 Preventive measures

5.5.1 New patch management from Microsoft

Just as the introduction of regular patch management for the operating systems of mobile phones is being discussed, Microsoft intends for Windows 10 users to eliminate the traditional patch day and introduce continuous updates. A patch day was introduced primarily due to the requirements of administrators in large companies so that they could better plan and test the installation of updates and thus avoid the situation of critical systems suddenly no longer working after the update has been installed.

For companies Microsoft wants to solve these problems under the label “Windows Update for Business” using what it calls distribution rings. In this process, a network is divided up into different rings. Depending on the ring, some systems receive the update earlier than the others. The updates are not distributed to the other computers until later. This method also enables the risk-based installation of updates. Computers with a higher risk of infection receive the update sooner while the others receive it later. In addition, administrators can set maintenance windows for when updates should and should not be installed. Nevertheless, Microsoft wants to maintain patch day initially for systems that companies declare as critic.[55]

5.6 Other topics

5.6.1 Simple theft with serious consequences

The *smartphone* is now an essential part of modern society: we use it to listen to music, read e-mails, manage appointments or measure our sports performance. We entrust almost all of our details to our smartphones. Clearly, the smartphone has become an interesting target for all types of criminals. What first springs to mind for electronic devices are electronic methods of attack, such as data theft via malware or attempts at extortion via *ransomware*. In June 2015, news stories circulated in the German media that reminded us not to underestimate even conventional extortion methods. In Germany, there has been an increase in the number of smartphone and laptop thefts with the aim of blackmailing managers and business people. The theft of such a device is becoming less appealing in principle because of falling smartphone prices and security precautions that are difficult to circumvent. However, if a device contains information that is very valuable to a particular person or their company or clients, then theft of this kind is worthwhile from a financial viewpoint.

A story about this sort of theft hit the headlines, and the victim was none other than Dieter Kempf, a leading figure from the IT world. As director of the service provider Datev and chairman of the German Federal IT Association (BITKOM), he was on his way to the 14th German IT Security Conference where he was due to moderate round table talks on the issue of "Secure mobile communications". Just as was getting off the train, three people approached him and snatched his laptop and BlackBerry. The description of how the crime took place matches other victims' stories: the thieves acted in a small group, mostly during peak times, in trains or stations and they stole from people whom they suspected were business people.

[55] http://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/ (as at 31 August 2015).

These incidents do not involve cybercriminals who obtain physical access to information, but rather everyday pickpockets who have realised that this line of business can be quite lucrative. It should not result in a wave of attacks, however, because the thieves must operate on the ground and take great risks in their physical contact with victims. Nevertheless, the example shows that ICT-devices confidential information is exposed to many dangers.

The following measures help to counter this type of extortion:

- Ensure that the security precautions on your smartphone are correctly activated (e.g. PIN entry and automatic screen lock).
- Do not save confidential business information on your private devices.
- Never leave devices that contain confidential information unattended.
- Save your data regularly (Backup / Cloud Sync) so that in case of a lost at least the data is still available.
- Anti-Theft-protection (for example “Find my iPhone”)
- Theft insurance for devices and data.

6 Trends and outlook

6.1 When data affects the lives of others

The problem of collecting personal data and the associated exploitation chain has already been discussed in the last semi-annual report.[56] Often in this regard, the possible abuses by companies and individuals are portrayed as the main problem. But what is barely addressed is how individuals can proceed when government bodies and regulating authorities make mistakes, as described in the incident below. There are no recommendations as to what those concerned can do to reverse the misinformation and above all how this can be prevented.

It becomes problematic, for example, if people with the same names and identical dates of birth live in Switzerland. A few stumbling blocks arise for these people which tie in with the resulting risk of confusion. The *Beobachter*, a Swiss consumer magazine, did a report entitled "Confusion – the two Mosers" about a specific case. While the incidents clearly show how each case of confusion can be resolved, the persons concerned still have to repeatedly demand these corrections through no fault of their own. The people mentioned in this case, Peter Moser from Ipsach and Peter Moser from Winterthur, were born on exactly the same day and have been muddled up by the AHV (the contributions for old-age and survivors' insurance) and other companies and authorities, and this happens time and again.[57]

MELANI was informed about a similar case in the last six months. This case concerned two Swiss citizens with the same first name and surname as well as the exact same date of birth. The person who reported this to MELANI, and will henceforth be referred to as the notifying party[58], only has a different second name. The series of mix-ups started with an entry in the criminal records which the notifying party received but was actually intended for the other person. It is very unpleasant to have to defend yourself against a criminal order which has nothing to do with you. Other mix-ups occurred with health insurers, tax authorities and communal administrations after changes of residence. Even the ombudsman service which was alerted to the problem mixed up the notifying party with the other person when sending the reply. In each case, the burden of proof is on the victim, in spite of the error being made by the company or authority each time. In other cases, the notifying party was able to actively intervene with the corresponding bodies and was only just able to prevent any mix-ups which would have led to entry bans in certain countries and wrongly assigned biometric data in the passport office. Once again, the system would have failed without the influence of the innocent victim.

From the perspective of the person concerned, the main problem is that the events described above are always attributable to the same cause, i.e. confusion relating to identity. However, as the affected party, one has to contact the body responsible for the sector, administrative unit, etc. in each individual case. The affected party has to go to enormous trouble through no fault of their own and are only compensated in very rare cases. Time and again one has to eliminate each problem individually. There is no central contact point which is responsible

---

[56] MELANI Semi-annual report 2014/II, chapter 5.1: https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2014-2.html (as at 31 August 2015)

[57] http://www.beobachter.ch/justiz-behoerde/buerger-verwaltung/artikel/verwechslung_der-doppelte-moser/ (as at 31 August 2015)

[58] The name is known to the Reporting and Analysis Centre for Information Assurance

in a cross-sectoral manner for all institutions concerned for the false identification and which could assume coordination for those affected. In addition, due to the fast propagation of inaccurate information, very often not all systems are updated after the correction has been made, which once again involves a great deal of trouble for those involved.

In view of upcoming agreements such as on the automatic exchange of information (AEOI), problems resulting from mixing up identities could quickly spread to the international level, which could increasingly exacerbate the problem of rectifying mistakes. When elaborating new agreements and laws, the focus should not just be placed on preventing abuse of the system by individuals, but should also include quality assurance of the system. In addition a simple method for correcting mistakes must be

6.2 Life and death – ICT in the healthcare system

Infusion pumps are practical aids in everyday medical treatment. The right dosage of the respective medication is automatically prepared for the corresponding symptoms. It is very unpleasant to think that the contents of the infusion tube which flow into the body could be controlled by outsiders.

In the last semi-annual report, we examined the problem of the complete connectivity of more and more appliances in the context of the *internet of things*. This trend also affects medical appliances. When they are interconnected, however, the reality is a whole range of associated risks. For instance, the security researcher Billy Rios found vulnerabilities in infusion pumps of the Hospira brand.[59] In the first attempt, he was only able to manipulate the limits whereby the responsible caregiver received a warning message. In further experiments, however, he was able to manipulate the prescribed dose remotely. The researcher informed the manufacturer and the relevant US regulatory authority, the US Food and Drug Administration (FDA), of this at the start of June 2015. It took until the end of July until the FDA finally issued an official warning.[60] Theoretically, this was enough time to test the research results in practice and to test the vulnerability. Yet another problem becomes apparent from the content of the warning: although the FDA recommends disconnecting the infusion pumps from the network, at the same time it warns that the dose databases must be manually kept up to date. This once again opens up new sources of errors. In many sectors, one quickly gets used to practical ICT-supported functionalities. It is absolutely essential to ensure that automated processes are as secure as possible, and fallback arrangements in the event of problems must be defined.

As a result of the internet-of-things trend, more and more new components and processes are automated and networked with each other. Alongside the new possibilities and optimisations which these applications provide for users, however, new problems also emerge for those parties who have a liability. As the example of the Boeing Dreamliner described in chapter 5.3.2 shows, a functioning workaround is used as a corrective measure in preference to changing the authorised configuration with a targeted patch, as this would involve system recertification.

But it is not only users who are confronted with new problems; the regulators of the sectors affected have to increasingly deal with ICT issues. In the case of medical devices, Council

[59] http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/ (as at: 31 August 2015)

[60] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm (as at: 31 August 2015)

Directive 93/42/EEC applies to the authorisation of the device in the EU and also in Switzerland. In the entire 65 pages, the term software only occurs in connection with ICT in one specific passage: "For devices which incorporate software or which are medical software in themselves, the software must be validated according to the state of the art taking into account the principles of development lifecycle, risk management, validation and verification".

The state of the art is established in norm EN62304: a methodical, comprehensive standard from 2006 on the software lifecycle of medical devices. If a vulnerability emerges, the problem very often not only involves the product concerned, but also the insufficient configuration of the surrounding networks.

Insurance companies are already dealing with new risks in depth. The new dangers obviously represent potential new lines of business for them. Whoever does not manage the risks resulting from this smart interconnectedness can at least insure themselves against the possible financial losses elsewhere.

7 Politics, research, policy

7.1 Parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Ip	15.3656	Risk for the Mühleberg nuclear power station posed by remote maintenance of the computer system. Questionable monitoring by the Swiss Federal Nuclear Safety Inspectorate (ENSI)	Martina Munz	18.06.2015	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153656
Po	15.3359	For innovative Armed Forces	Fathi Derder	20.03.2015	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153359
Po	15.3769	Report on public services. Restricting the internet presence of the Swiss Broadcasting Corporation (SRG) to audio/video library	Marco Romano	19.06.2015	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153769
Ip	15.3723	Implementation of the expert recommendations on the protection of children and minors in the media	Barbara Schmid-Federer	19.06.2015	NC	FDHA	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153723
Ip	15.3661	Violation of the SRG licence. Suppression of illegal internet series	Rutz Gregor A.	18.06.2015	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153661
Ip	15.3657	The right to be forgotten for internet users	Martina Munz	18.06.2015	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153657
Po	15.3618	Report on the public services mandate of the SRG. Analysis according to the subsidiarity principle	Christian Wasserfallen	18.06.2015	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153618
Ip	15.3615	Public services in the media sector	Edith Graf-Litscher	18.06.2015	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153615
Po	15.3407	Right to personal privacy	Yvonne Feri	05.05.2015	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153407
Mo	15.3358	Boosting the investment programme for the information society	Fathi Derder	20.03.2015	NC	EAER	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153358
Ip	15.3352	How much tax do the big internet groups pay in Switzerland?	Margret Kiener Nellen	20.03.2015	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153352
Po	15.3307	Society and the internet in Switzerland in 2030. Report	Edith Graf-Litscher	20.03.2015	NC	EAER	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_i

							d=20153307
Ip	15.3291	Exportation of surveillance and intelligence technology. What about human rights?	Pierre-Alain Fridez	19.03.2015	NC	EAER	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153291
A	15.1027	What precautions does the Federal Council want to take to prevent violent extremism in Switzerland?	Christian van Singer	20.03.2015	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20151027
Po	15.3759	Secure data network and other IT projects to do with civil protection. Status, perspectives and resource requirements	Ida Glanzmann-Hunkeler	19.06.2015	NC	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153759
Ip	15.3692	IT in the Federal Administration. A bottomless pit?	Sylvia Flückiger-Bäni	18.06.2015	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153692
Ip	15.3137	Outsourcing the processing of tax data	Philipp Hadorn	16.03.2015	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153137
Ip	15.3448	Provision of support for the introduction of autonomous vehicles?	Fathi Derder	06.05.2015	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153448
Ip	15.3375	Theft of SIM codes from the Gemalto company by the NSA and GCHQ security services	Luc Recordon	20.03.2015	CS	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153375

7.2 Other topics

7.2.1 National research programme on big data

At the end of June 2015, the Federal Council launched a new National Research Programme (NRP) on *big data*. The budget for the big data NRP amounts to CHF 25 million and proposes laying the groundwork for an effective and appropriate use of the ever-increasing volume of data (big data) in all spheres of society. The programme will have a research period of five years. The funded research projects should provide the scientific basis for new solutions in the field of computing (data analysis, algorithms, *cryptology*, data management services, security and access controls), making it possible to work with large volumes of data effectively and securely. Building on this, the intention is to critically examine social (healthcare and public infrastructure) and economic areas of application, in which large volumes of data are already a reality today and will become even more so in the future, in particular from the point of view of data and system security and with regard to regulation (data protection, privacy).

The Steering Committee of the Swiss National Science Foundation project on big data was formed in summer 2015. The calls for applications for the individual projects and the conditions of participation for research groups should be published in the course of autumn 2015. Scientific project outlines should then be submitted within three months, and a definitive selection of the research projects is expected in the course of next year.

7.2.2 Reorganisation of domain allocation

The Ordinance on Internet Domains (OID), which came into force on 1 January 2015, resulted in an extensive reorganisation of domain allocation in Switzerland. Up to now, SWITCH had not only held the position of a register operator (management of the domain name database or registry) but also that of registrar (marketing of domain names). This dual role is now no longer possible because of the new ordinance. The OID defines the role of the network information centre, i.e. the organisation which centrally manages the resources for operating a country's domain name system, being assigned to OFCOM or a third-party office appointed by OFCOM (Article 8 of the OID). In order to offer *top-level domains* (ccTLD or gTLD) on the market in Switzerland, a registrar contract with *ICANN* and the register operator is required. In the meantime, 79 registrars from all over the world have been authorised for the ".ch" TLD, 46 of which are companies from Switzerland. The transfer of the .ch domain names from SWITCH to the registrars has been in progress for some time now. On the other hand, the Administration (OFCOM) is exclusively responsible for gTLD .swiss in accordance with the OID to secure the particular long-term use for Switzerland.

To ensure an orderly and transparent migration process and to prepare the allocation of the registration body, OFCOM has extended the delegation to SWITCH within the meaning of temporary regulations under Article 62 of the OID up to mid-2017. At this time the registry-function will be contracted out again.

8 Published MELANI products

In addition to the semi-annual reports for the general public, MELANI also offers a number of diverse products. The following sections provide an overview of the blogs, newsletters, checklists, instructions and fact sheets published during the reporting period.

8.1 GovCERT.ch blog

8.1.1 Joining the DNSSEC Day in Germany

30.06.2015 - DNSSEC stands for Domain Name System Security Extensions and has been introduced in 1999. The goal of DNSSEC is to implement authenticity and integrity in the DNS by taking advantage of digitally signing DNS records using public-key cryptography. DNSSEC helps you to prevent man-in-the-middle attacks on the DNS layer and DNS cache poisoning. Besides that, DNSSEC also provides a secure ground that allows you making usage of further security mechanisms that rely on DNSSEC, such as DNS-based Authentication of Named Entities (DANE).

➔ http://www.govcert.admin.ch/blog/9/joining-the-dnssec-day-in-germany

8.1.2 Outdate WordPress: Thousands of websites in Switzerland are vulnerable

08.06.2015 - The internet has grown very fast in the past 15 years. Thousands of new websites are going online every day. According to Netcraft, there are currently more than 850'000'000 active websites in the internet (May 2015). One of the reasons why the number of websites has grown that much is the use of content management systems (CMS), for example WordPress, Typo3, Joomla and Durpal. By using a CMS, you can easily publish content in the internet without needing IT knowledge. While CMS are something great, they are also a valuable target for hackers.

➔ http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable

8.1.3 Increase in DDoS extortion (DD4BC)

08.05.2015 - In the past days MELANI / GovCERT.ch has received several requests regarding a Distributed Denial of Service (DDoS) extortion campaign related to 'DD4BC'. The DD4BC Team (that is how the attackers call themselves) started its DDoS extortion campaigns in 2014. Since earlier this week, the DD4BC Team expanded their operation to Switzerland. MELANI / GovCERT.ch is aware of several high profile targets in Switzerland that have recently received a blackmail from DD4BC and have consequently suffered from DDoS attacks, obviously conducted by DD4BC.

➔ http://www.govcert.admin.ch/blog/6/increase-in-ddos-extortion-dd4bc

8.1.4 e-Banking Trojan Retefe still spreading in Switzerland

01.05.2015 - In July 2014, Trend Micro published a report about a threat called Retefe, an ebanking Trojan that is targeting financial institutions in Switzerland, Austria, Sweden and

Japan. In fact, Retefe is already around since November 2013. Back then, MELANI already took appropriate action together with the affected financial institutions and ISPs in Switzerland to mitigate the threat. However, Retefe is still being distributed in recent spam campaigns, targeting Swiss Internet users.

➔ http://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

8.1.5 Critical vulnerability in Magento: Many Swiss websites are still vulnerable

30.04.2015 - In February 2015, Magento (a popular eCommerce software for webshops) released a security patch addressing a critical vulnerability in its product. The vulnerability allows an attacker to send a special prepared HTTP request to any website running a vulnerable version of Magento in order to execute malicious code on the remote webserver (a so called Remote Code Execution RCE vulnerability). More than two months later, MELANI / GovCERT.ch still sees a fairly big amount of websites in Switzerland running an old, vulnerable version of Magento, exposing themselves and its visitors to cyber-attacks from the internet. Hackers can (ab)use the vulnerability to e.g. place malicious code on the victims website to infect its visitors with malware (Drive-By exploits).

➔

http://www.govcert.admin.ch/blog/4/critical-vulnerability-in-magento-many-swiss-websites-are-still-vulnerable

8.2 MELANI newsletter

MELANI published the following newsletter in the first half of 2015:

8.2.1 Meldeportal gegen Phishing (only available in german, french and italian)

29.07.2015 - In den vergangenen Jahren ist die Zahl der durch die Melde- und Analysestelle Informationssicherung MELANI bearbeiteten Anfragen bezüglich Phishing stark angestiegen. Bei den meisten Anfragen wurden uns Phishing E-Mails und Phishing-Webseiten gemeldet, welche Kunden von Finanzinstituten in der Schweiz, aber auch international bekannte Internet-Plattformen (wie z. B. Social Networks, E-Mail Dienste oder Online Payment Service Provider) im Visier haben. Um die Vielzahl der eingehenden Meldungen betreffend Phishing effizienter bearbeiten zu können, hat die Melde- und Analysestelle Informationssicherung MELANI eine Website aufgeschaltet, auf welcher vermeintliche Phishing Seiten gemeldet werden können.

➔

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/meldeportal_gegen_phishing.html

8.2.2 DDoS Angriffe und Erpressung : eine äusserst aktuelle Kombination (only available in german, french and italian)

20.05.2015 - Verschiedene Fälle, welche MELANI in den letzten Wochen gemeldet wurden, deuten auf eine Zunahme von DDoS-Angriffen hin, welche vor allem den Zweck haben, von

den Opfern Geld zu erpressen. MELANI empfiehlt, nicht auf die Erpressung einzugehen und publiziert eine Anleitung mit verschiedenen Schutzmassnahmen vor DDoS-Angriffen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/ddos_angriffe_und_erpressung.html

8.2.3 E-Banking Trojaner «Dyre»: Lawinenartige Verbreitung (only available in german, french and italian)

07.05.2015 - Im Februar 2015 hat die Melde- und Analysestelle Informationssicherung MELANI vor dem E-Banking Trojaner «Dyre» gewarnt, welcher Schweizer KMU im Visier hat. In den vergangenen Wochen wurden MELANI täglich mehrere hundert Neuinfektionen in der Schweiz gemeldet. Mittlerweile sind nicht mehr nur KMU betroffen, sondern vermehrt auch Privatanwender.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/information_dyre_2.html

8.2.4 10 Jahre MELANI: Ein Blick zurück und auf die aktuellen Bedrohungen in der Cyberwelt im 20. Halbjahresbericht (only available in german, french and italian)

30.04.2015 - Die Melde- und Analysestelle Informationssicherung MELANI feiert ihr zehnjähriges Bestehen. Der 20. Halbjahresbericht legt deshalb nicht nur den Fokus auf die wichtigsten Ereignisse im zweiten Halbjahr 2014, welches vor allem durch Erpressungen sowie Angriffe auf schlecht geschützte Systeme geprägt war. Der Bericht, welcher heute publiziert wurde, wirft auch einen Blick auf die Entwicklung der Internetkriminalität während des letzten Jahrzehnts.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/20_melani_halbjahresbericht.html

8.2.5 Kunden von Schweizer KMUs: Ziel von massgeschneiderten Phishing-Angriffen (only available in german, french and italian)

31.03.2015 - Nach wie vor versuchen Betrüger an sensible Daten wie Passwörter, Kreditkartendaten usw. zu gelangen. Zu diesem Zweck werden meist Webseiten kreiert, welche derjenigen einer Firma täuschend ähnlich sehen (beispielsweise werden gerne Internetauftritte von Banken oder Kreditkarteninstituten missbraucht). MELANI interveniert täglich, um solche betrügerische Webseiten vom Netz zu nehmen und so die Internetnutzer zu schützen.
Schon seit einiger Zeit missbrauchen die Betrüger allerdings nicht mehr ausschliesslich nur die Namen von grossen und bekannten Unternehmen, sondern verüben auch sehr gezielte Phishing-Angriffe mit dem Namen kleinerer Firmen. Diese Tendenz scheint sich zu akzentuieren: verschiedene Fälle, welche MELANI kürzlich zur Kenntnis gebracht wurden, zeugen von einer zunehmenden Professionalität dieser Angriffe. Betroffen sind KMU in den verschiedensten Tätigkeitsbereichen, welche eine Website betreiben, die in irgendeiner Weise Kunden-E-Mail-Adressen verwenden respektive gespeichert haben, beispielsweise für den Versand eines Newsletters.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/kunden-von-schweizer-kmus--ziel-von-massgeschneiderten-phishing-.html

8.2.6 E-Banking Trojaner hat Schweizer KMU im Visier (only available in german, french and italian)

02.02.2015 - In den vergangenen Tagen gingen bei der Melde- und Analysestelle Informationssicherung MELANI vermehrt Meldungen von Schweizer KMU ein, welche verdächtige Spam E-Mails erhalten haben. Die gemeldeten E-Mails stammen dabei offensichtlich von angeblichen Geschäftspartnern und versuchen, den Empfänger der E-Mail mit einem e-Banking Trojaner zu infizieren. Bei einem kürzlich bekannt gewordenen Fall, welcher ein Freiburger Unternehmen betraf, wurde mittels demselben Trojaner ein siebenstelliger Betrag gestohlen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking-trojaner-hat-schweizer-kmus-im-visier.html

8.3 Checklists and instructions

MELANI published the following checklists and instructions in the first half of 2015:

8.3.1 Measures to counter DDoS attacks

2015.06.25 - A DDoS (distributed denial of service) is a type of attack on computer systems with the deliberate aim of making them unavailable. This can have far-reaching economic consequences for the victim.

The motivation behind such DDoS attacks is mostly political activism, extortion or damaging competitors. MELANI is currently observing a rise in extortion DDoS attacks demanding payment of a ransom in the form of cryptocurrencies such as bitcoin or litecoin.

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

8.3.2 Merkblatt IKT-Sicherheit für KMU (only available in german, french and italian)

2015.01.30 - Dieses Merkblatt richtet sich an Schweizer KMU und soll diesen dabei helfen die IT-Sicherheit im Unternehmensnetzwerk zu erhöhen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

9 Glossary

Term	Definition
0-day Exploit	A vulnerability that is unpatched by the vendor.
Adware	A contraction of the words “advertisement” and “software”. Adware is often used for targeted advertising purposes, by recording the user’s surfing habits and offering the corresponding products (e.g. through links).
Big data	Big data refers to data amounts which are too large or too complex to analyse using manual and conventional data processing methods.
Bitcoin	Bitcoin is a globally available, decentralised payment system and is the name of a digital monetary unit.
Bluetooth	A technology for wireless communication between two terminals and which is mainly used in mobile phones, laptops, PDAs and input devices (e.g. computer mouse).
Certificate	A digital certificate is the cyberspace equivalent of a personal identification card and serves to assign a specific public key to a person or organisation. This assignment is certified by the certificate authority with its own digital signature.
Ciphers	A cipher (encryption procedure) is used to convert plain text into ciphertext and, conversely, to convert the ciphertext back into plain text.
Command and 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 (XSS)	Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject (malicieous) client-side script into web pages viewed by other users

Cryptography	Cryptography is the science of encrypting information.
Defacement	Unauthorized alteration of websites.
Diffie-Hellman key-exchange	With the Diffie-Hellman key-exchange, two communication partners can generate a secret key that only they know.
Distributed Denial of Service (DDoS)	A DDoS attack has the goal of causing a loss of a specific service to users or at least to considerably restrict the accessibility of the service. The victim is simultaneously attacked by many different systems.
Drive-by Infection	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.
Ethernet	Ethernet is a technology that specifies software and hardware for cable data networks.
Exploit Kit	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Fallback function	A fallback function represents a second system which prevents a total breakdown in the event of failure of the first system.
FTP	File Transfer Protocol FTP is a network protocol for transferring data via TCP/IP networks. FTP can be used, for instance, to load websites onto a webserver.
Geolocation	Identification of geographic location
Global Positioning System (GPS)	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
Hacktivism	Hacktivism describes the breaking into a computer system for a politically or socially motivated purpose.
Honeypot	In the field of computer security, a honeypot is a computer programme or server that simulates the network services of a computer, an entire computer network, or the behaviour of a user. Honeypots are employed to obtain information on attack patterns and attacker behaviour.

ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) ICANN is a non-profit organisation under private law with headquarters in the small Californian town of Marina del Rey. ICANN decides on the foundations for administering top-level domains. In this way, ICANN coordinates technical aspects of the Internet without, however, using binding law. ICANN is subject to the US Department of Commerce and thus the US government.
Industrial control systems (ICSs)	Control systems consist of one or more devices that control, regulate, and/or monitor the behaviour of other devices or systems. In industrial production, the term "industrial control system" (ICS) is often used.
Industry 4.0	Industry 4.0 or the fourth industrial revolution, is a collective term embracing a number of contemporary automation, integral interconnectedness and data exchange. Industry 4.0 facilitates the vision and execution of a "Smart Factory".
Internet of things (IoT)	The term "internet of things" refers to the increasing computerisation and connectivity of (everyday-) objects.
IP-address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
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.
Malware	Comes from the terms "malicious" and "software". Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses.
On-board electronics	Electronics which are to be found in a moving object and help support the control of this object.
One Time Password	A one-time password is a password for authentication or authorisation. It is only valid for a single transaction and cannot be used a second time.

Patch day	Patch day refers to a day on which a vendor releases security patches for its software products.
Patch management	Patch management means the way in which the distribution and installation of software updates is organised.
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 and company logos.
Plug-In, Plugin	(Additional) software that extends the basic functions of an application, e.g. Acrobat plug-ins for internet browsers allow direct display of PDF documents.
QR code	A QR code is a method of writing information so that it can be very quickly found and read by a machine.
Radio Data System (RDS)	Radio Data System allows additional information to be transmitted by radio.
Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
RSA-encryption	Short for Rivest-Shamir-Adleman encryption. A public-key encryption algorithm introduced in 1978. RSA is an asymmetric algorithm.
SCADA-Systems	Supervisory Control And Data Acquisition Systeme. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
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
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
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.

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.
SSL/TLS Tunnel	In a network, a tunnel or tunnelling refers to the conversion and transmission of a communication protocol that is embedded in a different communication protocol for the purpose of transport. SSL and TLS Protocols provide encrypted communication on the internet.
Top Level Domains	Every name of a domain on the Internet consists of a sequence of character strings separated by periods. The term "top level domain" refers to the last name in this sequence, constituting the highest level of the name resolution. If the full domain name of a computer or website is de.example.com, for instance, the right-most member of the sequence (com) is the top level domain of this name.
Traffic distribution system (TDS)	Traffic distribution systems (TDS) are systems which direct internet traffic to the actual target site when accessing online advertisements. These are often used to deliver malware.
Web application firewall	A web application firewall (WAF) is a procedure to protect web applications from attacks via the Hypertext Transfer Protocol.