Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

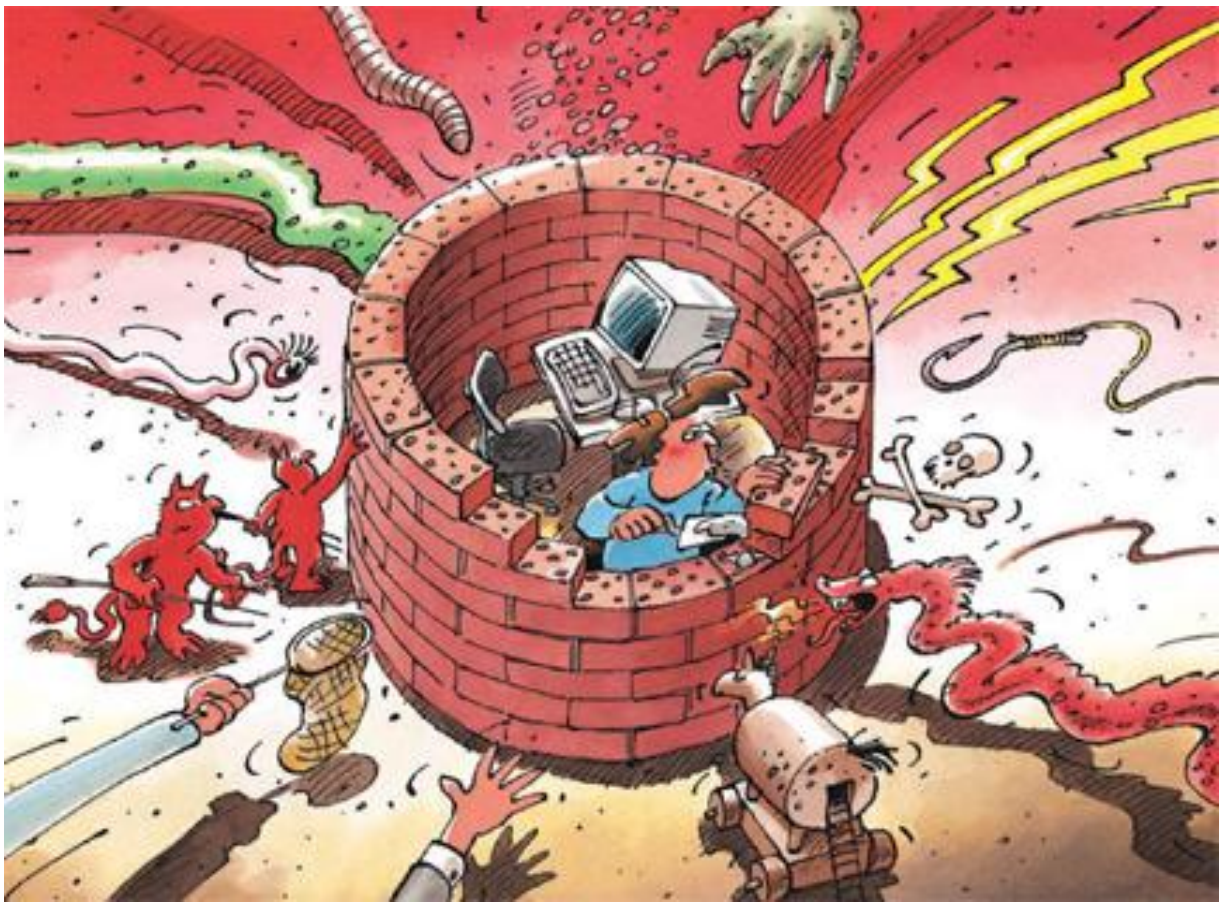
Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

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

Information Assurance

Situation in Switzerland and internationally

Semi-annual report 2014/II (July-December)



Contents

1 Focus areas of issue 2014/II

- **Ten years of MELANI**

  The Reporting and Analysis Centre for Information Assurance (MELANI) celebrated its tenth anniversary on 1 October 2014; ten years which have seen tremendous development in information and communication technologies (ICT). The growing number of platforms, services and internet users has also had an impact on criminal structures. In this time, a veritable cyber black market has developed where everything needed for an attack can be obtained. However, some countries have also greatly expanded and honed their espionage and surveillance methods. You can find facts and thoughts on the development of the internet over the last ten years in Chapter 3.1.

  ► Current situation nationally: Chapter 3.1

- **More security vulnerabilities in encryption**

  Already a victim of Heartbleed in the past, *SSL* was once again affected by a serious vulnerability. Unlike Heartbleed, however, the bug known as Poodle is not a programming flaw, but a design one. Therefore, the only way to remedy the vulnerability was to disable an old encryption standard. Various other security vulnerabilities have also been discovered, some of which are considerable. In 2014, a total of 7,945 vulnerabilities worldwide were recorded in the database of all publicly known program vulnerabilities maintained by the MITRE Corporation, which is the highest number ever. Given this high figure, the question increasingly having to be asked concerns the processes to be followed when security vulnerabilities are detected.

  ► Current situation internationally: Chapter 4.9, Chapter 4.10, Chapter 4.11
  ► Trends/Outlook: Chapter 5.5

- **Poorly protected systems – not just a risk for operators**

  Open webcams, poorly protected wireless networks and not up-to-date *content management systems (CMS)* are popular targets for attacks. Initially, it would seem that the attacks involve damages only for the operator, but often they have other repercussions. Compromised websites can be used for *phishing* or spreading *malware* and compromised e-mail accounts for sending spam. Meanwhile, Switzerland had the third-highest number of spam senders based on population size.

  ► Current situation in Switzerland: Chapter 3.2, Chapter 3.4, Chapter 3.5

- **Espionage – at work, on the move and when communicating**

  There is permanent interest in and accordingly constant pressure on sensitive data. The examples included in the report show that espionage attempts can occur anytime and anywhere, whether in the workplace, on business trips or when making or taking calls on a mobile phone.

  ► Current situation internationally: Chapter 4.5, Chapter 4.6, Chapter 4.10

- **Complete connectivity – smart and safe?**

  Nowadays, telephones are not the only things to have gone "smart": we also have smart cars/smart drive, smart homes and smart buildings, and even smart factories/smart manufacturing that can collect, receive, process and send data, redirect commands given by you and perform physical actions. The risks associated with this are discussed in Chapter 5.2.

  ► Trends/Outlook: Chapter 5.2

2 Introduction

The twentieth semi-annual report (July-December 2014) of the Reporting and Analysis Centre for Information Assurance (MELANI) presents the most significant trends involving the threats and risks arising from information and communication technologies (ICT). It provides an overview of events in Switzerland and abroad, sheds light on topics in the area of prevention, and summarises the activities of public and private players. Explanations of jargon and technical terms (*in italics*) can be found in a **glossary** (**Chapter 6**) at the end of this report. Comments by MELANI are indicated in a shaded box.

Chapter 1 gives a brief outline of selected topics covered in this semi-annual report.

Chapters 3 and 4 discuss breakdowns and failures, attacks, crime and terrorism connected with ICT infrastructures. Selected examples are used to illustrate important events of the second half of 2014. Chapter 3 discusses national topics; Chapter 4 international topics.

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

Chapter 5.6 contains selected parliamentary business items relating to information assurance.

On the occasion of the tenth anniversary of the Reporting and Analysis Centre for Information Assurance, this issue comes with an additional table with the most important events concerning the internet and information assurance over the last ten years.

3 Current national ICT infrastructure situation

3.1 Ten years of MELANI – a review

The Reporting and Analysis Centre for Information Assurance (MELANI) celebrated its tenth anniversary on 1 October 2014. Over the course of those ten years, there has been tremendous development in information and communication technologies (ICT). During this time, new platforms, *protocols* and communication devices have emerged. We only need to think of the development in the area of *social media* or the meteoric evolution of *smartphones*. It is worth remembering that Facebook was only eight months old and still in its infancy when MELANI was founded. The short message service Twitter was not created until 2006, and the first iPhone hit the market one year later. The number of internet users has also risen sharply: there were 900 million internet users in 2004 and three billion in 2014.[1]

Naturally, this technological and social development also brings with it criminals and other hostile players who have not missed their chance to reap the benefits of these new possibilities. The number of new, inexperienced internet users also generated new groups of victims. New services and applications produced further opportunities to find vulnerabilities and exploit them too. For example, the use of standardised *content management system* software, which is often not regularly updated, produced numerous new points of attack.[2]

- *Botnets*
  Apart from the practically unlimited (attack) possibilities that a large botnet offers its owners, the involvement of thousands of home computers and the resulting unknowing complicity of their owners poses prosecutors, intelligence services, and IT specialists with a nearly unsolvable problem. In this light, a paradigm shift is to be expected, affecting the execution of attacks over the Internet, as well as protection from and prosecution of such attacks.

- *Increasing organized crime*
  While sheer interest used to be the main motive of the hacker scene until recently, financial motives are now behind attacks on information technology infrastructures. Increasingly, organized crime, especially from Eastern Europe, is brought into connection with such attacks.

- *Professionalization of the hacker scene*
  Concomitant with the focus on financial interests, a professionalization of the attackers has been observed. With technologically increasingly clever hybrid pests, able to combine the attack vectors and destructive potentials of various types of malware, hackers at times even engage in veritable malware wars.

- *Targeted espionage attacks*
  In the first half year of 2005, a number of targeted espionage attacks took place against businesses and state systems. By employing espionage malware tailored to the specific victim, discovery of the pest is to be prevented for as long as possible. If the pest remains unknown to anti-virus software manufacturers, it can be employed undiscovered for a long period of time.

Figure 1: Focus areas of the first issue of the MELANI semi-annual report: botnets, increased crime, professionalisation of the hacker scene and targeted espionage attacks

[1] http://de.statista.com/statistik/daten/studie/186370/umfrage/anzahl-der-internetnutzer-weltweit-zeitreihe/ (as at 28 February 2015)

[2] See current semi-annual report, Chapter 3.5

If we examine the first MELANI semi-annual report from 2005, however, we find that the topics have largely remained the same: targeted espionage attacks, *phishing*, *DDoS*, *defacement* and *social engineering* already existed in 2005. Even the threats and risks for mobile phone users were covered in the first semi-annual report, and the ever-current issue of anonymity on the internet was also dealt with. While the core topics have changed only slightly, there has been major professionalisation among attackers, and their work has been divided up extensively in the last ten years. Nowadays, cybercriminals specialise in the various topic-specific areas such as vulnerability detection, malware production or the sending of spam e-mails. Ten years ago, the change from "hack for joy" to "hack for financial motives" had already been set in motion, and the field of players had only a small number of criminals. In the meantime, a veritable cyber black market has developed where everything needed for an attack can be obtained. However, some countries have greatly expanded and honed their espionage and surveillance methods too.

Naturally, this has led a massive increase in the number of attacks. In contrast to 2005, internet users no longer face isolated incidents, but rather a constant threat to their information or means of communication. Centres, such as the Reporting and Analysis Centre for Information Assurance MELANI, and their various partners active in the area of security of critical information infrastructures are always coming up against new challenges. In order to overcome these, countermeasures have to be reviewed and adapted where necessary. Companies constantly have to include findings about this quickly evolving environment in their risk strategy and adapt their processes accordingly. Nevertheless, a certain degree of routine and composure has been established. For instance, while a wave of *phishing* targeting Switzerland still caused discomposure as well as a media storm in 2005, and dealing with an incident like this represented new territory, defending against these kinds of *phishing* attacks, which occur several times a day nowadays, has become routine. Likewise, media interest is now limited to individual cases with prominent victims or spectacular losses.

The question still remains as to whether ICT security awareness has increased among the general public. It is clear from the reports received by MELANI on a daily basis that users have become more careful. However, it is just as clear that there is still huge potential for averting attacks in the area of prevention.

Did you know that, over the last ten years, the Reporting and Analysis Centre for Information Assurance MELANI has

- published 20 semi-annual reports
- organised 33 workshops for operators of critical infrastructure
- published 111 newsletters
- accepted 141 operators of critical infrastructure to the MELANI information network
- processed 1,765 pieces of information from and for operators of critical infrastructure
- written to providers over 3,000 times to get them to deactivate *phishing* websites
- responded to over 9,000 queries from the public
- received over 27,000 tip-offs from the public via the public reporting form

To illustrate these trends, MELANI has created a poster with a timeline based on three themes presented side by side: internet, risks and MELANI action. This is by no means exhaustive given the vast number of events that marked the past decade; it simply aims to show these themes in a dynamic way and give some landmarks. The poster is attached to this document.

3.2 Spam – for but also from Swiss people

Aside from the usual *spam* e-mails advertising medication and impotence treatments that have been filling the mailboxes of internet users for over a decade now, e-mails with *malware* (malicious code) in attachments were also increasingly in circulation again in the second half of 2014. Unlike in previous years, MELANI recorded more e-mails that contained a text document in *Rich Text Format* (file ending *.rtf*) instead of an executable file (typically with the file ending *.exe*, *.pif*, *.scr* or *.com*). The malicious code is embedded in the text document and the recipient is prompted to open the file contained in the e-mail by double-clicking on it.

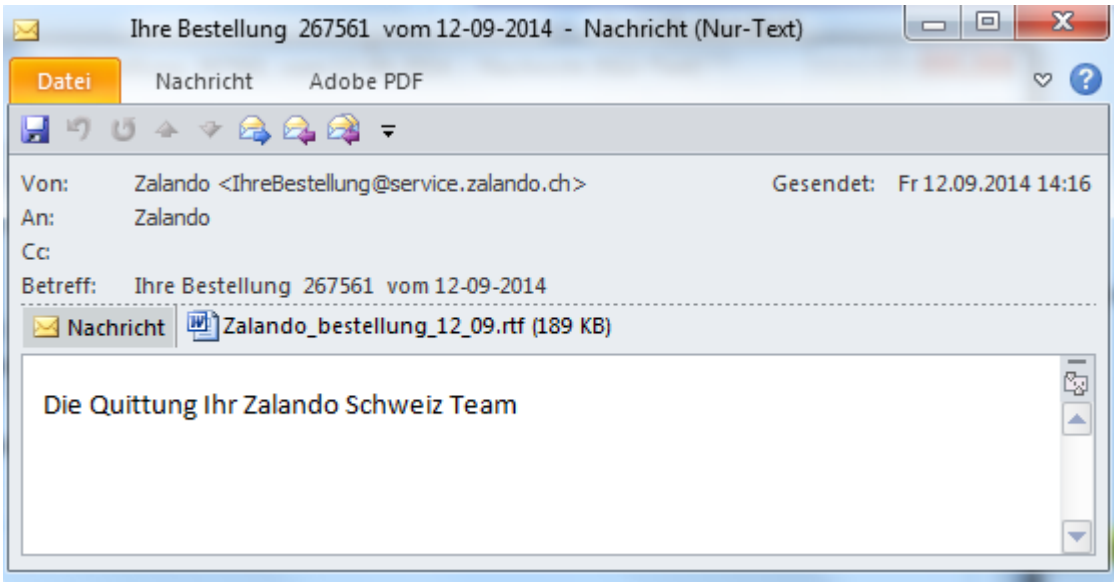


Figure 2: Bogus e-mail allegedly sent by Zalando with a malicious RTF document attached

Many of these spam campaigns were designed for Switzerland and passed themselves off as well-known online traders such as Zalando or Le Shop. Despite mistakes in the text, this misled many users in Switzerland into opening the document, running the malicious code and thus infecting their device with an e-banking Trojan.

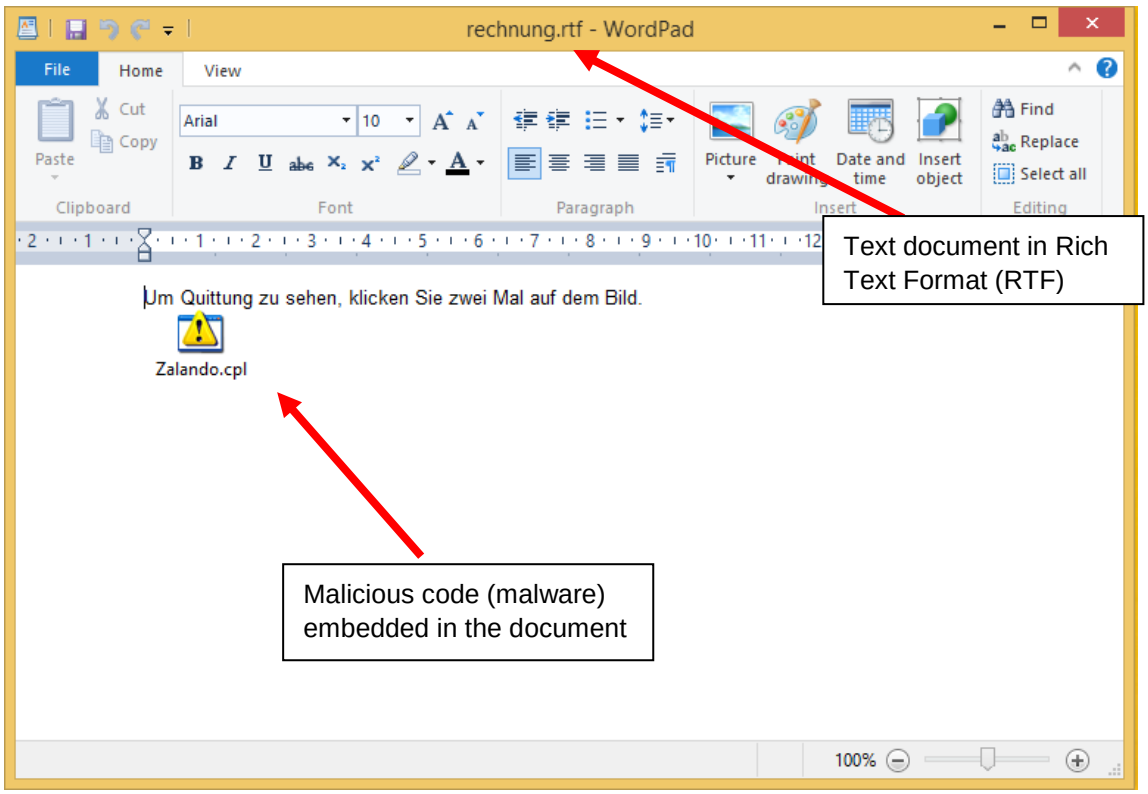


Figure 3: Example of a malicious RTF file

However, Swiss users are not only the targets of spam e-mails, but are often the senders of such undesirable digital communications too, as shown by a report published in July 2014 by the antivirus manufacturer Sophos.[3] The report presents the number of spam e-mails sent in relation to the number of inhabitants in the various countries. Switzerland secured third place in the second quarter of 2014. MELANI is aware of various cases where the sender of spam e-mails was from Switzerland. In one case, over 18,000 spam e-mails were sent via the hacked account of a Swiss e-mail address. In most cases, the unsuspecting e-mail account owners had previously disclosed their login details in a *phishing* attack. In other cases, malware was present on the computers in question.

[3] Sophos: Dirty Dozen Spampionship – which country is spewing the most spam? https://nakedsecurity.sophos.com/2014/07/22/dirty-dozen-spampionship-which-country-is-spewing-the-most-spam/ (as at 28 February 2015)

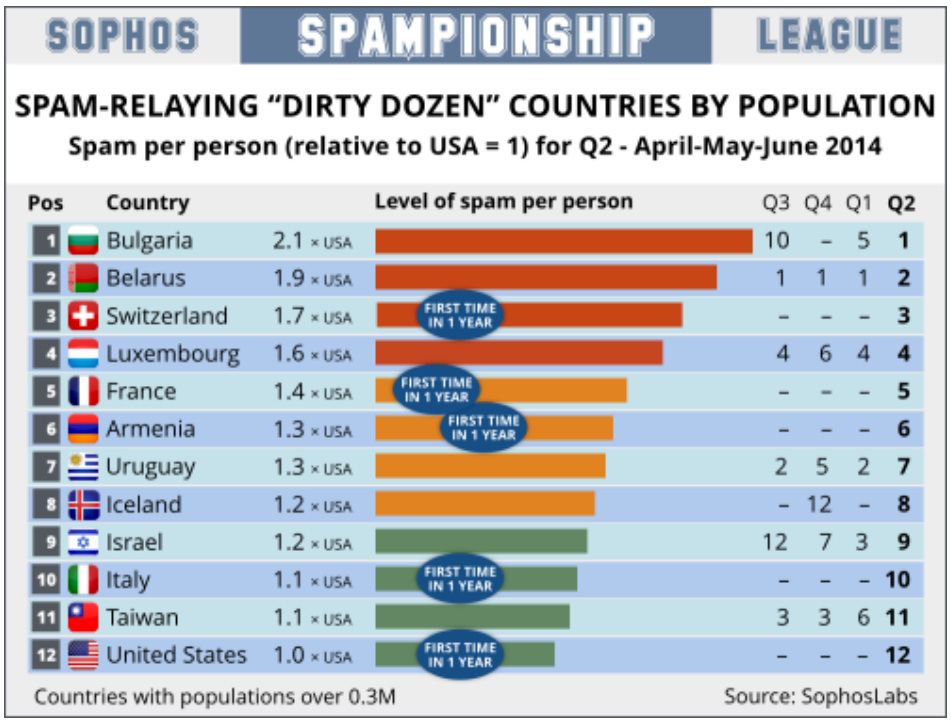


Figure 4: Spam statistics (source: Sophos)

MELANI recommends exercising caution when dealing with e-mails and refers users to MELANI's rules of conduct:
http://www.melani.admin.ch/themen/00166/00172/index.html?lang=en

To prevent or limit falsification of sender e-mail addresses, MELANI recommends that e-mail providers use the relevant technologies such as SPF and DKIM:

Sender Policy Framework (SPF):
http://www.openspf.org/

DomainKeys Identified Mail (DKIM):
http://www.dkim.org/

3.3 Weltwoche – a cyberattack victim

There are more and more online reactions to polarising events, particularly when these events are of a political or religious nature. The internet thus regularly serves as an outlet. The reactions to the attack on the satirical magazine *Charlie Hebdo* are a current example of this: while there was a worldwide show of solidarity on various social media platforms ("Je suis Charlie"), a huge number of websites in France were defaced and covered with Islamic militant propaganda. Such *defacements* do not require extensive knowledge, but they do attract massive media attention and therefore do not fail to achieve the desired effect.

Switzerland has also been affected several times by such politically or religiously motivated attacks. Examples include the *DDoS* attack on PostFinance after the account of WikiLeaks

founder Julien Assange was frozen in 2010[4] or the defacement of several thousand websites following the adoption of the minaret ban initiative in 2009[5].

The publication of an Andreas Thiel article criticising the Quran in the *Weltwoche* issue of 28 November 2014 also resulted in an online reaction: a *DDoS* attack left the *Weltwoche* website paralysed for some time.[6]

The rise and sometimes sheer force of *DDoS* attacks in recent months is an alarming development. For instance, the hacker group Lizard Squad managed de facto to take two of the biggest online services in the field of entertainment, the Sony PlayStation Network and Xbox Live, offline at the same time for at least 24 hours at Christmastime. It is difficult to estimate the damage caused by this. Therefore, it is recommended that every company which depends on its business activities being accessible via a website and/or internet connectivity should clarify the risks posed by attacks of this nature and plan defensive measures. In addition to the company's own technical measures to detect and eliminate problems, this also typically includes assessing the upstream provider's capabilities and its contractual obligations in the event of an incident.

3.4 Poorly protected systems – 141 open webcams in Switzerland

More and more devices have an *Ethernet* or *WLAN* interface and can be connected to the internet. Examples of the most common devices are webcams, file storage devices, printers, scanners and music or video servers. This range of devices will expand even further in the future (see Chapter 5.2 Complete connectivity – smart and safe?). The fact that these devices are mostly intended and preconfigured for use in an internal network is easily forgotten. This means that they are not protected at all or are only protected by a weak standard password. Protection is ensured via the central *firewall* or the router, which prevents the devices from being accessed directly from the internet. If there is no protection and the devices are directly connected to the internet, or they are intentionally enabled for internet access, they are thus visible to everyone and can theoretically be accessed by any number of people if no, or only poor, password protection is in place.

A case of this kind hit the headlines in November 2014. Numerous newspapers reported that thousands of webcams had been hacked and the live images could be accessed via a Russian website. This included 141 webcams that were traced to Switzerland.[7] Along with unspectacular views of garages, there were also problematic recordings such as images from baby monitor cameras (baby cams). However, closer inspection showed that the cameras had been hacked using only standard passwords. The users had forgotten to change the default passwords.

---

4 MELANI semi-annual report 2010/2, Chapter 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=en (as at 28 February 2015)

5 MELANI semi-annual report 2009/2, Chapter 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=en (as at 28 February 2015)

6 http://www.tagesanzeiger.ch/schweiz/standard/Nach-KoranKritik-Weltwoche-ist-Opfer-einer-CyberAttacke/story/19607439 (as at 28 February 2015)

7 http://www.tagesanzeiger.ch/digital/internet/141-Schweizer-Webcams-gehackt-und-live-ins-Netz-gestellt/story/20973442 (as at 28 February 2015)

Devices that are connected directly to the internet merit special protection. This includes not only the setting of passwords that meet the latest requirements, but also the consistent updating of devices with the most up-to-date software or *firmware*.

This case does not concern hacking as much as it does operator negligence in the configuration of devices. Nevertheless, it is an example of how criminals also focus on accessing cameras. This is also connected to the fact that web cameras are found in many devices nowadays. For instance, smartphones, tablets, laptops and also various television sets have a built-in camera. Furthermore, users' awareness of built-in cameras is still quite low. If malware is installed on a device that has a camera, for instance, the camera can be penetrated. Depending on the location of the device, this can result in major drawbacks for the victim, particularly if we consider all of the places where a smartphone is taken, for instance.

MELANI recommends covering webcams with adhesive tape when they are not in use. Nowadays, there are also special camera covers that can be used to temporarily cover the camera lens.

Figure 5: A temporary camera cover both open (left) and closed.[8]

3.5 CMS – vulnerabilities and a lack of awareness among web administrators

The majority of *phishing* pages and *drive-by infections* are placed on websites administered using *content management systems* (*CMS*) that are not up-to-date. In 2014 alone, 14 vulnerabilities were discovered in the CMS software Drupal, nine were discovered in Joomla! and 29 in WordPress.[9] It is therefore essential that all operators update their CMS software regularly. Nevertheless, too little attention is being given to this very area in many cases. There are still many website operators who install a CMS and then forget to download updates regularly. Such vulnerable websites can be found and attacked automatically using appropriate tools. It is thus relatively easy for criminals to detect and manipulate a large number of websites in this way.

In a particularly severe case, Google even blocked 11,000 websites from the search index. This was after supposedly over one hundred thousand WordPress installations had been

[8] http://www.soomz.io (as at 28 February 2015)

[9] http://www.cvedetails.com (as at 28 February 2015)

infected with the SoakSoak malware and had thus installed malware on the computers of those who visited the infected websites.

In another case, systems were not compromised by taking advantage of a security vulnerability. Instead, the attackers made a manipulated *plug-in* or (design) theme available to CMS operators free of charge. This contained malware which enabled access to the web servers. Tens of thousands of web servers were infected with this malicious code called CryptoPHP, which was spread above all for Drupal, WordPress or Joomla. Once infected with CryptoPHP, the code is used for what is known as *black hat search engine optimisation* (BHSEO). This mostly involves inserting keywords or manipulated pages into compromised websites to influence the search engine *ranking*. Using access to the web servers, however, the attackers can also change the content of websites, place drive-by infections or *phishing* pages, and even just upload false information. Furthermore, web servers infected with CryptoPHP act as part of a *botnet*.

Attacks on CMSs can be reduced dramatically by means of *patching* (prompt incorporation of security updates). However, several other measures can contribute to the security of CMSs. You can find recommendations on the MELANI website under "Checklists and instructions".[10]

3.6 Ransomware on the rise: new malware SynoLocker – cases in Switzerland too

The ransomware scene is continually expanding. A few years ago, the *ransomware* that was being encountered only froze the computer screen and could be eliminated with a few skilful tricks. In contrast, current versions have the potential to do far more damage. Following on from CryptoLocker, which we wrote about in our last semi-annual report, a new piece of malware by the name of SynoLocker emerged in the current reporting period. There have also been numerous cases in Switzerland that were reported to MELANI. In the case of infection, all data is encrypted on a *network-attached storage* (NAS) device and a demand for money is made in return for the private key needed for decryption. Only the public key needed for asynchronous encryption appears on the victim's computer. Decryption without the corresponding private key is virtually impossible. The infection in this case did not require any user interaction, but targeted a security vulnerability in the NAS devices of the company Synology to its own advantage. This was not an unknown security vulnerability; it had been detected and a *patch* has been available for it since December 2013.[11] The same security vulnerability had apparently been exploited by different malware already in February 2014. On that occasion, hackers had installed bitcoin-mining programs on the NAS devices and generated crypto coins without the users' knowledge.[12]

It is all too often forgotten that updates must also be downloaded for routers, network-attached storage devices and similar devices (see also the semi-annual report 2014/1[13]). This is particularly serious if these devices are connected directly to the internet.

---

10 http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=en

11 http://www.heise.de/security/meldung/Jetzt-updaten-Aeltere-Synology-NAS-Geraete-anfaellig-fuer-Ransomware-2287427.html (as at 28 February 2015)

12 http://www.synology-forum.de/showthread.html?50468-Aktive-Hackangriffe-auf-DSM-Versionen-kleiner-4-3-3810-Update-3 (as at 28 February 2015)

13 MELANI semi-annual report 2014/1, Chapter 4.13: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=en (as at 28 February 2015)

In August 2014, another encryption Trojan called CTB-Locker appeared on the scene. What is special about this Trojan is that communication with its command servers occurs in encrypted form and it uses the *internet anonymity tool Tor* to cover its tracks. This makes it difficult for the police and security firms to find and analyse these command servers.

However, there was a positive development in the second half of 2014: the ICT security service providers FireEye and Fox-IT made a free service available which makes it possible for CryptoLocker victims to recover the data that was encrypted by the malware.[14] Action taken by the FBI against the CryptoLocker *botnet* managed to secure the private keys. The data can be decrypted using these keys. It cannot be ruled out that the relevant cryptographic keys in the SynoLocker case will also be secured at a later date through research and investigations, as they were for CryptoLocker. Consequently, people who have irrecoverable data encrypted by SynoLocker should hold on to it nevertheless.

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. Operating systems as well as all applications installed on the computer (e.g. Adobe Reader, Adobe Flash, Sun Java, etc.) must be updated consistently, and preferably with the automatic update function if available. This also applies for the *firmware* on *routers*, *NAS*, music servers, etc.

3.7 Swiss Internet Security Alliance – cooperation for increased security on the internet

With the goal of joining forces to tackle cybercrime, internet service providers, banks and other partners founded the Swiss Internet Security Alliance (SISA) on 12 September 2014. Through this cross-sector partnership, members wish to highlight their commitment to the security of their services and customers. The founding of the SISA brings together the specialist knowledge of various industry representatives and promotes exchange among competitors. In this way, it also emphasises the knowledge, experience and technical skills of its members as its greatest asset. Its members include asut, Centralway, Credit Suisse, cyscon Schweiz, Luzern University of Applied Sciences and Arts, Hostpoint, Migros Bank, PostFinance, Raiffeisen, Sunrise, Swisscard, Swisscom, SWITCH, UBS, upc cablecom and Viseca. They have many years of experience in dealing with security on the internet. The alliance remains open to other interested parties.[15]

[14] https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html (as at 28 February 2015)

[15] https://www.swiss-isa.ch/ (as at 28 February 2015)

4 Current international ICT infrastructure situation

4.1 Cyberattack on network of Sony Pictures Entertainment

On 24 November 2014, employees of Sony Pictures Entertainment (SPE) worldwide discovered on their computers that a group calling itself Guardians of Peace had hijacked the company's network. The group indicated that it had copied internal data from the corporate network and threatened to publish it. Not only was the malware able to steal data, it apparently had a data deletion routine as well. The entire network then remained inaccessible for several days. The Guardians of Peace claimed to be in possession of 100 terabytes of data, i.e. the equivalent of around 150,000 CD-ROMs. They apparently copied sensitive data such as the salary list of the 6,000 employees and senior executives, internal e-mails as well as unreleased films. Five unreleased films then turned up on file-sharing networks at the start of December, and a version of the screenplay for the new James Bond film "Spectre" also did the rounds on the internet. Already on 21 November 2014, executives of Sony Pictures Entertainment had received an e-mail demanding monetary compensation. Another group called God'sApstls threatened in the e-mail that Sony Pictures would be "bombarded as a whole" in the absence of compensation for the great – undefined – damage that it had caused. The deadline set in the message to the executives was 24 November, i.e. the date the attack was published.[16] However, the link between the two groups Guardians of Peace and God'sApstls remained unclear.

It was quickly speculated that this attack was associated with the planned release of the film "The Interview", a comedy about a CIA plot to assassinate North Korea's supreme leader Kim Jong-un, which was scheduled to be shown in cinemas at Christmas 2014. In July 2014, North Korea's UN Ambassador complained to the UN Secretary-General about the planned film's scenario. On 1 December, it was suspected in US circles that the attack was sponsored by North Korea.[17] On 8 December, a message from Guardians of Peace appeared on the website of the repository hosting service GitHub, explicitly demanding that the release of the film be cancelled: "Stop immediately showing the movie of terrorism which can break the regional peace and cause the War!".

The FBI was tasked with investigating the incident and published its initial findings on 19 December.[18] The investigators explained that they had gathered enough information to conclude that the North Korean government was responsible for these actions. For example, the data deletion malware was apparently linked to other malware that North Korea had previously developed and there were similarities in lines of code, encryption algorithms and data deletion methods. Moreover, there was a significant overlap between the infrastructure used in this attack and earlier attacks supposedly of North Korean origin. The IP addresses that were hardcoded into the malware communicated with known North Korean infrastructure. Likewise, there were similarities with the attacks of March 2013 (DarkSeoul)[19]

---

16 http://www.hotforsecurity.com/blog/leaked-emails-reveal-that-hackers-demanded-money-from-sony-pictures-before-attack-10964.html (as at 28 February 2015)

17 http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202 (as at 28 February 2015)

18 http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (as at 28 February 2015)

19 MELANI Semi-annual report 2010/2, Chapter 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=en (as at 28 February 2015)

on South Korean banks and broadcasting corporations, which were also carried out by North Korea according to the FBI.

North Korea's foreign ministry immediately refuted the accusations, stating that it could prove that the attack had nothing to do with the North Korean government. At the same time, it invited the United States to conduct joint investigations.

On 7 January 2015, the FBI's director, James Comey, repeated at an ICT security conference in New York that the US Secret Service would assume that the attacks had been launched from North Korea.[20] He did not offer more precise details, however. It was said that the FBI had discovered that the hackers made critical errors, given that the group Guardians of Peace had posted various messages on their Facebook account after having logged in from North Korean IP addresses.[21] After having recognised their mistake, they rerouted everything through computers in other countries to cover their tracks.

According to several sources, North Korea was not behind this attack, or was not the only player involved. Some experts suspected that former Sony employees were behind it. It was thus speculated that an employee laid off in May 2014 was involved in the attack.[22]

The US sanctions against North Korea were stepped up following the attack on Sony Pictures Entertainment, with sanctions imposed on ten Pyongyang government officials as well as on three organisations and companies.

In response to the repeated cyberattacks on US companies and the US government, the United States plans to establish a new Cyber Threat Intelligence Integration Center, which is to pool and analyse information from various sources.

This incident demonstrates that it is extremely difficult in cyberspace to provide conclusive proof of attacks attributed to a state. On the one hand, unlike with conventional attacks, there are many ways of concealing the source of an attack and also of misleading people. On the other, it would be wrong to think that government employees are the only ones at their keyboards in the case of state attacks. There is likely to be a very thin line between state attacks, attacks ordered by states and those tolerated by states. At best, we find hackers who can be attributed to a specific country. However, proof that the country is behind the attack is still far from being provided and has to be sought onsite. Onsite investigations are typically impossible in such a case, though.

Consequently, the proof is frequently sought in the motives for the attacks. In the absence of monetary stakes, it is quickly concluded that a professional, state attack is involved. Individuals who steel data off their own bat in order to then offer it to states have been around since long before the sale of tax CDs started. The structure of the cybercrime underground market is certainly too complex for this simple formula to apply for all cases. Even in this case, it could well be that several players were involved and that they all contributed to the complexity of the case.

---

20 http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (as at 28 February 2015)

21 http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (as at 28 February 2015)

22 http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/ (as at 28 February 2015)

4.2 Attacks on industrial facilities

Industrial facilities are becoming increasingly networked. In addition to simplifying remote monitoring and maintenance, this also carries a higher risk of unauthorised access and manipulations. Aside from state players acting strategically, who might perhaps be interested in such facilities for military reasons, many security experts and hobby hackers have also had their attention drawn to this trend. That is why *SCADA* and industrial control systems were also topics at the 31st Chaos Communication Congress in December 2014.[23] Simulators for control systems such as those used in chemical plants have now been developed and can be used to test one's hacking skills. Moreover, there are *exploit kits* available that have been specifically programmed for identifying and exploiting security vulnerabilities in industrial facilities.

According to a report published by the German Federal Office for Information Security (BSI)[24] in December 2014, a steel plant in Germany was the victim of a targeted attack that caused damage to a smelting furnace. The attackers apparently used *spear phishing* and sophisticated *social engineering* to access the company's office network, and from there they gradually worked their way into the production network. The breakdown of individual control components or entire facilities subsequently prevented a smelting furnace from being shut down in a controlled manner, causing substantial damage to it. The BSI reckons that not only did the attackers know a great deal about classical ICT security, they also had a wealth of specialist expertise regarding the production processes and industrial control systems used. The BSI's report is merely factual and does not make any comment on the possible perpetrators.

Those who commit acts of pure sabotage are usually motivated by the same things: either a competitor is trying to gain an advantage or a dissatisfied (former) employee wants to get one over on his employer and uses his insider knowledge to do so, or else third parties want to find out or prove just how much is possible. It would appear unrealistic in this case that a foreign state would have wanted to sabotage steel production in Germany. However, the potential of cyber sabotage is increasingly being included in military strategies and war scenarios.

Last but not least, the possibility of sabotage also gives criminals the opportunity to blackmail facility operators.[25] This is particularly promising where a facility relies on a connection with other networks and systems and cannot simply be isolated in the short term in the event of such a threat. Besides, it is also conceivable that malware can be planted and activated at a specific time irrespective of internet connectivity. In such a case, the risk would not be eliminated even if the system were disconnected from the network; instead, the malware would have to be found and neutralised. Depending on the complexity of the system, this can be challenging if you do not know exactly what has to be searched for.

It is important to include the security aspect when networking physical systems. The most common vectors of attack for control systems are the office network, *removable storage devices* and insufficiently secured remote access. Remedial action can be taken here by ensuring stringent segmentation of networks (shielding control systems from the office network and controlling data exchanges well if these are necessary), using dedicated removable storage devices that are regularly checked and using strong authentication

[23] https://events.ccc.de/congress/2014/wiki/

[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[25] See also Chapter 5.3 of this semi-annual report

methods and encrypted data transmission to protect remote access. See also the MELANI checklist on measures for the protection of industrial control systems (ICS).[26]

4.3 Attacks on the energy and oil sector

In August 2014, it emerged that approximately 300 companies in Norway's energy and oil sector had been attacked. The attackers were at least partly successful with their *social engineering* methods: according to the statements made by the Norwegian security authorities, the attackers initially conducted searches to identify key functions and corresponding staff members in the companies in order to then send them customised, legitimate-looking e-mails with malware attached. Opening such an attachment installed an *exploit kit* that searched the system for vulnerabilities and downloaded a highly specialised spyware program where possible. This approach apparently made it possible to find out trade secrets as well as the access data for other systems.

Energy companies – particularly those in the area of oil and natural gas supply – have been exposed to increased pressure from cyberattacks for a long time now.[27] This could be linked to the political, but more so the economic, significance of this sector. Some players seek to use an information edge gained through espionage to secure an advantage over their competitors, be they in the public or private sector. Others try in a targeted manner to sabotage the operations of energy companies in order to then profit directly from their production stoppage or share price fluctuations. Finally, it is also worth remembering the (military) strategic importance of fossil fuels, particularly for motor fuel supply, which causes state players to intervene on both the offensive and defensive levels.

4.4 Points of sale targeted by attackers

In the past we have already discussed the problem of attacks on *point of sale* terminals such as those affecting the North American retailer Target.[28] The principal purpose of these attacks is to obtain credit card data, even if other personal details are sometimes stolen at the same time as well. Another similar case made the headlines at the end of 2014, as the US retailer Home Depot confirmed on 14 September 2014 that it had been the victim of a cyberattack between April and September involving the theft of data on around 56 million credit cards. This communication confirmed and brought clarification regarding many pieces of information that had been published in the preceding weeks by specialist blogs or newspapers. The method used for the attack was highly reminiscent of what had been seen in the Target case: *RAM scraper* malware was installed on points of sale after one of the company's suppliers had initially been compromised.

However, this modus operandi is not the only one used by criminals to compromise point of sale terminals. Back in July 2014, the network security company FireEye drew attention to the malware called BrutPOS, which seeks to exploit remote terminal administration interfaces that have weak passwords. According to FireEye, BrutPOS apparently uses a botnet consisting of more than 5,500 compromised computers to identify vulnerable systems of this

[26] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=en (as at 28 February 2015)

[27] MELANI Semi-annual report 2014/1, Chapter 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=en (as at 28 February 2015)

[28] MELANI Semi-annual report 2013/2, Chapter 4.4; Attacks on Target retail chain outlets: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=en (as at 28 February 2015)

kind. "Standard" passwords such as "admin", "client" and "password" are tried to do so. Once the system has been penetrated, the criminals attempt to obtain credit card data by means of RAM scraping.

These examples highlight the fact that point of sale terminals remain the core concern for certain groups of criminals. Significant resources are invested to target these systems, which enable huge profits to be generated. The credit card data seized is frequently sold on underground forums and is ultimately used to make online purchases without the card owner's knowledge. The reason why US companies in particular have been attacked is that they are comparatively appealing targets because they have high volumes of business and frequently have insufficient protection. As it happens, the chip-and-PIN system for credit card payments that is common in Europe is not widely used in the United States.[29] Although attacks on providers using this system are conceivable as well, the criminals' cost/benefit ratio is currently more favourable with attacks on systems that do not use this standard.

More specifically, the case of the BrutPOS botnet highlights just how important it is to protect all interfaces that grant remote access to a device or system. MELANI has already repeatedly drawn attention to the risks involved in the trend of networking growing numbers of control devices for physical processes in the manufacturing and home automation sectors. Even if the devices or systems concerned are very different, the rules for securing remote access largely remain the same.

4.5 Espionage – selected cases from the second half of 2014

Clues as to the originator of Regin

Several spying incidents were once again detected in the last six months. The biggest stir in this regard was caused by reports from Symantec, Kaspersky and F-Secure in November 2014 about a piece of malware known as Regin.[30] For several years, the Trojan Regin is supposed to have covertly spied on various victims, including targets in Russia and Saudi Arabia, as well as in Western European countries such as Belgium and Austria. Regin apparently provides its programmers with a powerful framework for mass surveillance and has been used in spying operations against government organisations, infrastructure operators, businesses, researchers and private individuals. Spying operations that target telecommunications companies are particularly worthy of mention: it would appear that one in four cases concerned such providers. In this regard, Symantec discovered a function that focuses on GSM-base stations. Kaspersky, which also examined the malware, specified that in April 2008, Regin was used to steal GSM administration access codes related to countries in the middle east. With such codes it is possible to manipulate GSM networks. Shortly afterwards, the website The Intercept reported that Regin had been used against the telecom operator Belgacom, among others. Based on the documents published by the whistle-blower Edward Snowden, it was suspected that Britain's security and intelligence organisation GCHQ was behind the attack. Kaspersky published further evidence concerning the perpetrators in January 2015. The security firm found similarities between Regin and a piece

[29] In the United States, just like in many other countries around the world, most of the credit cards in circulation have their data stored on a magnetic strip.

[30] http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance (as at 28 February 2015)
http://www.kaspersky.com/about/news/virus/2014/Regin-a-malicious-platform-capable-of-spying-on-GSM-networks (as at 28 February 2015)

of malware known as QWERTY. The German magazine Der Spiegel had previously published the *source code* of the QWERTY malware, found in the Edward Snowden archive. QWERTY is supposedly the *keylogger module* from Regin.[31]

At the end of 2014, several newspapers reported that the Regin malware had been found on a computer in Germany's Federal Chancellery. It was speculated that the virus scanner detected it when a USB flash drive that had previously been used on an employee's private computer was inserted in an official Chancellery computer. A government spokeswoman later explained that the network had not been infected.[32]

Red October reloaded?

In December 2014, the security firm Bluecoat discovered a targeted espionage attack that stood out because it could also infect Android, iOS and Blackberry mobile devices. However, iPhones and iPads could be infected only if they had been *jailbroken* beforehand. Furthermore, the malware used an unusual command and control mechanism. All of the infected devices communicated via https and WebDav with the same server of the Swedish *cloud* service called CloudMe. The malware, known as Inception, was used primarily to spy on senior executives in the oil and natural gas sector, as well as those in finance, military officers, government officials and embassy personnel. The malware delivery method was via *spear phishing* e-mails containing trojanised documents. Kaspersky also published information on this espionage campaign, called Cloud Atlas[33], suspecting that it could be a new version of the Red October malware. That espionage network was promptly shut down following the publication of Kaspersky's report on Red October in January 2013. Similarities were also found between Cloud Atlas and the Red October campaign. Aside from the group of victims being similar, a document used in a *spear phishing* attack was virtually identical.

Cloud Atlas is a typical example of an *advanced persistent threat* (*APT*). Aside from the high level of professionalism (*advanced*), the key in this case is that it is *persistent*. When a targeted espionage attack is discovered and thus also neutralised, it is to be expected that the attackers will either turn up elsewhere in the system or that they will repeat their attacks sooner rather than later.

Sandworm – attacks on NATO and members of the Ukrainian government

At the end of October 2014, the security firm iSIGHT announced a targeted espionage campaign that was conducted against NATO, EU and Ukrainian government members by exploiting a security vulnerability in Windows, among other things.[34] Other targets of the attack included a French telecommunications firm and a Polish energy sector company. The exploitation of this previously unknown security vulnerability in Microsoft Windows and Windows Server (CVE-2014-4114) suggests it was performed by a highly professional player.[35]

---

31 http://www.spiegel.de/netzwelt/netzpolitik/nsa-trojaner-kaspersky-enttarnt-regin-a-1015222.html (as at 28 February 2015)
http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html (as at 28 February 2015)

32 http://www.heise.de/newsticker/meldung/Offenbar-Spionagesoftware-Regin-auf-Rechner-im-Kanzleramt-entdeckt-2507042.html (as at 28 February 2015)

33 https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/ (Stand: 28. Februar 2015)

34 http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/ (as at 28 February 2015)

35 http://www.isightpartners.com/2014/10/cve-2014-4114/ (as at 28 February 2015)

The attacks on Ukrainian government officials apparently commenced in the summer of 2014 and were conducted by selectively sending a PowerPoint document that exploited the aforementioned vulnerability to the victims. However, iSIGHT was able to trace the group's first activities back to 2009. Although the interests and certain linguistic elements indicate a campaign of Russian origin, it has not been possible to determine the perpetrators beyond any doubt in this case either.

Various alleged attacks on Israeli firms

At the end of July 2014, the independent journalist Brian Krebs reported that plans for the Israeli army's Iron Dome missile shield were apparently stolen on several occasions in 2011 and 2012.[36] Krebs referred to the US threat intelligence firm Cyber Engineering Services Inc. (CyberESI), which investigated the campaign. The three Israeli defence technology companies Rafael Advanced Defense Systems, Israel Aerospace Industries and Elisra Group were supposedly affected. It was suspected that the attack was conducted by the Chinese group known as APT1, or PLA Unit 61398. The firms concerned did not confirm the attacks.

US Nuclear Regulatory Commission

It would appear that the US Nuclear Regulatory Commission was successfully hacked at least three times over the last three years. It was presumed a foreign government was responsible. It was apparently possible to trace two of the cases to a specific foreign country, but it was not said which one. According to Nextgov[37], the usual attack methods of *phishing* and *spear phishing* were used. Interestingly, an employee's e-mail account was used in the third attack to send a compromised PDF file to another 16 employees, thereby making it all the more difficult for the recipients to identify a malicious e-mail. This is a common procedure for reaching "interesting" computers within a company via interim workstations that are easier to infiltrate.

Targeted espionage attacks are not isolated incidents. There is ongoing interest in and accordingly constant pressure on sensitive data. It is difficult to determine the originator in all cases. Even if the choice of victims leads to suspicions of state involvement in most *advanced persistent threats* (*APT*), the boundary between state and criminal hackers is frequently blurred.

Amnesty International proposes tool for detecting surveillance software

In November 2014, Amnesty International proposed a tool designed to detect surveillance spyware used by governments. One example is FinFisher, which can be used to wiretap Skype calls, intercept e-mails and even control the camera on devices remotely, for instance. The software is also used for example against human rights activists and dissidents in countries with authoritarian regimes and limited freedom of expression. It is unclear, however, just to what extent the tool can detect the various types of surveillance software.[38]

---

36 http://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/ (as at 28 February 2015)

37 http://www.nextgov.com/cybersecurity/2014/08/exclusive-nuke-regulator-hacked-suspected-foreign-powers/91643/ (as at 28 February 2015)

38 http://www.amnesty.ch/de/themen/weitere/meinungsaeusserungsfreiheit/dok/2014/detekt-software-zum-aufdecken-von-ueberwachung (as at 28 February 2015)

4.6 Espionage attack during business trips

For a long time now, there have been warnings about being particularly vigilant when using public *WLAN* connections. Up to now, the most famous example of an attack on such a network was known as Firesheep, which allowed effortless *session hijacking* on an unsecure, i.e. open, network (e.g. in an internet café) in order to capture user data such as passwords. However, this attack works only with unencrypted data transmission without an HTTPS secure transfer protocol. In November 2014, the software security group Kaspersky published a report on a spy network, dubbed Darkhotel, which had been conducting targeted attacks in the WiFi networks of hotels that went far beyond the attacks known up to then.[39] Over a period of four years, there had apparently been targeted attacks on top managers during their business trips in Asia, which suggests that it was a case of economic espionage. However, other people were also attacked randomly. The attack commences as soon as the targets check in, start using their computers and want to log on to the hotel's WLAN, upon which they are notified that a specific program needs updating. Examples of the programs mentioned are Google Toolbar, Adobe Flash and Windows Messenger. Of course, these updates are nothing more than malware that can steal data from the computer in question.

Furthermore, the US Secret Service issued a warning in the last six months about *keyloggers* on computers made available to people in hotels and airports. An advisory distributed to companies in the hospitality industry recommended inspecting computers made available to guests. This advisory was triggered by the arrest of suspects who had allegedly compromised computers in several major hotel business centres in the Dallas/Fort Worth areas with *keyloggers*.[40]

It is always necessary to exercise a healthy amount of caution when using public WLANs. Care has to be taken not to accept prompts to install programs when attempting to connect to the wireless network. Moreover, the utmost attention has to be paid to keeping the computer fully up to date. Otherwise, even so-called *website infections* are sufficient to infect a computer. People who have to process business-critical data while travelling should consider whether it might not be better to use the personal hotspot function and *roaming* on their mobile phone even if *roaming* is very costly.

No services requiring a login or password should be used on public computers. These computers provided by hotels should be used solely to get information on the city's tourist attractions, for example.

4.7 Large-scale data theft

Several cases of data theft made the headlines once again in 2014. One case in particular stood out – not because of the amount of data stolen, but rather the manner in which the theft was carried out. In August, one of the largest US hospital groups reported the theft of personal data belonging to 4.5 million patients. Precisely in the area of health, patients expect a great deal of attention to be paid to data protection. However, the rate of digitisation is very fast also in healthcare. While this has advantages and also helps to reduce the number of errors, it is not without risk either.

[39] http://blog.kaspersky.com/darkhotel-apt/ (as at 28 February 2015)

[40] http://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-centers/ (as at 28 February 2015)

In the case at hand, Community Health Systems (CHS), one of the leading operators of hospitals in the United States, reported in August 2014 that its computer system had been broken into and that data had been stolen on up to 4.5 million patients who had received treatment at one of the company's hospitals in the preceding five years. The cybersecurity firm Mandiant attributed the theft to Chinese hackers. According to CHS, which manages 206 hospitals in 29 states, the stolen data included names, addresses, telephone numbers, dates of birth and social security numbers. It was not possible to determine the precise aim of the attackers or whether state players were also behind the attack.

The financial sector is another focal point when it comes to data theft. This time it was the attack on JPMorgan Chase, one of the largest banking institutions in the United States, that made the headlines. Apparently, data concerning around 76 million households and 7 million small businesses was copied during the breach, which was discovered in mid-August 2014. The cybercriminals managed to steal client data such as names, addresses, telephone numbers and e-mail addresses from the banking institution's servers. As yet, there is no evidence that sensitive data such as account numbers, dates of birth, passwords or social security numbers was stolen in the breach. According to JPMorgan, the vector of attack was identified as being exploitation of a security vulnerability that existed already in June 2014. It is not known precisely what sort of a security vulnerability it was. Accounts deemed vulnerable were disabled and the passwords of all ICT technicians reset. According to officials, several indicators suggest that the attack was performed by highly professional hackers, possibly in Russia. While it was suspected that the attack was motivated by US sanctions against Russia, this was not proved.

In a somewhat different development, the company Hold Security announced at the start of August 2014 that it had discovered what could be the largest data breach known to date, involving 1.2 billion login and password combinations, apparently pulled off by a Russian cyber gang. The access data came from over 420,000 websites, including those of well-known companies. What was special about this case is that Hold Security announced in the same breath that it would be offering a new service that would make it possible to determine whether people had been impacted by this or other breaches.[41]

Security firms often make such data available to the competent government bodies or affected providers so that the victims can be informed. The question of responsible handling of such information will be increasingly important in the future, and Chapter 5.5 addresses the matter in detail.

4.8 iCloud hacked – celebrity photographs on the internet

At the end of August 2014, stolen photographs of nude celebrities were posted online, firstly on the image board 4chan and then on various other platforms. It quickly transpired that the photographs came from different iCloud accounts, Apple's cloud storage service. Several theories were put forward as to the method used to access the photographs, but it was very quickly believed that the images were obtained using an exploit in the Find My iPhone service for locating lost or stolen devices. According to many expert reports, the program was vulnerable to a *brute force* attack, which consists in the automated testing of a large number of passwords to access a service. This suspicion was driven by the fact that a *proof of concept* (*POC*) concerning this method had been published on the GitHub site shortly before the incident. A classical security measure to protect against *brute force* attacks

[41] http://www.forbes.com/sites/kashmirhill/2014/08/05/huge-password-breach-shady-antics/ (as at 28 February 2015)

involves blocking the service after a certain number of unsuccessful attempts to gain access. This system was not in place for Find My iPhone at the time, but it was implemented soon after the stolen photographs scandal. Apple rejected the theory of a vulnerability in Find My iPhone or another Apple service. In an official statement, the company attributed the leak to a highly targeted attack on user names, passwords and security questions for certain accounts.[42]

This is not the only affair which has called into question the security of cloud storage services. Dropbox, for example, was targeted when account credentials for the service were posted on Pastebin, a web application where anyone can store plain text, in October 2014. These cases bring the focus of attention back to the issue of the security of data stored in the cloud. This means of storage gives a hacker the possibility of accessing a large volume of personal data remotely by compromising a vulnerable system or account. In the case of iCloud and similar services, it also has to be noted that many users are unaware that the photographs they take are automatically synchronised with a cloud account. This setting can actually be activated by default. It is thus essential for users to check if this is the case for each app and deactivate automatic synchronisation if it is not something they want.

For users who decide to use the cloud, the security rules that apply for other online accounts, such as an e-mail account, are recommended. A complex password with different types of character should be chosen for each individual service. MELANI also recommends using *two-factor authentication* whenever possible.[43] Finally, the publication of photographs of nude celebrities should serve as a serious reminder that the best way to prevent compromising material from leaking is not to store it or at least not to store it on a connected digital device.

4.9 Further serious security vulnerabilities in central software components

Over the last six months, not only were numerous bugs found in applications such as Flash, Acrobat, Java and Office, but serious vulnerabilities in operating systems and base libraries were also detected.

Poodle

Already a victim of Heartbleed in the past, the *SSL* network protocol for secure data transmission was once again affected by a serious vulnerability. Unlike Heartbleed, however, the bug known as Poodle[44] was not a programming error, but rather an error in the protocol itself, specifically *SSL* version 3.0. The vulnerability lay in the fact that *SSL/TLS* first protects the integrity of the data and only then encrypts it. As encryption is generally performed in fixed-size blocks, a number of characters, or padding, is tacked on the end of each line in order for the block to be the appropriate length. The last *byte* denotes how many padding bytes were added before. And that is precisely where the problem lies. While the padding and the last byte are encrypted, their integrity is not checked. Attackers can thus insert any characters they want unnoticed, including parts of the lines that are to be encrypted. This is

[42] http://www.bbc.com/news/technology-29039294 (as at 28 February 2015)

[43] A list of sites that allow two-factor authentication is available at: https://twofactorauth.org (as at 28 February 2015)

[44] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 (as at 28 February 2015)

conditional on the attacker being able to carry out a *man-in-the-middle* attack, which is possible in an open wireless network, for instance.[45]

For this reason, MELANI recommends that website operators completely deactivate SSL 3.0 and use only the TLS 1.1 or TLS 1.2 encryption protocol insofar as possible. Support for SSL 3.0 connections has since been removed from most current browsers.

Shellshock

Virtually all Unix-based operating systems were affected by the Shellshock[46] vulnerability, which makes it possible for arbitrary commands to be executed. It was discovered in the widely used Bash shell software. This affects not only servers and clients, but also devices such as *routers* and *security gateways*. Several bugs were found, and patches to fix these were provided on an ongoing basis. The vulnerability arose because the environment variables submitted are not correctly checked, which means it is possible to add malicious code to a variable.

```
$ env x='() { :;}; echo VULNERABLE' bash -c ""
```

There are various attack scenarios:

- HTTP/web server using the CGI interface
- SSH
- DHCP
- SIP
- and many more

After the vulnerability was brought to light, MELANI noticed a massive increase in scan and exploit attempts. Although these have since decreased somewhat, the level remains high.

Kerberos

Another vulnerability (MS14-068[47]), which can have serious consequences for companies in particular, lies in Kerberos implementation in Microsoft's *Active Directory*. A user with an unprivileged account can exploit this vulnerability to achieve an escalation of privileges to those of the domain administrator account and thus take control of an entire *Active Directory*. In principle, this means that a single successful attack (e.g. with a piece of malware) on a user within a company can lead to the entire *Active Directory* and thus all Windows resources being controlled by the attacker. Consequently, MELANI recommends not only fixing the vulnerability, but also preparing and regularly testing emergency plans for restoring the *Active Directory*. Moreover, highly privileged accounts should be specially secured.

---

[45] An extensive explanation of how the Poodle vulnerability works is available here: https://nakedsecurity.sophos.com/2014/10/16/poodle-attack-takes-bytes-out-of-your-data-heres-what-to-do/ (as at 28 February 2015)

[46] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271 as well as the other CVE numbers 2014-7169, 2014-7186, 2014-7187, 2014-6277, 2014-6278 (as at 28 February 2015)

[47] https://technet.microsoft.com/en-us/library/security/ms14-068.aspx (as at 28 February 2015)

Schannel

Another security vulnerability in Windows (MS14-066[48]) concerned Secure Channel, Microsoft's implementation of SSL/TLS encryption, which allows sensitive communication to be exchanged over a public network in encrypted form. According to Microsoft, a remote attacker could exploit the security vulnerability to execute arbitrary malicious code on an affected system via specially crafted packets. Moreover, Cisco mentioned several *buffer overflows* in a blog entry.[49] Microsoft had great difficulties with this patch, which had to be improved several times in order to deal with undesirable side effects such as performance problems.

In general, MELANI has noticed that, in terms of the internet, attacker focus is very much on widely used software such as Flash, Acrobat and Java. As soon as a patch appears, attackers analyse it with regard to the eliminated vulnerability and incorporate a corresponding attack in their *exploit kits* in order to then attack devices that have not yet been patched. This typically occurs in a matter of a few days. Individual *exploit kits* even have *zero-day exploits* that take advantage of previously unknown vulnerabilities and are used for attacks on devices. Consequently, MELANI recommends that home users and SMEs should activate automatic updates and larger companies should implement very swift patch management with clearly defined processes that are prioritised.

4.10 Vulnerability in mobile communication standard

In December 2014, experts working with the Berlin-based ICT specialist Karsten Nohl announced a security vulnerability in the mobile network which makes it possible to circumvent the encryption deemed secure in the *UMTS* network and thus intercept *SMS*s, for instance. The SS7 (Signalling System 7) protocol affected by the security vulnerability is used to exchange information between the individual telecom providers, for example to carry SMSs and calls across the various networks. The protocol itself dates from the 1980s and is therefore relatively old. Despite the fact that it has been upgraded twice to incorporate new functions, the main problem of inadequate authentication between the partners has never been eliminated. This did not represent a major problem when there was only a small number of large providers that both knew and trusted each other. Nowadays, however, there are many providers of varying degrees of trustworthiness on the global mobile telephone market, some of which sell SS7 access on to other companies.

Specifically, the security vulnerability presents attackers with the following different vectors of attack:

- Tracking a device:
  Every device is connected to the nearest network cell. To find the network cell currently used by a person to be monitored, the attacker only needs to know that person's mobile phone number. The location of the network cell used can then be determined by looking up a database. In this way, a user can be located quite precisely in densely populated areas with many network cells. If the *International Mobile Subscriber Identity* (*IMSI*) and the global title (address used for routing calls) are known, there are other vectors of attack that also work if the provider blocks certain protocol functions.

[48] https://technet.microsoft.com/en-us/library/security/MS14-066 (as at 28 February 2015)
[49] http://blogs.cisco.com/security/talos/ms-tuesday-nov-2014 (as at 28 February 2015)

- Intercepting and tapping calls:
  When a device is connected to a foreign network, there are certain events which involve queries being made of the home network provider. If an attacker overwrites the data establishing where the device is directed to with his own address, the device will connect to the attacker's network. In this way, he can divert the calls to himself and tap them and thus carry out a *man-in-the-middle* attack without the victim noticing.

- Intercepting mTANs:
  Likewise, the updating of information regarding how to contact a certain device at a particular time is not authenticated and thus presents points of attack. In this way, an attacker can pretend that his victim is connected to his network by telling the home network provider this. The home network provider will then redirect calls or SMSs to the attacker's network. Using this method, an attacker can intercept a mTAN (SMS authentication for online banking), for example.

- Intercepting IMSIs:
  In order to notify a device of an incoming call, a temporarily assigned ID (TIMSI) is used, and this is sent unencrypted over the network. If this temporary ID is intercepted, it can be used to request the device's real ID (IMSI) from the telephone exchange. Knowing the IMSI gives the attacker further possibilities, such as finding out the real telephone number or requesting the key for the current connection's encryption.

It is relatively easy to put these attack scenarios into practice and it is highly likely that they are also being applied by governmental institutions and other similar agencies. For this reason, very sensitive information concerning company secrets, for instance, should not be exchanged using mobile networks, particularly if one of the partners involved in the conversation is abroad and roaming. MELANI is in contact with mobile network providers in Switzerland to ensure protection against these vulnerabilities insofar as possible.[50]

4.11 Vulnerabilities – in Mac OS X too

MELANI has found that bugs in the Mac OS X operating system are increasingly being exploited both for targeted attacks and for spreading malware in general. Like in Windows, this often involves vulnerabilities in Java or in browser plug-ins such as Acrobat Reader or Flash.

In recent months, two families of malware have attracted huge attention:

- iWorm[51] is a multipurpose *backdoor*. What is interesting is how the malware receives information about which command and control servers it should communicate with. For this, it uses messages posted by the attackers on the social news site Reddit to generate the URL of the current command and control server. iWorm is spread mainly via compromised pirated copies that are shared using BitTorrent software.[52]

[50] Source: Tobias Engel, http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2553/original/31c3-ss7-locate-track-manipulate.pdf (as at 28 February 2015)

[51] http://news.drweb.com/show/?i=5977&lng=en (as at 28 February 2015)

[52] http://www.thesafemac.com/iworm-method-of-infection-found/ (as at 28 February 2015)

- WireLurker[53] is a piece of malware that contains both a Mac OS X component and an iOS component. If the malware is activated on an OS X device, it waits until an iOS device (iPhone, iPad) has been connected via *USB*. The malware then harvests various sets of information (telephone numbers, iTunes Store information, etc.) and sends them to a command and control server. Because the USB connection is a trusted connection, the malware can pass itself off as a normal app. To do this, the app requires an enterprise certificate and a provisioning profile to sign the malware. This process requires a response from the user. If the user accepts, the malware is installed. This step is skipped in *jailbroken* devices. Enterprise certificates of this kind enable companies to install their own apps on their iOS devices. Like iWorm, the malware for OS X is spread via pirated copies of commercial software.

In addition to malware attacks, MELANI has also found that iTunes and iCloud accounts are increasingly being targeted by *phishing* attacks. This is a classic case of authentic-looking e-mails luring users into entering their login details on an attacker's server, thus giving the attacker access to the accounts.

In the device interface Thunderbolt, there is also a vulnerability that has been designed in particular for targeted attacks and should be taken very seriously.[54] This bug enables an attacker who has physical access to a device to directly modify the Mac computer's EFI *firmware* by plugging in a modified Thunderbolt device, such as a gigabyte adapter. Malware spread in this way is very difficult to detect, as it loads before the operating system and can thus completely hide from the operating system and any virus scanner. Apple has released a patch which fixes the bug at least for OS X Yosemite (10.10.2).

5 Trends/Outlook

5.1 Gathering and exchanging information in the age of big data

Already at the end of the last millennium, the belief that data and information were the new gold was gaining ground. Countless internet start-ups shot up, with business plans that often simply referred succinctly to the gathering of data and information as their source of revenue. The question of how precisely this was to be converted into money was deliberately overlooked. Consequently, there was a rude awakening on the markets when primarily losses were presented in addition to the vast amounts of information and data hoarded. The pioneering mood turned into what felt like a bad hangover and the dot-com bubble burst in March 2000 almost as quickly as it had formed. Around 15 years later, internet companies in particular appear to have done their homework. Either services are now paid for online or else personal data has to be provided in order to gain access to free offers. This is the case for Facebook, Google or Twitter, for example, which have meanwhile been making substantial profits from gathering and analysing data and information.

Seen in the positive sense, the collection of data and information makes it possible to analyse profiles, post personalised advertisements and offer clients services that are increasingly well tailored. In their own interpretation of the facts and in a bid to provide the

[53] https://www.paloaltonetworks.com/resources/research/unit42-wirelurker-a-new-era-in-ios-and-os-x-malware.html (as at 28 February 2015)

[54] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4498 (as at 28 February 2015)

product security in a rational manner, certain intelligence services like to point out that it is necessary to have the whole haystack in order to find the needle (generally terrorism). Even at the international and intergovernmental level, the collection of data and information and the exchange of what has been collected are increasingly being seen as a sort of panacea in the fight against excesses in the area of tax evasion, for example, or with a view to the effective international alignment of wanted lists. However, it can be assumed at least in the case of the state collection and analysis of personal data, as well as its exchange at the international level, that the legal framework is very strict, which is far from the case with private-sector activity.

Whatever the case, this trend is doubly problematic. Firstly, centralised collections of data and information constitute a key point of attack. Not surprisingly, the quantity of data stolen during attacks on companies has been rising consistently. While the theft of a few thousand e-mail addresses made the news a decade ago, an incident today probably has to involve millions, including the associated passwords, in order to draw attention. It should not come as a surprise that in certain places there can be the theft of data that the actual data owner did not even give the company directly. As it happens, there is a flourishing trade in such information and data. This is generally with the implicit authorisation of the owner, who once upon a time accepted the general terms and conditions or a data protection provision so as to finally be able to order a much-desired book or create a social media account. The principle that a chain is only as strong as its weakest link applies very much to the technical security of data storage. No matter how precise or strict an agreement or contract on how data can be collected and exchanged technically is, it cannot ultimately be ruled out that the data will eventually end up in the wrong hands. This applies not only to the private sector; it also concerns state institutions, as demonstrated by the hacking of the Schengen Information System (SIS) in Denmark.[55]

Secondly, there is the question of the intended use of this enormous volume of data. In the private sector, it can be assumed that primarily commercial considerations play a role. By transmitting data, the owner hopes to gain an advantage. Consequently, it can make perfect sense to give a third party access to data in order to receive the most appropriate offers in return. It is another story if this data also has to be transmitted to a country's security authorities. The question of the intended use also has to be asked in the intergovernmental area. While it may be perfectly reasonable to simplify the fight against tax evasion with the automatic exchange of information, it is also a matter of urgency to set out how precisely this information will then be used in the recipient states. For example, Switzerland lobbied strongly within the OECD for the automatic exchange of information to focus not only on the type of data to be collected but also on the area of use. Apparently, there can be no guarantee that the partner state will stand by its commitments, as shown by a Federal Administrative Court ruling of 2014.[56]

In this case, where a Swiss citizen was suspected of insider trading, the Pakistani authorities asked the Swiss Financial Market Supervisory Authority (FINMA) for administrative assistance in the summer of 2012. FINMA granted administrative assistance, whereupon the accused Swiss citizen submitted an appeal to the Federal Administrative Court, explaining in essence that the competent Pakistani authority was unable to ensure compliance with the principle of speciality and confidentiality. As it happens, internal e-mails of the Pakistani authority as well as the internal communication between the authority and FINMA were then

---

55 MELANI Semi-annual report 2013/2, Chapter 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=en (as at 28 February 2015).

56 http://www.bvger.ch/publiws/download;jsessionid=F01EA73D27D15FF364A9203975D0B648?decisionId=f736b6ed-38ba-4d10-bf8f-c0312d05030f (as at 28 February 2015)

also passed on to the Pakistani press and provided evidence of the violation of official secrecy. FINMA immediately suspended the administrative assistance procedure.

The development of big data with all of its pros and cons raises not only questions concerning technical security and the responsibility of the operators of such collections of data, but also fundamental questions on due diligence in the area of the analysis and use of this data. The main people concerned here are all those who voluntarily make their data available and have to be clearly aware of what precisely happens to their data. However, state authorities also have a role to play in that they have to ensure that lawfully collected and transmitted data is genuinely used only for the purpose originally intended. The development of effective audit and control processes to ensure this will undoubtedly be one of the biggest challenges in the near future.

5.2 Complete connectivity: smart and safe?

The internet – the network of networks – connects ICT systems and allows information and data to be transferred. However, it is not comprised solely of the World Wide Web, which enables people to visit websites. As a global telecommunications infrastructure, the internet also enables people to communicate with machines and give them instructions that then have an impact on the physical world. Meanwhile, machines are also able to interact with one another – provided of course that they have been duly programmed (up to now). Communicating microcomputers are playing an increasingly important role in various areas of life. The recording of statuses by sensors and the execution of commands by actuators to achieve a specific effect allow for the extensive automation of processes to support people not only in the virtual world anymore, but now also in the physical world.

This trend has seen the creation of various terms such as internet of things, pervasive computing, ubiquitous computing and wearable computing, and now telephones are not the only things to have gone "smart": we also have smart cars/smart drive, smart homes and smart buildings, not to mention smart factories/smart manufacturing[57] that can collect, receive, process and send data, as well as use it to derive commands and execute specific actions.

The success of the technology underlying the internet and the need for interoperability mean that more and more applications that require the exchange of data are based on internet protocols. That is why the home automation sensors and actuators in smart homes are integrated into the home's WLAN, as this infrastructure already exists and the inhabitants want to be able to control their home with their smartphones, which are likewise already connected to the home network. This inevitably leads to interfaces between the internet, designed for the global exchange of data and information, and local devices such as heating temperature sensors or networked light bulbs in the living room. Whereas it may be practical to be able to use a smartphone to turn on the heating and hot water heater in a holiday home before arriving, it would appear significantly less useful to be able to turn lights on and off when not at home, let alone put up and down a home cinema screen. Although the manufacturers only very rarely propose home automation functions based on the internet (preferring to use the home network), such possibilities exist at least in theory.[58] However, all of these systems have to be protected not only against attacks from the internet, but also

[57] In its high-tech strategy, Germany's federal government talks about "*Industrie 4.0*", according to which the computerisation of the manufacturing industry should be promoted: http://www.bmbf.de/de/9072.php

[58] See also MELANI Semi-annual report 2013/2, Chapter 5.5; Attacks on home routers: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=en (as at 28 February 2015)

against local threats. Aside from the WLAN, other wireless interfaces (e.g. *Bluetooth* or *NFC*) can also be used as gateways if they are not used correctly and secured.

With regard to users, the smartphone is increasingly being used as the main identification and operating device as well as a tool for collecting and analysing data. This can be seen very clearly in the newly fashionable health apps, for example. Hence, due account has to be taken of smartphone security for data protection and security reasons. Moreover, consideration should also be given to the best way to proceed if a smartphone is compromised or lost in order to prevent misuse by unauthorised persons and to transfer the usual functions and data to a replacement device without any loss.

Despite all the conveniences offered by a "smart" environment, people should not forget to take a critical look at the collection, processing and storage of data and consider if and how they would manage without small connected accessories and also if they could do still things manually, for example in the case of a smart toilet[59] that will not flush until the toilet paper has been replaced or because the internet is down. Finally, it is necessary to think about the risk of unauthorised third parties maliciously tampering with physical processes controlled remotely via networked IT resources. Someone who is perhaps acting merely to get mischievous glee out of the inconvenience caused could actually trigger serious problems or third parties could even use their control over devices and services to blackmail the legitimate users.

5.3 Various forms of blackmail

Of the various methods used by criminals to make the most of their attacks, there is one which has seen a spectacular increase in popularity in recent years: extortion. Criminals are increasingly seeking to extort money, usually by using the victim's data as leverage.

One way of operating is to access sensitive data in order to blackmail the victim, threatening disclosure, i.e. the data will be published if a certain amount of money is not paid. Several cases like this targeting companies were reported during the six months under review. Examples include the actions of the Rex Mundi group of hackers, which operated in an identical manner to claim several victims. An *SQL injection* on the company's website firstly makes it possible to access a database, typically one containing information on clients and their exchanges with the company. The pirates then contact the targeted company, stating that the stolen data will be published if a payment is not made. There have also been reports of more sophisticated attacks that likewise have the ultimate aim of blackmailing and threatening the disclosure of sensitive information. One such example is the attack on Sony Pictures Entertainment, which is discussed in Chapter 4.1 of this report. In these cases, the criminals hope that the risk of damage to the company's image will prompt it to pay up in order to prevent the leak from going public.

While threats based on data confidentiality breaches are used as leverage to obtain money, an even more salient trend that concerns primarily individuals involves ransomware, which restricts access to data. The different families of ransomware, from the first cases where victims' computers are blocked to CryptoLocker and its variations which encrypt data on infected machines, are proving to be an inexhaustible source of income for criminals. Many experts agree that this trend will be a lasting one. The main reason they are successful is

[59] http://www.heise.de/newsticker/meldung/31C3-Hacker-nehmen-vernetzte-Toiletten-ins-Visier-2507287.html (as at 28 February 2015)

victims' propensity to pay to regain access to their data or computer. This appears to be high according to a study by the University of Kent, which found that 40% of CryptoLocker victims agreed to pay a ransom to recover files[60]. For the criminals, therefore, it is not the intrinsic value of the targeted data and the possibilities of selling or using it that counts, but rather the value that victims place on their data, which determines their decision to pay in the hope of recovering it. Consequently, when individuals forget about protecting their personal data on the grounds that it is of no value for a potential attacker, their logic can be dangerous. Once data is of value (even if it is only emotional) for the user, it also becomes valuable for a potential blackmailer.

In the future, many other areas may be explored by the criminals behind these techniques for exacting ransoms. A recent example draws attention to the possibilities for attackers to target insecure websites. In this case[61], the modus operandi involved encrypting the website's database and then demanding a ransom from the administrator to recover access to the data. Another worrying prospect is linked to the development of the internet of things and the networking of growing numbers of devices, which would appear to offer endless attack options to potential blackmailers. Any household control system, tool or device whatsoever that is connected to the internet can in fact be attacked. It is quite possible to envisage scenarios in which criminals seek to make a household appliance inaccessible and then demand money from the victim in order to be able to use the appliance again. Even if in many cases there could be ways for the victim to unblock the appliance himself or simply activate its "physical" operating mode, the inconvenience caused and the lack of know-how could nonetheless cause many people to pay up, especially in the case of small sums of money.

These topical examples and the prospects suggested highlight just how important it is not to neglect the attacks conducted from an availability standpoint. With regard to the classical trio of confidentiality, integrity and availability, people frequently tend to focus on confidentiality when current attacks are mentioned, as well as when evaluating new products and services. However, it is worth bearing in mind that attacking the availability of data or services is a highly profitable exercise for criminals, particularly by targeting the user. This aspect is already very topical with the different types of ransomware circulating, but it is likely to increase with the growing networking of various services and devices. Therefore, the concerns about them should not regard solely the problem of the user's personal data that could be accessed and used, but also the possibility of making such services inaccessible for ransoming purposes.

5.4 Satellite navigation in aviation

The *Global Positioning System* (*GPS*) is a global navigation satellite system for determining position and measuring time. The latitude and longitude of one's position can be transmitted via a receiver. GPS receivers can be found almost everywhere nowadays, such as in smartphones, digital cameras and cars. Increasingly, satellite navigation is also being implemented in safety-related applications as well.

An example worth looking at here is civil aviation. On 17 February 2011, for instance, the Federal Office of Civil Aviation (FOCA) for the first time in Switzerland approved a procedure

[60] http://www.kent.ac.uk/news/science/528/cryptolocker-victims-pay-out (as at 28 February 2015)

[61] https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html (as at 28 February 2015)

for satellite-supported landing on North Runway 14 at Zurich Airport.[62] Together with the air traffic control company Skyguide, the airport operator introduced satellite-guided take-off on Runway 34 on 18 October 2012. This was the first time in Switzerland that the departure procedure defined a radius for the turn to be made. Then on 14 October 2014, a Swiss plane performed the first landing at Zurich airport using a satellite-supported precision approach system.[63] However, it is not planned to upgrade the entire fleet with this new technology until most of the airports served are equipped for satellite-supported approaches.

Despite these developments, it should not be forgotten that satellite navigation was not developed specifically for use in civil aviation, and it can easily be interfered with either intentionally or unintentionally. Think back to the malfunctions suffered by the GPS system at Newark Airport. After several months of investigations, it turned out that the malfunctions were caused by a truck driver who regularly stopped near the airport and had a *GPS jammer* with him.

Therefore, the existing GPS signals cannot be used on their own. It is necessary to have a second system that monitors the integrity of the data and identifies breakdowns or manipulations. Moreover, the normal GPS signal with a specified accuracy of 9 to 17 metres is not precise enough for precision approaches. External factors such as ionising radiation as well as a change of GPS satellite can also lead to deviations. The additional procedure used in Zurich is called a Ground-Based Augmentation System (GBAS). Four reference stations whose precise position is known can calculate the differential correction to be applied to the "normal GPS", in other words the error rate of the current GPS signal. This differential is then radioed to the aircraft.[64] Special attention is paid to secure transmission of the differential correction, particularly in terms of data integrity.

Another flight navigation system used in Europe is the European Geostationary Navigation Overlay Service (EGNOS).[65] Here too, reference points throughout Europe increase the precision of the GPS signal and check its integrity. If the GPS system sent out false data, the error would be detected within six seconds and forwarded to the pilot. The differential correction is transmitted to aircraft via geostationary satellites in this case. The signal is also sent over the internet. Existing GPS receivers can receive and interpret the signal. The error is thus significantly less than ten metres. EGNOS is a joint project of ESA, the European Commission and EUROCONTROL, the European Organisation for the Safety of Air Navigation, and is a precursor to Galileo, the satellite navigation system being developed in Europe. It is less expensive than GBAS, as no additional technology has to be installed on the ground. Aside from its greater precision, its main difference relative to GPS, which is operated by non-European states, lies in the fact that it is controlled by the aforementioned operators and the signal quality can be monitored constantly.

In the case of EGNOS, the correction signal is transmitted by geostationary satellite to aircraft and can be received publicly. EGNOS is nothing more than an extension and refinement of the existing GPS signal. Just like the GPS signal, it is difficult to manipulate, but manipulations cannot be ruled out entirely, as is the case for any technical system.

---

62 MELANI Semi-annual report 2011/1, Chapter 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=en (as at 28 February 2015)

63 http://www.swiss.com/corporate/de/medien/newsroom/medienmitteilungen/medienmitteilung20141015 (as at 28 February 2015)

64 http://www.skyguide.ch/fileadmin/user_upload/publications/Factsheets/1201_Factsheet_Satellitennav_System e_Verfahren_de.pdf (as at 28 February 2015)

65 http://www.esa.int/Our_Activities/Navigation/The_present_-_EGNOS/What_is_EGNOS (as at 28 February 2015)

Security and safety depend on the individual components and their producers, and are the top priority. Companies that supply EGNOS components have to meet special security requirements. Consequently, Swiss companies that wish to be involved in the Galileo and EGNOS programme are checked by security experts from the Federal Department of Defence, Civil Protection and Sport (DDPS). [66]

Modern ICT systems continuously give rise to new desires, also in domains where safety is the top priority. In many cases, it is a matter of modernisation or using systems that can be operated in a more efficient and resource-neutral manner. However, the desired efficiency gains should be included in a risk assessment and be weighed up against security and safety considerations. On the other hand ICT systems can be a valuable complement to older systems. The challenge for using such systems does not lie only in the integrity of the data transmitted, however, but also in the systems' availability. A GPS signal disruption means that approaching aircraft have to land using alternative systems that are available. This is not a problem as long as the landing regimes do not make a distinction between the available systems or alternative systems such as the instrument landing system (ILS) are still available. In the case of airport-specific landing systems, disruptions would be limited to the airport in question, as is the case with an ILS. In contrast, an EGNOS outage would have repercussions for air traffic throughout Europe.

5.5 Security vulnerabilities – responsible disclosure

Directly or indirectly, internet users are constantly exposed to security vulnerabilities of one sort or another. The average user is mainly aware of vulnerabilities in Microsoft products as well as Acrobat Reader and Flash Player. Vulnerabilities concerning security or encryption components also make the headlines. The most well-known example is the Heartbleed *vulnerability*, which was discussed in the last semi-annual report. Regarding the period under review, the Poodle and Kerberos bugs are worthy of mention (see Chapter 4.9). According to the database of all publicly known program vulnerabilities maintained by MITRE Corporation, a total of 7,945 vulnerabilities were recorded worldwide in 2014, which was the highest number ever.[67] In reality, the range is much bigger altogether, going from vulnerable websites to incorrect configurations, which are not included in this database. It can thus be assumed that virtually every software program in use has a bug of one form or another. Based on this development, the question increasingly having to be asked concerns the processes to be followed when security vulnerabilities are detected.

For example, most internet users believe that someone who finds bug information passes it on to the corresponding company (for free) so that it can make an update available as soon as possible. However, the security business market is extremely competitive and dealing with security-related information is always a balancing act. Different interests are at play, including financial ones of course. Finding a vulnerability involves a certain value; the finder plays a role that should actually be performed by the manufacturer during quality control. It can be assumed that various companies actively perform targeted searches for security vulnerabilities in programs in order to make a profit. An example of this that made the headlines in 2012 concerned the Maltese company ReVuln, which specialised in selling information on previously unknown security vulnerabilities in SCADA products to governments and other "paying clients" rather than reporting them to the affected software

66 https://www.news.admin.ch/message/index.html?lang=en&msg-id=53264 (Stand: 28. Februar 2015).

67 http://cvedetails.com/browse-by-date.php (as at 28 February 2015)

vendors.[68] This can be a lucrative business precisely in the area of critical infrastructure, as the pressure to ensure flawless operations is particularly high here and governments are obliged to ensure the security of these critical systems. With this form of commercialisation, however, there is the inherent danger of security vulnerabilities not being eliminated for cost reasons and of paying criminals getting their hands on vulnerability information. Moreover, by paying for vulnerability information, governments run risks that we were aware of even before the publication of the Snowden documents. Already in 2012, Chaouki Bekrar, CEO and lead hacker at the security firm Vupen, stated in an interview that his company would not share the security vulnerabilities found in the Chrome web browser with Google for a million dollars and would instead sell them to its clients, specifically NATO partners and NATO governments.[69]

At the same time, however, certain security bugs are not taken seriously by the software vendors, which is frustrating for those who find them. Until the vulnerability is publicly known, some manufacturers see no reason to eliminate it promptly. It has turned out in many cases that the manufacturer was aware of the bug already months before it became public knowledge but yet failed to do anything about finding a solution in the meantime. This is potentially frustrating for people who find bugs. To step up the pressure, they threaten to publish the vulnerability on a certain date in order to force the manufacturer to act quickly. In the worst-case scenario, the security bug is published without a corresponding update being available.

While the first problem area could be solved only with state regulation, if anything at all, the second one is certainly solvable. For example the National Cyber Security Centre (NCSC) in the Netherlands has published a guideline on how reporters and victims of vulnerabilities should proceed. In this regard, the NCSC acts as an office to which the vulnerabilities discovered can be reported. Incident reporters are instructed not to publish the information. In return, they are assured that the seriousness of the vulnerability report will be assessed within three working days and that the expected problem resolution date will be set. Moreover, they are kept abreast of the progress made on eliminating the problem. Once the bug has been published, the incident reporter gets the credits and at least a t-shirt.[70]

68 http://www.computerworld.com/article/2493333/malware-vulnerabilities/security-firm-finds-scada-software-flaws--won-t-report-them-to-vendors.html (as at 28 February 2015)

69 http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/ (as at 28 February 2015)

70 https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html (as at 28 February 2015)

5.6 Items of political business

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Po	14.3739	Control by design. Strengthen property rights in the event of undesirable connections	Schwaab Jean Christophe	17.09.2014	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143739
Po	14.3782	Digital death rules	Schwaab Jean Christophe	24.09.2014	NC	FDJP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143782
Ip	14.3884	Intentions of various power companies to sell their shares in Swissgrid	Killer Hans	25.09.2014	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143884
Fr	14.5642	Internet services. Splitting of dominant groups in the case of quasi-monopolies	Glättli Balthasar	03.12.2014	NC	EAER	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20145642
Ip	14.4138	Procurement practices for critical ICT infrastructures of the Federal Administration	Noser Ruedi	10.12.2014	NC	FDF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144138
Ip	14.4123	Development of the ICT infrastructure. Create a more favourable environment for investments	Guhl Bernhard	10.12.2014	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144123
Ip	14.4194	Big data. Potential and development prospects of the data economy in Switzerland	Graf-Litscher Edith	11.12.2014	NC	FDHA	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144194
Po	14.4294	Web index for a free and open internet. Switzerland is only ranked 18	Glättli Balthasar	12.12.2014	NC	DETEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144294

6 Glossary

0-day Exploits	An exploit which appears on the same day as the security holes are made public.
Active Directory	Active Directory (AD) is a directory service for Microsoft Windows Server operating systems.
Advanced Persistent Threat	This threat results in very great damage impacting a single organisation or a country. The attacker is willing to invest a large amount of time, money and knowledge in the attack and generally has substantial resources.
Backdoor	"Backdoor" refers to a software feature that allows users to circumvent the usual access control of a computer or of a protected function of a computer program.
Backup	"Backup" means the copying of data with the intent of copying them back in the event of data loss.
Black hat search engine optimization (BHSEO)	Search engine optimization (SEO) refers to techniques that are used to get higher search engine rankings for websites. Undesirable methods with regard to search engines are referred to as black hat SEO techniques.
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).
Botnet	A collection of computers infected with malicious bots. These can be fully remotely controlled by the attacker (the owner of the botnet). Depending on its size, a botnet may consist of several hundred to millions of compromised computers.
Brute force	The brute force method is a solution to problems that relies on trying out all possible cases.
Buffer overflow	Buffer overflows are one of the most common vulnerabilities in current software, which can also be exploited via the Internet.
Byte	A byte is a measurement unit in digital technology and IT that most commonly

	consists of eight bits.
Cloud	Cloud computing involves saving data in a remote data centre as well as executing programs that are not installed on the local computer.
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 Systeme (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".
Cookie	Small text files stored by a web page when viewed on the user's computer. For example, with the assistance of cookies, user preferences for a web site may be stored. However, cookies can also be abused to compile an extended user profile about one's surfing habits.
DDoS	Distributed denial of service attacks. A DoS attack where the victim is simultaneously attacked by many different systems.
Defacement	Website defacement is an attack on a website that changes its visual appearance.
Digital signature	A digital signature makes it possible to check the integrity of a message using the public key.
Ethernet	Ethernet is a technology that specifies software and hardware for cable data networks.
Exploit kits	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Firewall	A firewall protects computer systems by monitoring incoming and outgoing connections and rejecting them if necessary. A personal firewall (also called a desktop firewall), on the other hand, is designed to protect a stand-alone computer and is installed directly on it.

Firmware	Instructions stored in a chip to control a device (e.g. a scanner, graphics card, etc.). Firmware, as a rule, may be modified by upgrades.
Global Positioning System (GPS)	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
Global System for Mobile Communications (GSM)	The Global System for Mobile Communications (previously Groupe Spécial Mobile, GSM) is a standard for fully digital mobile networks, mainly used for telephony, but also circuit-switched and packet-switched data transmission and short messages.
GPS-Jammer	Device for disrupting GPS data.
Injection sql	SQL injection refers to the exploitation of a vulnerability in connection with SQL databases, resulting from insufficient verification of the variables to be transmitted. The attacker attempts to inject his own database commands, in order to change the data as desired or to gain control over the server.
International Mobile Subscriber Identity (IMSI)	The International Mobile Subscriber Identity is used in GSM and UMTS cellular networks to unambiguously identify network users.
Jailbreak	Jailbreaking is used to overcome the network restrictions on Apple products by using suitable software.
Keylogger	Devices or programs in operation between the computer and the keyboard to record keystrokes.
Malicious Code	Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses.
Man in the Middle	Man-in-the-middle attacks (MITM) Attacks in which the attacker infiltrates unnoticed the communication channel between two partners and is thereby able to spy on or even modify their data exchanges.
Message authentication code (MAC)	A message authentication code is used to provide integrity and authenticity assurances on data or messages.

Near Field Communication (NFC)	Near field communication is an international communication standard for the contactless exchange of data across short distances.
Network protocol	A network protocol is a communication protocol for exchanging data between devices in a computer network.
Network-attached storage (NAS)	Network-attached storage refers to an easy-to-manage file server.
Patch	Software which replaces the faulty part of a program with a fault-free version. Patches are used to eliminate security holes.
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.
Plug-in	(Additional) software that extends the basic functions of an application, e.g. Acrobat plug-ins for internet browsers allow direct display of PDF documents.
Point of Sales	A POS terminal (in Switzerland: EFT/POS terminal) is an online terminal for cashless payments at points of sale.
Proof of concept (POC)	Brief, not necessarily complete proof that an idea or method works. For example, exploit codes are often published as PoC so as to underline the effects of a weak point.
Ram Scraper	This malware manages to copy the data stored on the credit card's magnetic strip in the instant after it has been swiped at the point-of-sale terminal and is still in the system's random-access memory (RAM).
Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts or deletes data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
Removable storage device	An ejectable data carrier for computers that is not installed in a fixed manner and is usually portable.

Request	A client's request to a server in the client-server model.
Rich Text Format	The Rich Text Format (RTF) is a file format for texts.
Roaming	GSM roaming refers to the ability of a cellular network user to access mobile phone services on a foreign network.
Router	Computer network, telecommunication, or also Internet devices used to link or separate several networks. Routers are used, for instance, in home networks, establishing the connection between the internal network and the Internet.
SCADA-Systems	Supervisory Control And Data Acquisition System. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
Search engine ranking	Ranking of several comparable items based on a search engine query, whereby the position indicates a rating.
Security gateway	A security gateway is an umbrella term covering all ICT systems that ensure ICT security in an organisation.
Security holes	A loophole or bug in hardware or software through which attackers can access a system.
Session	A session refers to a client's connection established with a server.
Session hijacking	Session hijacking refers to the exploitation of a client's established connection with a server by an unauthorised third party.
Short Message Service (SMS)	Service to send text messages (160 characters maximum) to mobile phone users.
Smartphones	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.

Social networking sites	Websites for communication among users by means of personally designed profiles. Often, personal data such as names, dates of birth, images, professional interests, and hobbies are disclosed.
Source text	In computer science, source text (or source code) refers to the text of a computer program written in a programming language that humans can read.
Spam	Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Spear-Phishing	Targeted phishing attacks. The victim is made to believe that he/she is communicating via e-mail with a person they are acquainted with.
SSL	Secure Sockets Layer Protocol that provides secure communication on the internet. SSL is used today, for instance, in online financial transactions.
Tor anonymity tool	Tor is a network for enabling anonymous communication. Tor protects its users from analysis of web traffic.
Two-factor authentication	For this at least two of the following three authentication factors are required: 1. Something you know (e.g. password, PIN, etc.) 2. Something you have (e.g. a certificate, token, list of codes, etc.) 3. Something you are (e.g. finger print, retina scan, voice recognition, etc.)
Universal Mobile Telecommunications System (UMTS)	The Universal Mobile Telecommunications System (UMTS) is a third-generation mobile communication standard for the exchange of data.
Universal Serial Bus Serial bus (USB)	Universal Serial Bus Serial bus (with a corresponding interface) which enables peripheral devices such as a keyboard, a mouse, an external data carrier, a printer, etc. to be connected. The computer does not have to be switched off when a USB device is unplugged or plugged in. New devices are for the most part automatically identified and configured (depending on the operating system).

Upstream provider	An upstream provider gives internet access to internet service providers (ISP) that they do not have themselves.
Drive-by infections	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.
WLAN	WLAN stands for Wireless Local Area Network.