Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

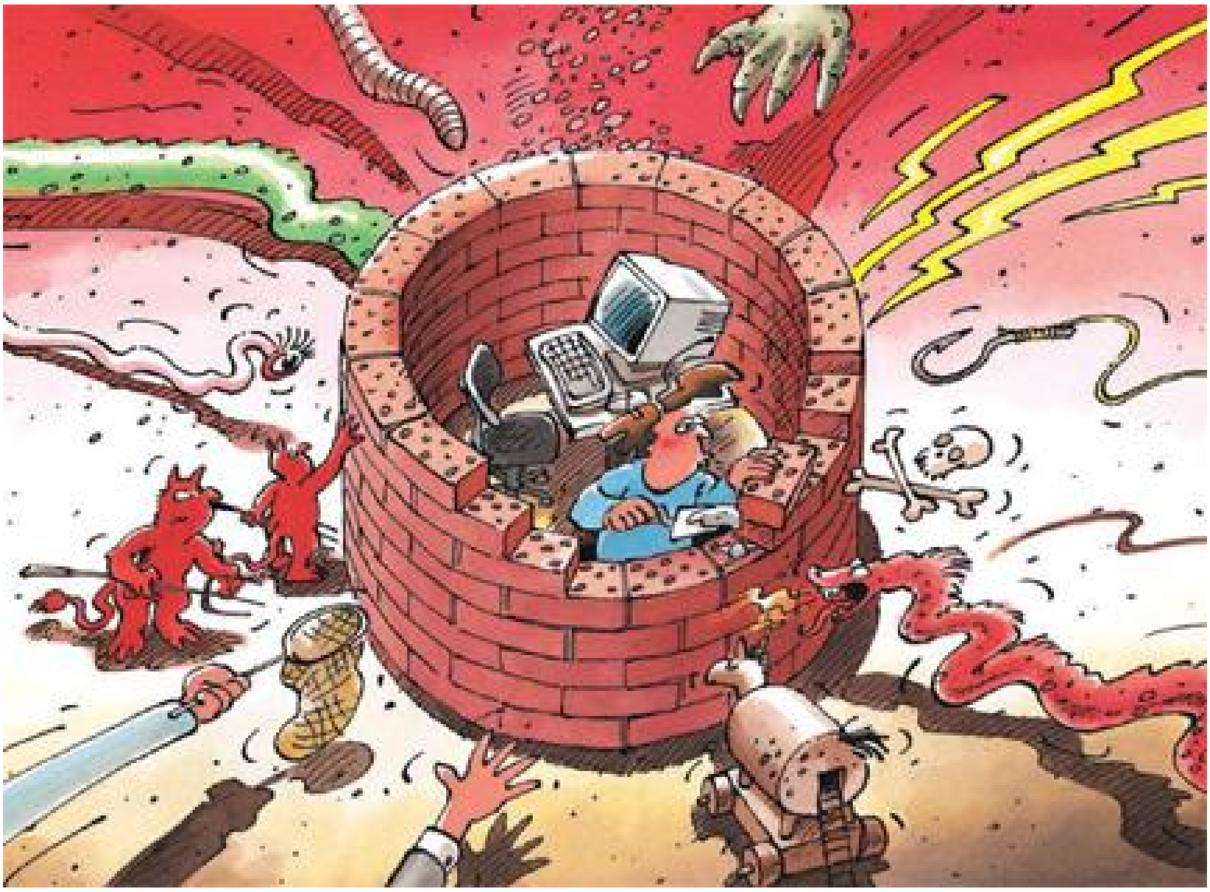
Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

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

Information Assurance

Situation in Switzerland and Internationally

Semi-annual report 2011/II (July – December)



Contents

1 Focus Areas of Issue 2011/II

- **Attacks on certificate service providers and their impact**

  In the course of an attack on DigiNotar, a Dutch certificate authority, more than 530 bogus certificates were issued, including for the domain windowsupdate.com, which is home to the update function for all Microsoft Windows products, and various Google domains.

  ► Current situation internationally: Chapter 4.1
  ► Trends / Outlook: Chapter 5.5

- **Cyberactivism**

  "Anonymous" once again caught the media's interest with various operations in cyberspace over the past months. But who exactly is behind "Anonymous"? According to numerous statements, "Anonymous" is not an organisation per se, but rather something more like an attitude to life. Support is not tied to any particular form: Every activist does what he or she believes to be right. This may in fact also lead to actions that do not enjoy broad support in the movement and thus provoke contradictory messages.

  ► Current situation internationally: Chapter 4.3
  ► Trends / Outlook: Chapter 5.2

- **"Good" and "bad" surveillance on the Internet**

  The analysis of the German law enforcement trojan (often referred to using the undifferentiated term "federal trojan") by the Chaos Computer Club triggered debates about its use not only in Germany, but also in Switzerland. Additionally, WikiLeaks began to publish numerous documents on 1 December 2011, which are purported to show that private security companies are selling ICT solutions to states with predominantly autocratic governments and lack of respect for human rights. This debate, which is in fact old but has been rekindled, arises from one of the fundamental problems of the Internet, the networked society, and ICT. The emergence of new options all the time to communicate, to exchange data and information, and to make them available everywhere and always, has consequences: The measures to locate and obtain information, and generally the work of the security authorities of a state, are becoming much more complicated.

  ► Current situation internationally: Chapter 4.7, Chapter 4.8
  ► Trends / Outlook: Chapter 5.3

- **Phishing, fraud and ransomware on the rise**

  A new phenomenon observed in Switzerland since summer 2011 is calls by scammers who pretend to be employees of Microsoft customer service, in order to gain access to computers. Phishing has also increased heavily in the last 6 months and is targeting primarily e-mail providers and credit card companies. To keep fraudulent websites active for as long as possible, criminals are trying new methods intended to make it more difficult to shut down phishing sites. At the beginning of November, ransomware was disseminated, claiming to be from the Federal Department of Justice and Police.

  ► Current situation in Switzerland: Chapters 3.1, 3.2, 3.3, 3.4, 3.5

2 Introduction

The fourteenth semi-annual report (July – December 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 second half of 2011. Chapter 3 discusses national topics, Chapter 4 international topics.

Chapter 5 includes in-depth analyses and trends on current topics.

3 Current National ICT Infrastructure Situation

3.1 Calls by scammers claiming to be employees of Microsoft customer service

Recently there has been an increase worldwide, and also in Switzerland, of calls by scammers claiming to be employees of Microsoft or other ICT support companies. The callers generally speak English and claim to be from the United States, England or Australia. In many cases, the callers refer to error messages that supposedly had been transmitted by the computers of the contacted business or individual. The persons called are, for instance, told to launch the *Event Viewer*[1], which can be used to display all events and activities running on the computer. It should be noted in this regard that even a perfectly functioning system may on occasion generate error messages. Depending on the age and configuration of the computer, the list of error messages in the Event Viewer may even be very long, although the system does not have any fundamental problems. The launch of this programme is generally used by the "support" callers to present a credible backdrop for the victims and to scare them. The scammers' goal is to convince the persons called that they should download a programme, thereby giving the scammer remote access to the computer. Once this access is granted, the caller has the same options to manipulate the computer as if he were sitting directly at the computer (copy/change/delete data, install programmes, set up a "*back door*" to access the system at a later time, etc.).

Sometimes, the callers also offer to set up a support subscription or a guarantee and ask for credit card data or other form of payment for that purpose.

The callers apparently look for victims using public directories, such as the Swiss Commercial Register or public telephone books.

In principle, it should be noted that Microsoft never makes unannounced or unrequested support calls to remedy computer problems. More on this topic is available on the *blog* of the security advisor of Microsoft Switzerland.[2]

If the callers have in fact been given access to the computer, it is recommended to have the computer examined and, where necessary, cleaned by a specialist. But even this doesn't guarantee that *malware* can be found or that manipulations can be discovered.

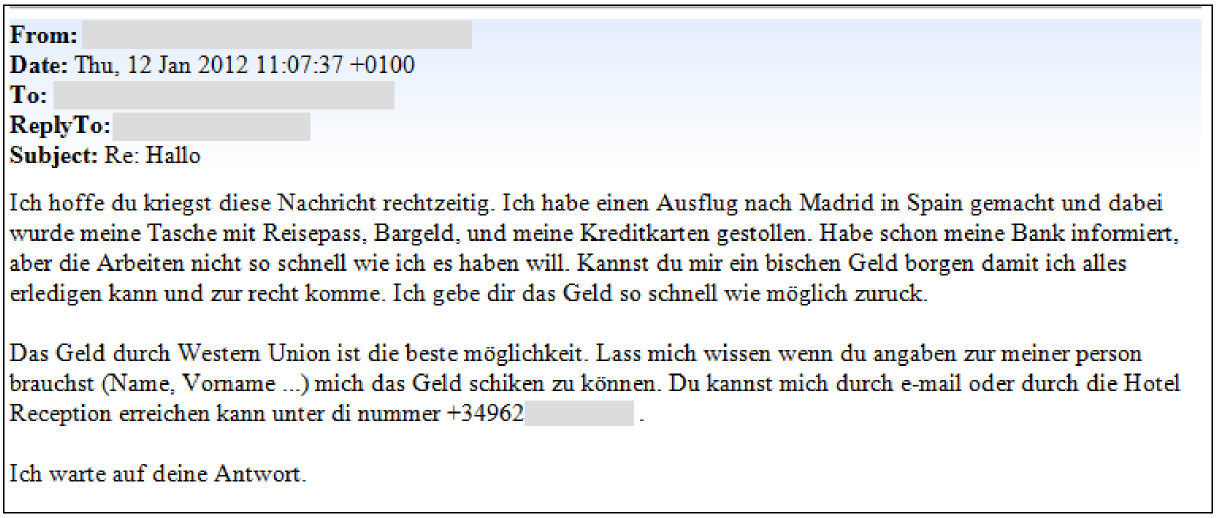
The most secure method is to delete the computer's hard drive completely and to reinstall the operating system. This is one of the reasons why it's so important to regularly make a *backup* off all important data on an external storage medium, so that these data are not lost if problems arise with the computer.

[1] a Windows system programme

[2] http://www.retohaeni.net/2011/07/microsoft-does-not-call-you/ (as of 23 February 2012).

3.2 Increase in hacked e-mail accounts

The Reporting and Analysis Centre for Information Assurance (MELANI) has increasingly received reports that e-mail accounts have been hacked. Typically, the criminals change the password and other personal information in the account (alternative e-mail address, mobile phone number, etc.), so that the rightful owner can no longer access it. Messages are then addressed to all contacts or targeted contacts from the account. Usually, these e-mails are bogus calls for help, according to which the sender is stuck somewhere abroad and all his money and his passport have been stolen. Finally, the recipient is asked to send money.



From: [redacted]
Date: Thu, 12 Jan 2012 11:07:37 +0100
To: [redacted]
ReplyTo: [redacted]
Subject: Re: Hallo

Ich hoffe du kriegst diese Nachricht rechtzeitig. Ich habe einen Ausflug nach Madrid in Spain gemacht und dabei wurde meine Tasche mit Reisepass, Bargeld, und meine Kreditkarten gestollen. Habe schon meine Bank informiert, aber die Arbeiten nicht so schnell wie ich es haben will. Kannst du mir ein bischen Geld borgen damit ich alles erledigen kann und zur recht komme. Ich gebe dir das Geld so schnell wie möglich zuruck.

Das Geld durch Western Union ist die beste möglichkeit. Lass mich wissen wenn du angaben zur meiner person brauchst (Name, Vorname ...) mich das Geld schiken zu können. Du kannst mich durch e-mail oder durch die Hotel Reception erreichen kann unter di nummer +34962[redacted] .

Ich warte auf deine Antwort.

Figure 1: Example of an e-mail sent from a hacked account.

In addition to inconvenience for the recipient, there are further nuisances for the e-mail owner, since he no longer has control over his account and can no longer access e-mails and contacts. This can be disastrous and have extremely unpleasant consequences in the real world if no *backup* of the data and contacts has been made and if all business contacts also are administered through the e-mail address in question.

Access to a third party's e-mail account of course also makes numerous other scams possible. Many services on the Internet can be accessed simply by entering a username and password. If the client forgets his password, it can be reset using the "Reset password" link. The new password is then sent by e-mail. An attacker who succeeds in hacking the e-mail account can use this service to access various services of the victim and use them for the attacker's own purposes.

Here are a few suggestions for how to minimise damage in the event of an incident.

1. Make a *backup* of the contacts so that an alternative e-mail address can be used in the event of an incident. In this way, contacts can be warned of scam e-mails as quickly as possible.
2. Careful selection of the e-mail provider, especially if e-mails are used for business purposes.
3. If an incident occurs, try immediately to regain control of the account. In rare cases, the alternative e-mail address is not changed: In this case, a replacement password can be sent to that address. But if the alternative address has also been changed, a *recovery process* must be initiated. Most e-mail providers make a recovery form available for this purpose. Here is a non-exhaustive selection of the most popular e-mail providers:

Google	https://www.google.com/accounts/recovery/
Hotmail/ Live	https://account.live.com/resetpassword.aspx
Yahoo	https://edit.europe.yahoo.com/forgotroot
GMX	http://www.gmx.com/forgotPassword.html

It's best not to let the account be hacked in the first place. Please see our recommendations on password use in this regard.[3] As a general rule, it should also be noted that no serious service provider will ever ask a client by e-mail to enter a password. For this reason, never click on a link in an e-mail to reach the site of a provider, financial service provider, credit card company, etc.. See our information on *phishing* in this regard.[4] Always exercise caution when asked to enter a password on a website. See also the following discussion in Chapter 3.3.

One should no longer only be critical in regard to e-mails from unknown persons, but also be cautious in the case of known senders. Where unusual events occur – especially when money is at issue – MELANI recommends verifying reachability by telephone, asking questions that only that person can answer to verify his or her identity, or discussing the credibility of the story with common acquaintances.

File attachments should not be opened carelessly or links clicked on even if they come from known senders – especially if the e-mail appears impersonal or no personal touch of the sender can be discerned in the message.

3.3 A holiday card to steal passwords

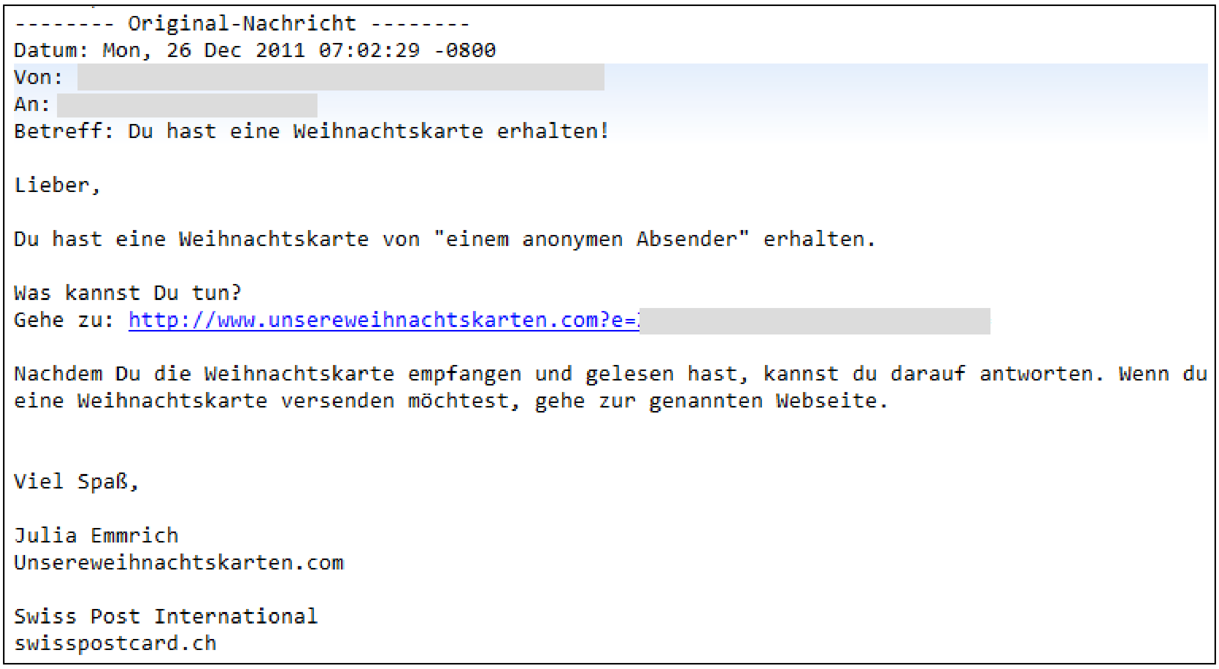
Sending and receiving electronic cards over the holidays is very popular. But not all electronic cards are reputable. Two especially professional scams were observed over the Christmas holidays that directly targeted Swiss victims.

In the first case, e-mails were sent in the name of Swisspostcard[5] with senders known to the recipients, inducing the recipient to click a link. The recipients were made to believe they'd received an electronic Christmas card, which could be downloaded from the website unsereweihnachtskarten.com.

[3] http://www.melani.admin.ch/themen/00166/00172/01005/index.html?lang=en (as of 23 February 2012).

[4] http://www.melani.admin.ch/themen/00103/00203/index.html?lang=en (as of 23 February 2012).

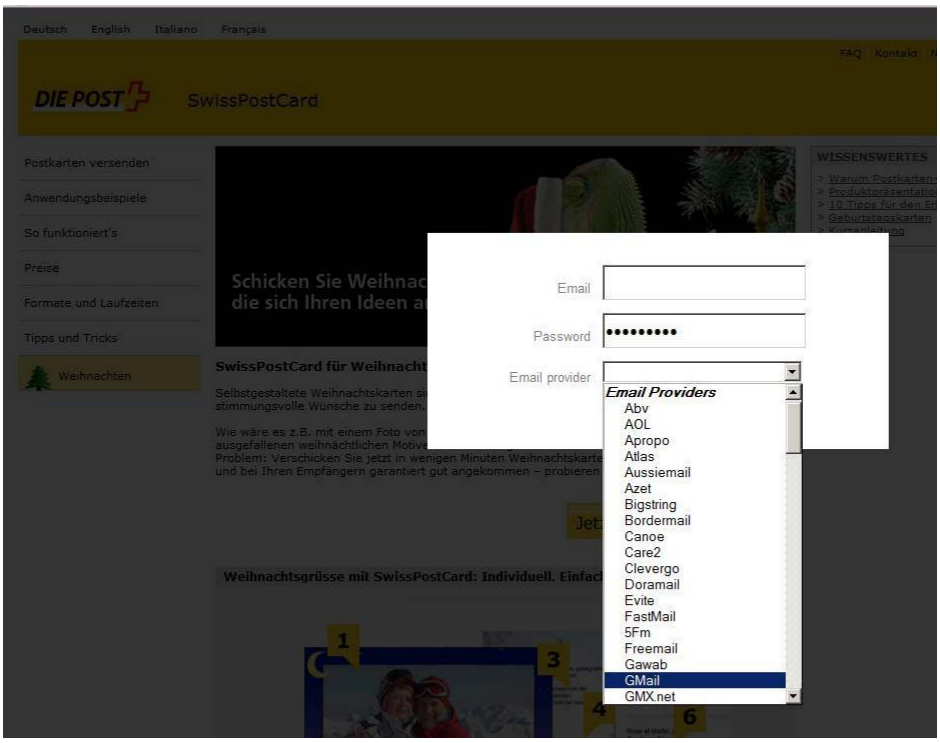
[5] Postcards can be prepared electronically using Swisspostcard (a service of Swiss Post). Swisspostcard physically prints the postcards and sends them to the desired addressee by regular mail.



```
-------- Original-Nachricht --------
Datum: Mon, 26 Dec 2011 07:02:29 -0800
Von: [redacted]
An: [redacted]
Betreff: Du hast eine Weihnachtskarte erhalten!

Lieber,

Du hast eine Weihnachtskarte von "einem anonymen Absender" erhalten.

Was kannst Du tun?
Gehe zu: http://www.unsereweihnachtskarten.com?e=[redacted]

Nachdem Du die Weihnachtskarte empfangen und gelesen hast, kannst du darauf antworten. Wenn du
eine Weihnachtskarte versenden möchtest, gehe zur genannten Webseite.


Viel Spaß,

Julia Emmrich
Unsereweihnachtskarten.com

Swiss Post International
swisspostcard.ch
```

Figure 2: Example of a phishing e-mail making the recipient believe that he has received a Christmas card.

A click on the link did in fact open the original Swisspostcard site in the background. In the foreground, however, a form was displayed asking the victim to enter the username and password of his e-mail account, in order to download the personalised Christmas card. The access data entered were directly sent to the scammers, who used them to access the e-mail account right away. *Phishing* e-mails of the same type were immediately sent to all contacts in the address book, in order to generate a snowball effect.



Email

Password •••••••••

Email provider

Figure 3: Phishing site loading the Swisspostcard page in the background and requesting e-mail access data in the foreground.

One week later, the attackers tried the same scam again. This time, however, the *phishing* e-mail wasn't sent in the name of Swisspostcard, but rather in the name of Fleurop.

In the first attack, it was possible to compile statistics on the number of hits. A total of 25,939 persons clicked on the link, of which 4,148 accessed the site several times, which indicates that they at least tried to enter their username and password. This corresponds to about 16%. Whether these persons actually did enter their username and password is unknown to us, however.

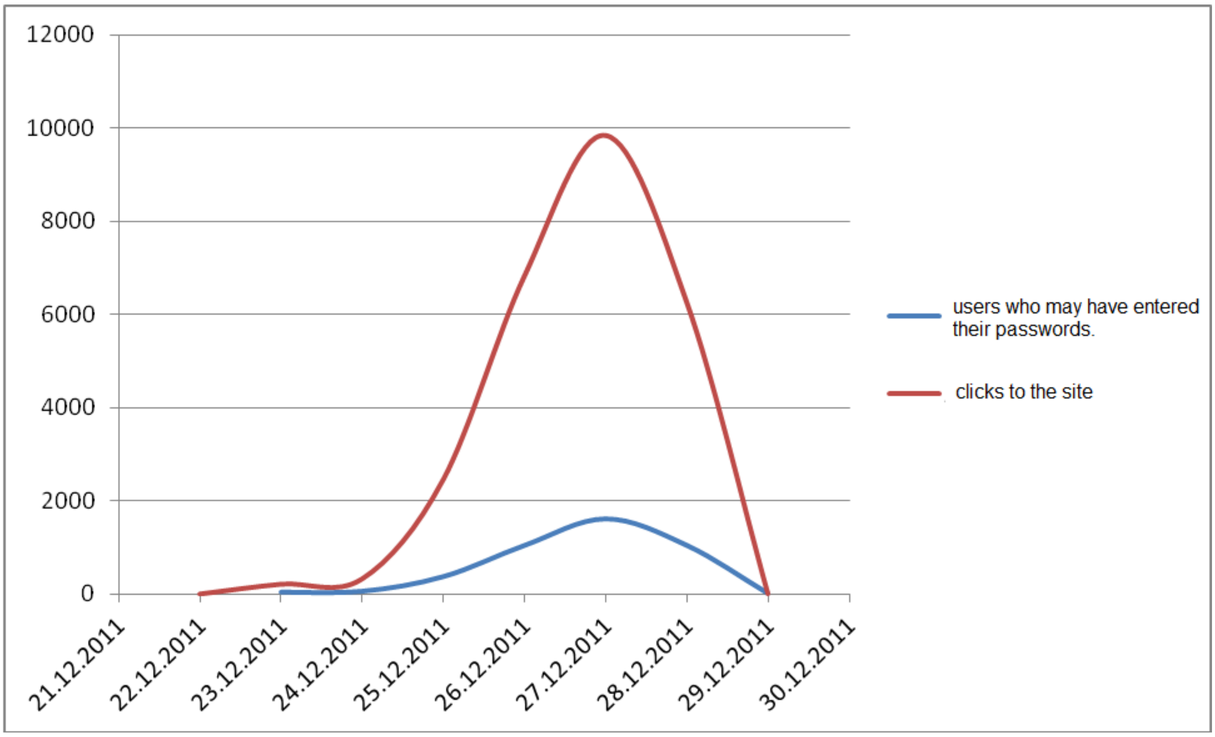


Figure 4: Hits on the phishing site "unsereweihnachtskarten.com". The red line represents the clicks to the site. The blue line represents the users who accessed the site several times and accordingly may have entered their user names and passwords.

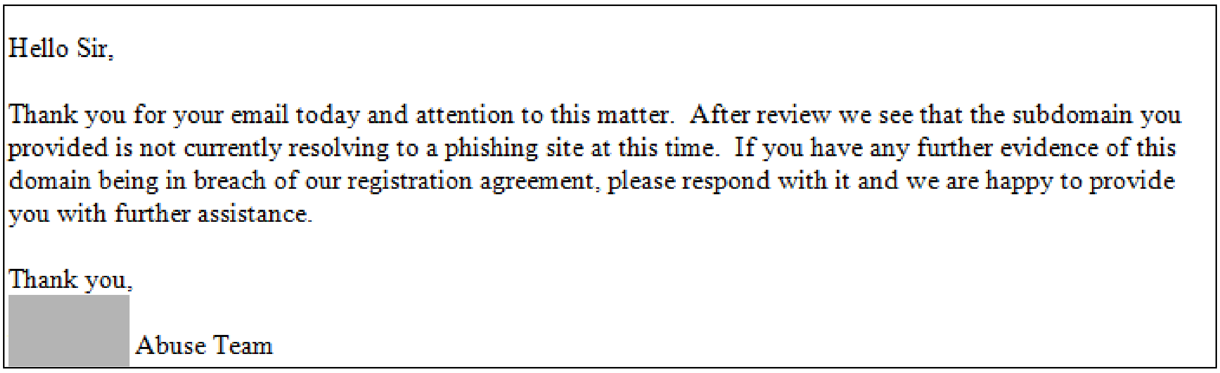
After only sporadic hits were recorded between 22 and 24 December 2011, which was certainly due to Christmas, the number surged on 25 December and reached its maximum on 27 December 2011. On 29 December, the site was shut down.

One should no longer only be critical in regard to e-mails from unknown persons, but also exercise caution in the case of known senders. One should always pay special attention if a website asks for a password.

3.4 Phishing attacks: Technical optimisation

Public authorities, private organisations and hosting providers are fighting against phishing attempts. Practically most of the phishing sites can now be deactivated within a reasonable period, "reasonable period" being defined as several minutes to one day. Criminals therefore try new methods to make it as difficult as possible for the authorities to shut down phishing sites.

In the case of the *phishing* attempt described in Chapter 3.3, for instance, the link was specially generated for each victim and was valid only once. Specifically, the e-mail address was encoded using *base64* in each link. If the initial link was clicked twice, an error message appeared. Also on the home page, nothing more than an error message was displayed. This made it more difficult to shut down the domain, since registrars/providers do not react without active proof by third parties. In requiring such proof, registrars/providers are assuming in good faith that the domain does not contain a phishing site. The following response by a registrar clearly shows this:



Hello Sir,

Thank you for your email today and attention to this matter. After review we see that the subdomain you provided is not currently resolving to a phishing site at this time. If you have any further evidence of this domain being in breach of our registration agreement, please respond with it and we are happy to provide you with further assistance.

Thank you,
[redacted] Abuse Team

Figure 5: Response by the registrar to MELANI's request to block the domain of the phishing site

Another variant that can be employed is to implement IP filtering (e.g. geo-restrictions). A phishing site is then only reachable from certain IP ranges. An error message is displayed to visitors with other IP addresses. Someone accessing the site from the "wrong" IP address is thus given the impression that the site has already been removed from the Internet.

It should be noted in this regard that most phishing sites hide behind entirely normal websites on a compromised webserver. Unlike scenarios in which a domain is used exclusively for criminal purposes, both the user and the hosting provider have the possibility here of deleting the website. Since the providers generally verify the sites only online and do not look for the fraudulent page in the directory structure of the *server*, the error message *"404 Not Found"* was until now a sure indication that the page had already been removed by the owner.

3.5 Now also in Switzerland: Malware blocking PCs and demanding payment

At the beginning of November, *malware* spread in Switzerland that blocked computers for the purpose of extortion. A window popped up with a message purportedly from the Federal Department of Justice and Police (FDJP). This message demanded that the computer user pay a fine of 150 francs because child pornography and other illegal material had been found on the computer. Of course, this message did not originate with any Swiss authority.

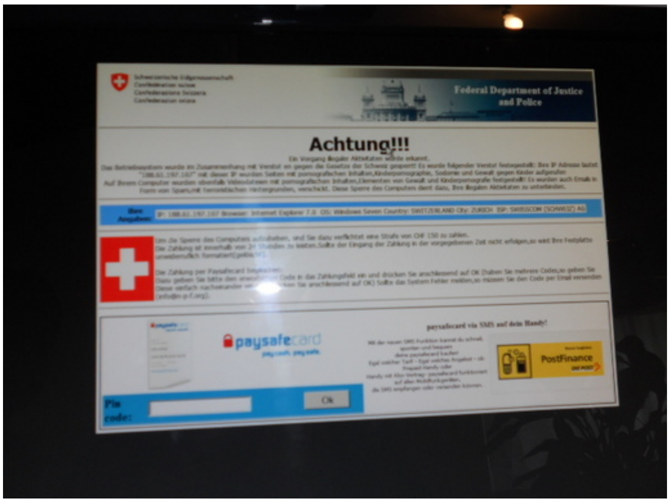


Figure 6: Screenshot of a computer infected with ransomware

Already in March and April 2011, *malware* was circulating that displayed a message on infected computers purportedly from the Federal Criminal Police Office of Germany. This message demanded payment of a fine of 100 euros, since illegal data had supposedly been found on the infected computer. The message said that if no payment was made, the computer would be blocked and the *hard disk* formatted. Also in other countries, similar versions of this *ransomware* – modified for the country in question – were observed.

If this message (or a similar message) is displayed, MELANI recommends scanning the computer with the latest antivirus *live CD* in order to remove the malware, or consulting a computer specialist. Additionally, if an infection occurs, the passwords used with the affected computer should be changed.

3.6 Politicians targeted by hackers

In the second half of the year, there were several incidents on the Internet targeting Swiss politicians or parties directly or indirectly. Politicians are especially publically exposed and thus offer more of a target.

During the Federal Council elections on 14 December 2011, for instance, a message was spread on Twitter, supposedly in the name of National Councillor Andrea Caroni, according to which Eveline Widmer-Schlumpf had been re-elected – even before the official election results had been announced. Although Andrea Caroni had nothing to do with this account, he had to demonstrate credibly that he was not the source of the *tweet*. He quickly set up his own Twitter account and sent out messages to that effect. This example shows that anyone can take on any role on the Internet and say whatever they want.

On 3 August 2011, the SVP website was again brought down by a denial of service attack. Already in November 2009, the websites of the Federal Council parties had been attacked and disabled prior to the popular vote of 29 November 2009 on the initiative against the construction of minarets. The other Federal Council parties were not affected by the recent incident, however.

National Councillor Chantal Galladé was confronted with a completely different problem. Since she failed to renew her domain chantal-gallade.ch on time, it was acquired by a third party, who used it to place advertisements. All attempts to contact the new owner failed. There was no response.[6] Ms Galladé has meanwhile registered a new domain. The advertisements have been taken down from the old domain – it is now for sale.

During a television interview, another politician showed his identity card to the camera. An unknown person took a screenshot, used it to make a "copy" of the ID, and tried to use the picture as proof of identity for the creation of a profile on a gay dating site. The dating site contacted the politician to check whether he really had set up a profile. When he said no, the profile was deleted immediately. Thanks to the good and attentive work of the dating site, the problem was nipped in the bud.

[6] http://www.tagesanzeiger.ch/zuerich/region/Warum-Chantal-Gallad-fuer-Bikinis-wirbt/story/15004208 (as of 23 February 2012).

3.7 Mass hacking of webshops

In August 2011, MELANI observed a surge in *website infections* of webshops, including numerous ones in Switzerland. Webshops using the osCommerce software were affected.

The attacks took place via an insufficiently secure *admin interface*. In older versions no administration access control was implemented. Instead of the use of a password, the folder with the administration panel was renamed with an obscure name and/or one have to secure the directory by creating a *.htaccess* file. htaccess ("hypertext access") is a configuration file of an Apache webserver in which directory-specific settings can be specified. Unfortunately, many users failed to do this. Consequently, administration access control was subsequently included to increase security in version 2.2RC2. As a result of incorrect implementation, however, this security feature could be circumvented relatively easily on an Apache webserver using *URL manipulation*.[7] This made it easy for the attacker to log into the administration and install *code* as desired. This was exploited on a massive scale in July/August 2011. The hacked shops were subsequently used to place *website infections*. According to the IT and tech channel gulli.com, up to 90,000 online shops were compromised by the attackers.[8]

Protection was possible in this case by securing the entire admin directory by creating a *.htaccess* file. This access control is carried out by the webserver itself and is independent of the login prompt of the shop software. Detailed instructions were published by heise.de.[9] Generally speaking, not only the server software, but also the installed applications, such as in this case the webshop, should be kept up to date, and all available security updates should also be installed.

3.8 Bogus websites of real estate companies advertise jobs for financial agents

After an e-banking scam, the attained money must be "laundered". For this purpose, *financial agents* are often recruited, for instance via online job listings. Sometimes, however, special websites are created that claim to be company sites with a "job vacancies" page or similar. These jobs all have the same purpose: Money must be received from unknown sources and forwarded to specific accounts. *Spam* messages are used to draw attention to these "job vacancies".

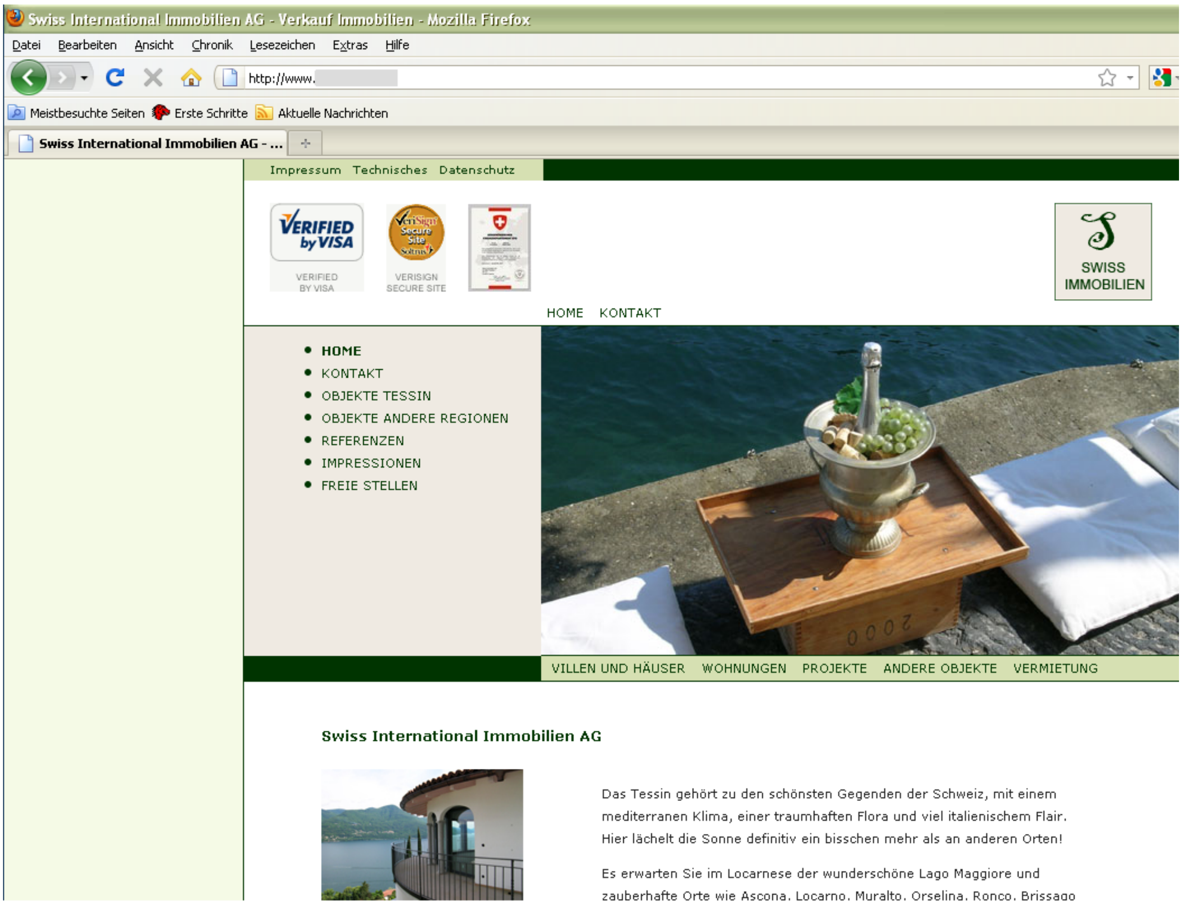
An especially brazen and persistent case of financial agent recruitment is currently being observed in Switzerland. Specifically, the information of companies is used which are entered in the commercial register, but do not have a website. Using this address information, the websites claim to belong to companies dealing in real estate in Ticino and looking for regional representatives to transfer client money. The sites look very professional.

[7] http://www.oscommerce.info/confluence/display/OSCOM23/%28A%29+%28SEC%29+Administration+Tool+Log-In+Update (as of 23 February 2012).

[8] http://www.gulli.com/news/16740-zahlreiche-online-shopping-websites-kompromittiert-2011-08-01 (as of 23 February 2012).

[9] http://www.heise.de/security/artikel/Schnellhilfe-fuer-osCommerce-Admins-1323536.html (as of 23 February 2012).

They are usually a 1-to-1 copy of the website of a third party company. The problem here is that the criminal motivation – unlike in the case of *phishing* websites, for instance – is not obvious. Normally, criminal websites are quickly deactivated by providers. In this case, however, it is difficult to get the provider to take down the website. If this succeeds nevertheless, it doesn't take long for an identical website to appear under a different domain. It seems to be the case here that a group of criminals has specialised in keeping these websites up and running for as long as possible, in order to recruit as many financial agents as possible.


Swiss International Immobilien AG - Verkauf Immobilien - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.[redacted]
Meistbesuchte Seiten
Erste Schritte
Aktuelle Nachrichten
Swiss International Immobilien AG - ...
Impressum Technisches Datenschutz
VERIFIED by VISA
VERIFIED BY VISA
VeriSign Secure Site
VERISIGN SECURE SITE
SWISS IMMOBILIEN
HOME KONTAKT
HOME
KONTAKT
OBJEKTE TESSIN
OBJEKTE ANDERE REGIONEN
REFERENZEN
IMPRESSIONEN
FREIE STELLEN
VILLEN UND HÄUSER WOHNUNGEN PROJEKTE ANDERE OBJEKTE VERMIETUNG

Swiss International Immobilien AG

Das Tessin gehört zu den schönsten Gegenden der Schweiz, mit einem mediterranen Klima, einer traumhaften Flora und viel italienischem Flair. Hier lächelt die Sonne definitiv ein bisschen mehr als an anderen Orten!

Es erwarten Sie im Locarnese der wunderschöne Lago Maggiore und zauberhafte Orte wie Ascona, Locarno, Muralto, Orselina, Ronco, Brissago

Figure 7: Example of a website for recruiting financial agents.

Such offers are circulated not only by way of e-mail and specially created websites, but can also be found on various Internet sites with serious job offers. As a general matter, caution is called for when money previously received (intentionally or erroneously) is to be transferred to unknown recipients by way of a cash transfer. In all cases, one should be sceptical of offers promising disproportionately high returns. Also on the Internet, the general rule applies that big money cannot be earned legally without equivalent work. One should never make one's own bank accounts available to third parties.

3.9 Control systems with Internet connections – Special security awareness necessary

Search engines for websites are part of the everyday life of an Internet user. Until recently, it was less known that search engines also exist to find *servers*, *routers*, *firewalls*, printers and other devices connected with the internet. "SHODAN" is such a search engine and has already existed for several years. It has only recently entered the public focus, however, since the publication of research results about *SCADA* systems connected with the Internet.

The researchers at the University of Cambridge aimed to provide a quantitative estimate of industrial *control systems* with Internet connections, which are especially vulnerable. The research[10] was intended to dispel the myth that industrial control systems are not connected with the Internet and therefore do not give rise to concerns about the security of sensitive infrastructures. The researchers discovered dozens of vulnerable systems connected with the Internet, including Siemens Simatic systems (targeted by Stuxnet), *SCADA* systems and *building management systems* (BMSs).

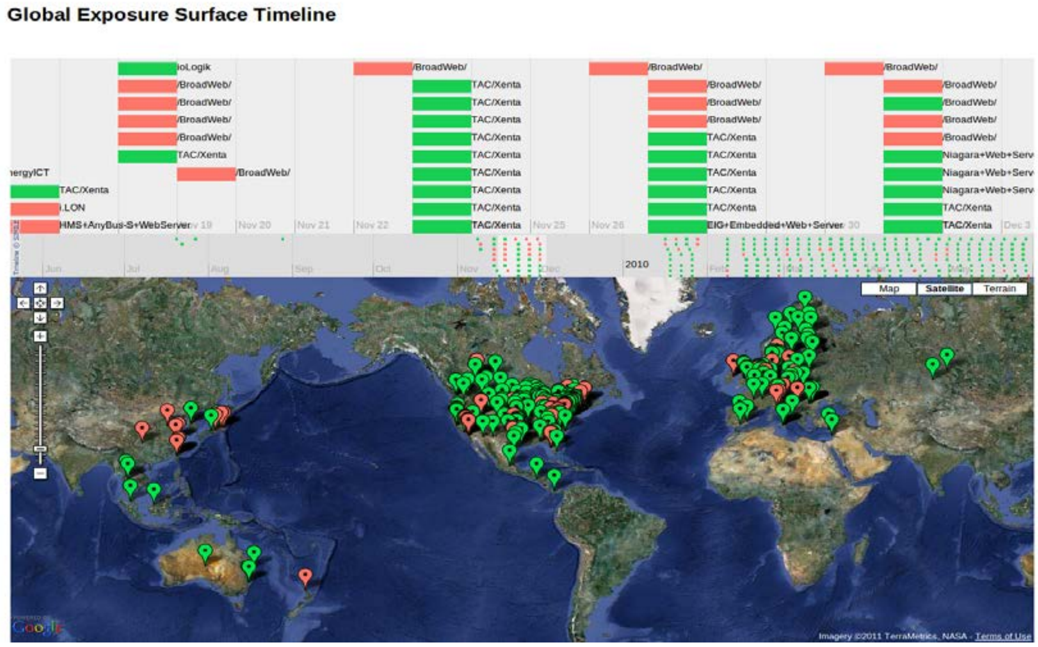


Figure 8: Quantitative analysis and visualisation of industrial controls systems providing a target. (Source: Eireann Leverett)[11] Systems with a known exploit are marked red.

In Switzerland, this research led to the discovery of 34 vulnerable systems. These are mainly applications used for *building management systems*. For these control systems with web access, it was simply forgotten to change the standard password. In this way, it was possible to access the facilities and control them completely. When verifying the information, MELANI determined that the vulnerable systems did not belong to sensitive infrastructures, but rather especially to businesses such as hotels and offices.

[10] http://www.wired.com/images_blogs/threatlevel/2012/01/2011-Leverett-industrial.pdf (as of 23 February 2012).

[11] http://cryptocomb.org/2011-Leverett-industrial.pdf (as of 23 February 2012).

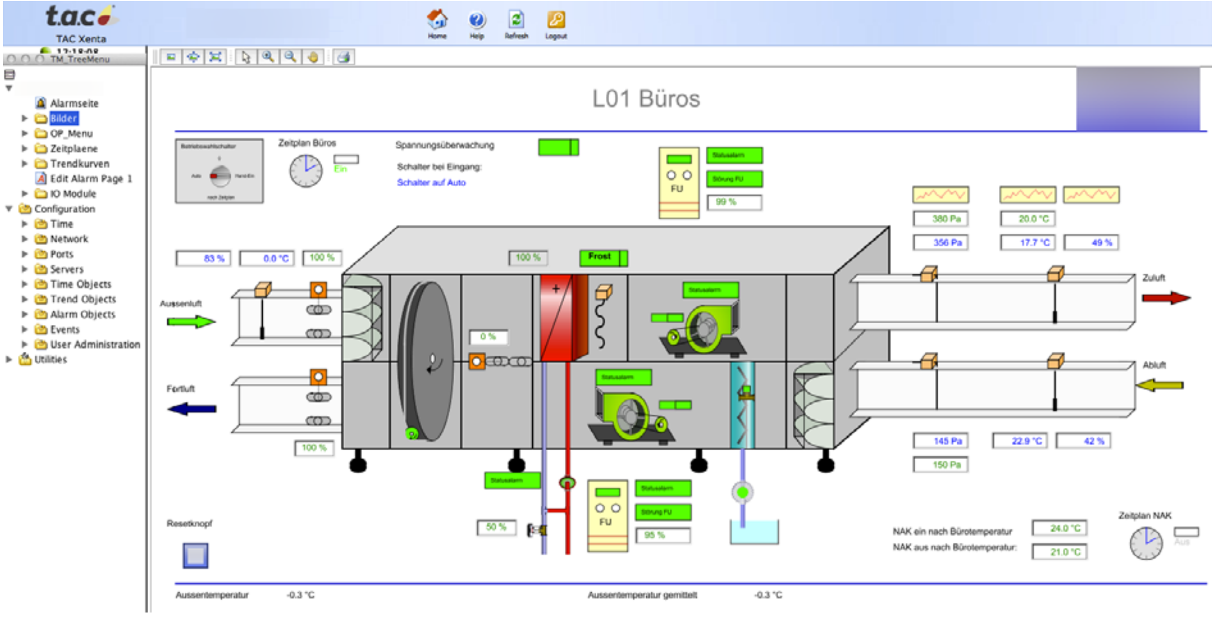


Figure 9: Example of an application by manufacturer TAC (now Schneider Electric Buildings Germany GmbH) for managing buildings

The potential targets may not be considered sensitive, but the fact that the default password was not changed when installing a *building management system* (BMS) with an Internet connection represents a grave violation of basic IT security rules. The ability to, for instance, access and manipulate the heating or air conditioning network of a third-party enterprise has the potential to cause serious problems. Additionally, the partial inclusion of and access to other enterprise-internal administration applications, such as invoicing software and the like, gives rise to potential abuse. In principle, industrial control systems should not be connected with the Internet. If it is absolutely necessary to do so, great care must be taken. A detailed assessment can be found in Chapter 5.1.

4 Current International ICT Infrastructure Situation

4.1 Attack on Dutch certificate authority

During an attack on DigiNotar, a Dutch *certificate authority* (CA)*,* more than 530 *certificates* were issued abusively, according to current knowledge. These included *certificates* for the domains of intelligence services, for instance: The attackers were able to issue several *certificates* for www.sis.gov.uk, www.cia.gov and www.mossad.gov.il. *Certificates* were also issued abusively for several other domains, including windowsupdate.com, which is home to the update function of all Microsoft Windows products, as well as various Google domains.

DigiNotar is an issuer of *certificates* that guarantee the identity of websites and ensure encrypted communication. If such *certificates* are counterfeited, users might assume they have accessed the desired website, when in fact they have been connected with the attacker's infrastructure. In this way, an attacker can change the path taken by the data, intercept encrypted data and also send incorrect data back. Through the attack on DigiNotar, *certificates* that are bogus – but classified as trustworthy by *browsers* and computers – have been brought into circulation. This makes it possible to decrypt an encrypted connection with a webmail account, for instance, or to falsify a Windows update. However, a bogus *certificate* alone does not suffice. The connection must also be redirected via a *server* set up for that purpose. DigiNotar apparently already discovered the attack on 19 July 2011; at the end of

August, Google then discovered *man-in-the-middle* attacks against its e-mail services and made them public.

Shortly thereafter, Microsoft issued updates for its operating systems Windows XP and later and for Internet Explorer; these updates withdraw trust from the *root certificates* of the compromised DigiNotar CA and put it on the list of untrustworthy issuers. Other *browser* manufacturers such as Mozilla (Firefox) and Google (Chrome) have meanwhile marked the *certificates* issued by DigiNotar as untrustworthy.

According to an interim report published by the security firm[12] assigned to investigate, an evaluation of the data shows that the bogus *certificates* were actually used. About 300,000 *IP addresses*, for instance, used the bogus Google *certificate*. According to the report, 99% of these *IP addresses* can be attributed to Iranian computers. To intercept and decrypt the data, the attacker also had to initiate a further interaction directly on the data path, e.g. at the provider. An Iranian hacker meanwhile claims to be the author and to have attacked other certificate issuers. It is not yet clear whether he actually did initiate the attacks or whether a state actor with the intent of espionage was behind them.

The hacker attack against DigiNotar plunged the firm into insolvency. According to its parent company Vasco, the business operations of the subsidiary have been suspended, and the company has been liquidated. Already shortly after announcement of the incidents, the Dutch government took control of the operational business of DigiNotar. In addition to its own *certificates*, DigiNotar also issued them as a sub-CA for the "PKI Overheid" of the Dutch government, and there are indications that the systems used for that purpose were also compromised. The "PKI Overheid" root certificate was not revoked, however, since this might have led to breakdowns in communication between computer systems relying on encrypted connections. It could also not be proven that abusive *certificates* were issued using that infrastructure. All "PKI Overheid" *certificates* issued by DigiNotar as a sub-CA were, however, replaced by new *certificates* from other sub-CAs as a precautionary measure.

In another case, a hacker claimed to have penetrated the systems of the certificate issuer GlobalSign. The Belgian certificate issuer subsequently took its *servers* off the Internet for a week and launched an investigation. It turned out that the hacker hadn't penetrated any *server* used for the issuing of certificates, however, but rather a *server* that makes the public company websites for North America available. According to GlobalSign, these did not contain any web applications or client data.[13]

The secure use of *cryptosystems* with public keys (public key cryptography) relies on the security of the *certification service provider* (CSP) and public key infrastructure (PKI)[14]. The security of CSPs and PKIs has thus always been an issue that security technicians have had to deal with. The focus of interest has been on scenarios in which either *certificates* have been falsified (using vulnerabilities in the collision resistance of the cryptographic hash functions employed[15]) or code signing certificates have been abused. In the second case – as the Stuxnet worm showed – such a *certificate* allows *malware* to be smuggled into the

[12] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html (as of 23 February 2012).

[13] http://www.zdnet.de/news/41558800/globalsign-comodohacker-hat-die-falschen-systeme-erwischt.htm (as of 23 February 2012).

[14] In this sense, CSPs and PKIs represent an Achilles' heel for public key cryptography.

[15] This point is discussed in-depth e.g. in the technological considerations of 4 August 2010 ("Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen"): http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de (as of 23 February 2012)

operating system in the form of digitally signed *driver software*, for instance. The recent attacks against CSPs have now shown, however, that the compromising of a CSP for the purpose of issuing bogus *certificates* represents a real threat. Hackers appear to be targeting the source more frequently than before, thus avoiding the much more tedious path through the crypto-procedures, which are secure as such.

4.2 SCADA – Malware, attacks and vulnerabilities

Supervisory Control And Data Acquisition systems are used to supervise and control technical processes (e.g. energy and water supplies). Originally, these systems weren't very similar to traditional ICT; they were isolated from the computer networks, used proprietary hardware and software, and employed their own protocols for communicating with the central computer. The wide availability of comparatively inexpensive devices with built-in interfaces to the Internet protocol has brought about huge changes in this area in recent years. The advantage of using low-cost, standard ICT is purchased by the fact that SCADA systems are now in principle exposed to the same threats encountered on the Internet: The doors are open to malware and attackers.

Symantec discovers "Duqu", malware with ties to Stuxnet

On 14 October 2011, *malware* named "Duqu" became known, the purpose of which is to spy on computers used by businesses and developers of industrial control systems (*SCADA* systems). Data stolen in this way can be used for later attacks on industrial control systems. The basic components (drivers) of this new *malware* are based on components of the already known *malware* Stuxnet.[16] In contrast to Stuxnet, the new *malware* does not have a spreading routine and or *SCADA* components, for instance to manipulate control systems. To stay as undetected as possible, the *malware* activates itself only 15 minutes after installation. After 36 days, the *malware* removes itself from the infected system, which makes detection even more difficult. Several variants of "Duqu" have been observed. In one case, a stolen *certificate* of a Taiwanese company was used for the installation; this is a further parallel to Stuxnet. The other variants were apparently not digitally signed.

The functions of the *malware* include recording of keystrokes, analysis of network information, and saving of screen contents. This information is hidden in an inconspicuous image file and sent to the attacker. In principle, however, the function is not tied to the *malware* and can be varied as desired by the attacker. "Duqu" uses encryption to communicate with a *command server* with an Indian *IP address*, to which the infected computer sends collected data and from which it receives new commands. A variant is said to have been circulating already in December 2010; new variants are from September/October 2011. "Duqu" apparently has been found on computers of seven or eight European companies, including an *IP address* in Switzerland.

Alleged attacks on water supplies

An alleged electronic attack on the water supply system in Springfield/Illinois in US at the beginning of November 2011 has triggered a broad debate in specialist circles. Allegedly, an attacker was able to penetrate the control system of the water supply and destroy a water pump by turning it on and off several times. In the time before the defect, the facility's

[16] See MELANI Semi-annual report 2010/2, Chapter 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=en (as of 23 February 2012).

network was apparently accessed by a computer with an *IP address* in Russia, which additionally fed the rumour mill. A few days later, the FBI and the Department of Homeland Security (DHS) denied the reports about the attack in Springfield, saying there were no indications of a cyber attack. The claims from a report of the terrorism situation centre in Illinois, which had become public and on which the speculations relied, were supposedly based on unconfirmed raw data. There were no signs that access data for the system had been stolen, and likewise no signs of penetration had been found. The accesses from Russia had been by an authorised technician who happened to be traveling in Russia and dialled into the facility's network using (regular) remote access. The pump had been a problem for quite some time and had turned on and off several times before failing completely.

Possibly motivated by the reports on this case, a hacker penetrated the water supply of Houston/Texas on 18 November 2011 and published *screenshots* of the facility's control system as proof. In this case, a person with the pseudonym "pr0f" claimed responsibility for the attack by posting a message on the pastebin.com site: "The moment has come to show that sensitive systems should not be connected with the Internet. You shouldn't be worried about a supposedly huge cyber war, but instead should be afraid of individual perpetrators who are able to attack sensitive systems for various motives and without major IT knowledge."

US observation satellite hacked in 2007 and 2008

According to a report in Bloomberg Businessweek[17], several attacks on the control systems of two US observation satellites were discovered in 2007 and 2008. These satellites were used to observe the Earth and the climate and for mapping. Hackers apparently took control of the satellites for several minutes. It is not known how the attack proceeded in detail. Conceivably, the data were falsified. Theoretically, it would have been possible to guide the satellites and even cause them to crash.

Security concerns regarding the network of the Boeing Dreamliners

According to a report by the FAA[18], there are security concerns regarding the network cabling of the new Boeing Dreamliner. Apparently, the network for passengers, which allows Internet access during the flight, is physically also connected with the control and navigation network of the aeroplane, which controls the functions relevant to security.

Boeing itself said that the FAA document is misleading and that the passenger network is not completely connected with the other networks. A combination of physical separation and software *firewalls* was used, along with other solutions not publically disclosed. While data could be exchanged between the networks, the installed protection mechanisms are intended to make it impossible under all circumstances, that the passenger internet service is able to access the maintenance data or the navigation system.

A physical connection between the passenger network and the plane's control network would make the control system vulnerable to hacker attacks. Boeing itself has recognised the problem and plans to test and implement a new solution.

The basic problem regarding *SCADA* systems is related especially to its history: Originally, they were separated, independent and proprietary systems that could be accessed remotely, if at all, by the manufacturer only for maintenance purposes via a *dial-up modem*.

[17] http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (as of 23 February 2012).

[18] Federal Aviation Administration of the United States, http://www.faa.gov (as of 23 February 2012).

Accordingly, these systems hardly had functions to protect from electronic attacks. Recently, however, *SCADA* systems increasingly are being networked, they use standardised protocols and technologies, and some of them may even be accessed via the Internet and sometimes can be found using special search engines (see the SHODAN search engine described in Chapter 3.9). Stuxnet has also shown that a separated system alone cannot guarantee security. As long as it is possible to transfer data to the separated systems using a *USB* stick, for instance, the possibility also exists to smuggling in *malware*. The media presence of Stuxnet has generated interest in industrial control technology and *SCADA* systems among many security experts as well. Accordingly, various vulnerabilities have since been identified in such products. Methods have been discovered that allow systems to be remote-controlled, data to be downloaded and uploaded at will, *codes* to be smuggled in and launched, and bogus data to be introduced that trigger reactions by the control systems.

4.3 Anonymous

On 27 July 2011, the British police arrested the alleged speaker of the hacker groups "Anonymous" and "LulzSec" in the Scottish Shetland Islands, a 19-year old man. In several countries, including the US, the UK, the Netherlands, Spain and Turkey, other members of the Internet protest movement had already been arrested. Such arrests tend to trigger attacks on the websites of the police corps or government involved. This happened again after a coordinated action of the Italian and Ticino police at the beginning of July, in which 15 alleged activists were arrested in Italy. Likewise, a 26-year-old Italian living in Ticino, who is said to be the head of the Italian cell of Anonymous, was arrested. The Anonymous collective had attacked the Italian firms Eni, Finmeccanica and Unicredit, among others. Institutions such as the Italian postal service, the Senate, the Chamber of Deputies, and the website of the government of Prime Minister Berlusconi were targeted by Anonymous too. As a response to the arrest, Internet activists claim to have stolen data from the *servers* of the Italian cyber police CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastructure Critiche) and made them available on the Internet. This state authority is responsible for the protection and maintenance of the critical IT infrastructure in Italy. A letter claiming this was retaliation had its authenticity denied by Anonymous; but a certain link is likely nonetheless.

Also in July 2011, Internet activists claimed to have penetrated a NATO *server* and to have copied numerous documents. As proof, two PDF documents from 2007 and 2008 were published. The break-in is said to have been committed using an *SQL injection*. Another action was the publication of 25,000 datasets with the names, addresses and birthdates of police officers in Austria. This action was justified in part with reference to the introduction of *data retention* in Austria in April 2011.

The greatest stir, however, was certainly caused by the attack on client data of the US company Strategic Forecast (Stratfor) at the end of the year. Stratfor specialises in international security analyses and supplies its clients with reports on current geopolitical security issues such as terrorism, political upheaval, and changes of government in individual countries. The hacker attack obtained e-mail files, user data, passwords and credit card information, among other data. One goal of the action was supposedly to make transfers to charitable organisations with the stolen credit card data and in that way "to redistribute more than USD 1 million to charitable organisations". Allegedly, unauthorised payments with stolen credit cards also occurred. The activists thus likely did a disservice to the charitable organisations – such payments cause administrative hassles on all sides. After Anonymous first claimed responsibility under the name "LulzXmas", a denial also was circulated on the Internet in the name of Anonymous, and finally a denial of the denial. In yet another statement, the real reasons for the attack were cited as the disclosure of contacts to intelligence services and the armament industry.

The label "Anonymous" subsumes Internet activists from around the world who demonstrate on behalf of a free Internet and against state control. Although Anonymous regularly emphasises that it is a collective of activists on equal terms, just a few persons should be regarded as the driving forces of the movement. These are likely to be more or less experienced users who open up possibilities for the masses and give them momentum. These positions may also be assumed by any number of persons, even for short periods of time. An analysis of the membership structure can be found in Chapter 5.2.

4.4 Alleged state actor spied on computer systems worldwide for many years, including the UN in Geneva and the IOC

On 3 August 2011, the security firm McAfee published information about a coordinated attack on various companies, authorities and organisations. Due to faulty design, the security firm was able to find *log files* on the attackers' control computer, in which access activities since 2006 had been logged. The analysis of these data provided conclusions about the attackers' targets and how long these attacks had lasted. According to the security firm McAfee, the discovery of this attack was one of the largest known espionage attacks so far. Since 2006, 72 companies, organisations and governments had apparently been spied on, including the UN headquarters in Geneva and the headquarters of the International Olympic Committee (IOC) in Lausanne. The bulk of the attacked networks were in the US, however. These include satellite communication companies, various security firms, and a production company for solar cells. Specific company names were not divulged. In addition, government offices in the United States, Canada, India, Vietnam and Taiwan were said to have been affected. Concerning the type of the information stolen, there is only a statement by the security firm that the stolen information in the wrong hands may constitute a massive economic threat.[19]

For the infection, the attackers used traditional infection methods such as targeted e-mails and prepared links. The victims received tailored e-mails with bogus sender addresses. As soon as the recipient clicked on the link, *malware* was loaded and installed. Additionally, a channel to the control server was opened.

A state actor appears likely in this case, since the stolen information can hardly be sold by the criminals. The fact, for instance, that the control server was poorly protected on the Internet shows either that the attackers are likewise not perfect when protecting their infrastructure, or that they are not (very) concerned about securing it, since there are sufficient alternatives available. This espionage attack once again shows that there is a constant interest in data and information, and that the pressure on sensitive data is increasing every day. It must be assumed that further espionage networks are being built up, and that others have already been built up and are possibly active, but haven't been discovered yet.

Targeted e-mails continue to be sent. This was seen, for example, in a targeted attack against armament companies in July 2011. In this case, the attackers sent professionally formulated e-mails to employees of armament companies, advertising a conference of the American Institute of Aeronautics and Astronautics (AIAA). The document supposedly

[19] http://www.spiegel.de/netzwelt/web/0,1518,778126-8,00.html (as of 23 February 2012).

classified as "secret" requested the recipients to submit papers for the upcoming conference by 30 July.[20] E-mails referring to a conference are especially popular with the attackers.

It should be noted that not only internationally operating major companies can be targets of economic espionage, but also innovative small and medium-sized companies.

The attackers are repeatedly suspected of being from China, but this is always denied by the Chinese government. In fact, it is difficult to identify the perpetrators of an attack unambiguously, since the only traces in such attacks are generally *IP addresses*. If an *IP address* is from China, this is not proof that the attacker is actually from China. It is, for example, relatively easy to rent *servers* in any given country, which are then used to carry out the attacks and the sole purpose of which is to conceal the attack's origin. And even if the attack is really from China, it is not clear who the actual perpetrators are. According to a report in the Wall Street Journal the US intelligence service has identified 20 Chinese hacker groups from which most of the cyber attacks against the United States are carried out.[21] Even though the report claims that 12 of these groups have connections to the Chinese People's Liberation Army, it will be difficult to prove that the attacks are actually commissioned by the state. What makes the situation even more difficult is that several states are able to launch major espionage operations via networks.

4.5 Various hacking attacks

Also in the second half of the year, there were various hacking and espionage attacks or such attacks became public. Here is a non-exhaustive list of examples:

Espionage attack on the US Chamber of Commerce

According to the Wall Street Journal, Chinese hackers installed at least six backdoors in the computer network of the US Chamber of Commerce. This probably allowed the umbrella organization of the US business community in Washington to be spied on systematically for several months. The vulnerability was already discovered and fixed in May 2010, but the incident became public only in the second half of 2011.[22]

New attack on Sony's online services

After the attack on Sony client data in the last half-year, hackers in October 2011 were again able to penetrate user accounts for Sony's online services Play Station Network (PSN) and Sony Entertainment Network (SEN). This succeeded in 93,000 cases. These account data were apparently blocked, and credit card data were not in danger. Unlike the first time, Sony was not attacked directly in this case: With the help of password information obtained elsewhere, an attempt was made to enter the accounts. The explanation is simple: Many computer users use the same password for most services, or even all services. The owners of the accounts were notified by e-mail and had to run through an authentication process to

[20] http://www.heise.de/security/meldung/Gezielte-Angriffe-auf-Ruestungskonzerne-dauern-an-1282837.html (as of 23 February 2012).

[21] http://online.wsj.com/article_email/SB10001424052970204336104577094690893528130-lMyQjAxMTAxMDEwMjExNDIyWj.html ; entire report by the Office of the National Counterintelligence Executive: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (as of 23 February 2012).

[22] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,805052,00.html (as of 23 February 2012).

re-activate their accounts. Sony says that it will reimburse money if fraudulent purchases are made in the Sony network.

Hackers attack South Korean networks

In a hacker attack in South Korea, data of about 25 million Internet users were stolen. As the country's authorities reported at the end of July, the attacks against the online platform Nate and the social network Cyworld were perpetrated from computers with *IP addresses* in China. It is reported that the illegally obtained data included telephone and social insurance numbers as well as e-mail addresses and passwords. The South Korean stated that investigations would probably take several months.[23]

4.6 Deactivation of DNSChanger botnet

During an infection with the DNSChanger *malware*, the *DNS* system on the infected computers was manipulated in such a way that the *webbrowser* redirected users to manipulated websites without their knowledge when they tried to access popular sites.

In November 2011, the criminal administrators of this *botnet* were arrested by the FBI. The FBI replaced the manipulated *DNS* servers of the criminals with correctly functioning *DNS* servers so that no further manipulations are possible.

These *servers* were supposed to be shut down on 8 March 2012, but the FBI extended the transition period until 9 July 2012. From that date, infected computers will no longer be able to resolve domain names and the affected users will accordingly no longer be able to access websites. Depending on the way the computer is used, this may lead to serious problems.

SWITCH[24] and the German authorities have therefore made online tests available to check whether one's computer has been infected by the DNSChanger *malware*[25].

According to the information available to MELANI, the FBI identified 20,500 *IP addresses* in Switzerland alone within a week. This does not mean that this many systems have been infected, since most of them are dynamic *IP addresses*. Nevertheless, possibly several thousand computers in Switzerland have been infected with the DNSChanger *malware*.

4.7 Law enforcement trojans

On 8 October 2011, the Chaos Computer Club (CCC)[26] announced that it had gained possession of a law enforcement trojan of the German authorities. This trojan allows investigators in Germany to carry out "source telecommunication surveillance". In this way, Internet telephones, i.e. *Voice-over-IP conversations* (VoIP), can be tapped before they have been encrypted by the sender or after they have been decrypted by the recipient.

This trojan is often referred to using the undifferentiated term "federal trojan" and thus incorrectly equated with espionage programmes of intelligence services and large-scale

[23] http://www.tagesanzeiger.ch/digital/internet/Hacker-greifen-suedkoreanische-Netzwerke-an/story/31054597 (as of 23 February 2012).

[24] http://www.dns-check.ch (as of 23 February 2012).

[25] http://www.dns-ok.de/ (as of 23 February 2012).

[26] http://www.ccc.de (as of 23 February 2012).

phone tapping. The legal foundations for the different types of operation should not be mixed up or confused, however.

The CCC examined the law enforcement trojan and accused the authorities of not limiting its functions to the recording of conversations, but rather also allowing it to read and forward data on the computer. For instance, the content of the *webbrowser* could be seen with the help of screenshots. Remote access is also claimed to allow the subsequent downloading of any number of functions. The CCC has also criticised the encryption, claiming that outgoing communications are only *symmetrically encrypted*, while there is no encryption at all for incoming communications. This is especially relevant in that data and commands allegedly are not transacted via German *servers*, but rather via foreign *servers*. The trojan is also claimed to have vulnerabilities that in principle could be exploited by third parties for the purpose of themselves attaining access to the computer under surveillance.

Also in Switzerland, the use of law enforcement trojans was discussed after this incident. The Federal Criminal Police has employed trojans in Switzerland in four cases – three times to fight terrorism and once against organised crime. The Canton of Zurich has used a trojan at least once against drug dealers[27]. After disclosure of these trojan operations, the Pirate Party Switzerland brought action before the Office of the Attorney General of Switzerland because of the use of espionage software in the fight against terrorism and organised crime. The Office of the Attorney General rejected the action, however.[28]

Already before the Internet age, law enforcement authorities were allowed to tap telephone conversations of suspects, if approved by a judge in the concrete case. The providers of telecommunication services are legally required to allow law enforcement authorities to carry out such surveillance.[29]

New challenges arise for the investigations of law enforcement authorities due to the spread of alternative communication technologies. Since in the case of Internet telephony (e.g. Skype), no classic telephone service provider is responsible for routing the conversation, and the communication is encrypted during transmission, surveillance is only possible at the terminal devices. To carry out surveillance, technical aids may be used during criminal procedures.[30] In the case of Internet telephony, this may be a programme that is smuggled into the target person's computer and consequently intercepts communications before they are encrypted and sends them to the law enforcement authorities.

Whether the current[31] legal framework in Switzerland suffices for this kind of surveillance is controversial in legal theory as well as among policymakers.[32] It has not aided clarification of this issue that the debate regularly mixes up law enforcement and intelligence services as well as telephone surveillance and online searches of computers. On the one hand, the various entities and measures on the legal-political side must be considered separately; on the other hand, the scope of functionality of the software on the application side should be limited to the approved operations, and changes of function or abuse of the methods used

[27] http://www.nzz.ch/nachrichten/politik/schweiz/trojaner_im_fall_stauffacher_eingesetzt_1.12994241.html (as of 23 February 2012).

[28] http://www.aargauerzeitung.ch/schweiz/anzeige-der-piratenpartei-zu-spionage-software-bleibt-ohne-folgen-115718001 (as of 23 February 2012).

[29] See Federal Act on Postal Service and Telecommunications Surveillance (BÜPF) and the associated ordinance (VÜPF): http://www.admin.ch/ch/d/sr/c780_1.html (as of 23 February 2012) and http://www.admin.ch/ch/d/sr/c780_11.html (as of 23 February 2012).

[30] Art. 280 of the Swiss Code of Criminal Procedure: http://www.admin.ch/ch/d/sr/312_0/a280.html

[31] The Swiss Code of Criminal Procedure has been in force only since 1.1.2011; previously, every canton and the Confederation had their own law of criminal procedure.

[32] The use of surveillance software in Switzerland is only possible in the context of criminal prosecution; the use in the context of intelligence services is not allowed in Switzerland.

should be ruled out. For instance, tapping software intended (and authorised) for the recording of VoIP conversations must not be allowed to make screenshots or intercept e-mails. It becomes even more problematic if it cannot be ruled out that unauthorised third parties obtain knowledge of the data gathered, or even are able to manipulate the software being used. Security must have the highest priority when these means are employed.

Finally, it should be noted that the hurdles for "normal" telephone surveillance as well as the hurdles for Internet telephone surveillance are high: In Switzerland, surveillance can only be justified after approval by a judge, in the case of specific serious offences, and if "the previous investigative acts were unsuccessful or if investigations would be futile or made disproportionately more difficult otherwise".[33] The principle of proportionality must be taken into account here, as in the case of any interference with basic rights.

4.8 WikiLeaks divulges trade in surveillance and forensic software

Since 1 December 2011, WikiLeaks and its media partners have published documents around the world which are claimed to prove that the market for ICT security, surveillance, and forensics solutions is flourishing not only in regard to the government authorities of democratic countries, but also that business is being done with "rogue states". The overwhelming majority of these documents are sales brochures, public presentations, and price lists of about 100 companies working in the fields of global security solutions as well as ICT security and forensics, including DigiTask and Siemens in Germany, FoxIT in the Netherlands, Dreamlab Technologies AG in Switzerland and Hewlett-Packard in the United States.

After the fall of various regimes in the Arab region, documents were published showing that some of these companies at least made product offers to the former rulers. After the fall of the Egyptian government, it became public that the German-English Gamma Group had offered their products to the Mubarak regime. In Libya, the Gaddafi government should have employed the ICT solutions of the French company Amesys for its "Public Safety System and Passport Network".[34] Also in Syria, surveillance software of Western ICT companies is allegedly employed. In addition to software of the Germany company Utimaco, which connects tapped phone lines with the computers in its surveillance centre, mail archiving software of the US company NetApp is being used. The French company Qosmos allegedly supplies the technology for the surveillance of communication networks. The manufacturers supposedly never delivered directly to Syria, however.[35]

In the current "exposure case", WikiLeaks and various groups working on strengthening the freedom of information argue that this type of technology transfer to rogue states is not only morally and ethically reprehensible, but also aids and abets the surveillance and thus the suppression of the population in these countries, and even costs human lives. However, the sale more generally of such products to Western law enforcement authorities, intelligence services, and the military is also criticised. In its editorial, WikiLeaks makes clear that the use of such ICT surveillance solutions and the resulting market are in principle objectionable, and that there is a complete lack of appropriate legal provisions to control such "data weapons".

[33] Art. 269 of the Swiss Code of Criminal Procedure: http://www.admin.ch/ch/d/sr/312_0/a269.html (as of 23 February 2012).

[34] http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html (as of 23 February 2012).

[35] http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html (as of 23 February 2012).

The companies mentioned by WikiLeaks work in the fields of ICT forensics, *lawful interception* and *data retention* (see also Chapter 5.3).

Interestingly, only Western suppliers are mentioned in the documents published under the name of "Spy Files". They do not mention up-and-coming Asian companies that offer programmes for comprehensive surveillance and intelligence evaluations or generally for internal security, specialising in user identification, censorship measures, surveillance of social networks and HTTPS connections. Among these newcomers on the security market, there are few inhibitions about selling surveillance software to interested states irrespective of their internal order.

4.9 Strategies and exercises

New EU strategy for network security

The European Union has announced a major European strategy for the security of European networks in the coming year. In a letter to the responsible ministries in the member states, the respective "security capacities" are first assessed. The EU says it must enhance its political efforts in this field, and it has assigned the European Network and Information Security Agency (ENISA)[36] a key role for its strategy.[37]

National crisis management exercise in the field of ICT in Germany

On 30 November and 1 December 2011, the Federal Ministry of the Interior, especially in coordination with the states of Hamburg, Thuringia, Saxony, Hesse and Lower Saxony. In the course of this exercise, referred to as LÜKEX (Länder Übergreifende Krisenmanagement-Übung/Exercise, or National Crisis Management Exercise), which will take place every two years with different emphases, the cooperation of several affected offices at the federal level with the crisis staffs of the states as well as selected companies was trained. This year's exercise was based on a fictitious exercise facility, which confronted the crisis staffs at the federal and state level with a whole range of damaging events (i.e. massive *spam* attacks, malicious programmes, and the wilful overloading of systems) in the administrations and the participating companies. A total of 2,500 participants from 12 states took part in the exercise.

The focus of the exercise was on federal-state harmonisation for the analysis of the causes of the ICT attacks as well as preventive measures at the political and administrative level. Also rehearsed were the coordination of measures to protect the population as well as the corporate and administrative networks, and the cooperation of public and non-public organisations at the federal and state level. Together with all participants, the exercise will be evaluated in detail over the coming months. The goal is to achieve improvements in the crisis planning and management processes.[38]

[36] http://www.enisa.europa.eu (as of 23 February 2012).

[37] http://www.heise.de/security/meldung/Neue-EU-Strategie-fuer-Sicherheit-in-den-Netzen-angekuendigt-1394814.html (as of 23 February 2012).

[38] Press release of the German Ministry of the Interior: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/12/luekex.html?nn=109632 (as of 23 February 2012).
An overview of previous exercises: https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/IT-Krisenreaktionszentrum/Uebungen/Beispiele/beispiele_node.html (as of 23 February 2012).

Switzerland and especially representatives of the Federal Chancellery and the National Strategy for Protecting Switzerland against Cyber Risks took part as observers in the LÜKEX exercise. In Switzerland, strategic leadership exercises similar to LÜKEX are carried out. The theme of the next exercise of this kind will likewise be a cyber attack on Switzerland. In this way, the Federal Council wishes to verify the national strategy for the defence against such an attack and especially the concept for its implementation. The exercise will consist of four parts and take place from September 2012 to May 2013. It targets the crisis staffs of the departments and the other bodies of the federal administration that are called upon in a crisis event.[39]

Cyber Atlantic

Figure 10: Logo of Cyber Atlantic 2011

The first cyber security exercise between the EU and the US was conducted on 3 November 2011 in Brussels. The one-day table top exercise, Cyber Atlantic 2011, examined how cooperation between the EU and the US works in the event of an attack on critical information infrastructures. The scenarios of an *advanced persistent threat (APT)* and an attack on a *SCADA* system in the energy sector were simulated. More than 20 countries took part in the exercise, 16 of which actively. The exercise is part of an EU-US agreement in the field of cyber security adopted at the EU-US summit in Lisbon on 20 November 2010.[40] Switzerland participated in the Cyber Atlantic 2011 exercise as an observer and was able to gather valuable insights for international coordination in the event of a cyber incident.

[39] http://intranet.bk.admin.ch/aktuell/media/03238/index.html?lang=de&msg-id=43517 (as of 23 February 2012).

[40] http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011 (as of 23 February 2012).

5 In-depth Analyses and Trends

5.1 Smart grid and home automation

As already mentioned in Chapters 3.9 and 4.2, *SCADA* (Supervisory Control and Data Acquisition) systems are primarily used for the control of power plants and transport systems, but increasingly also in homes, office buildings and hotels for the control of heating, air conditioning and shutters. Modern systems can even be controlled using tablets and smartphones with the appropriate apps. The desire to use these control systems not only from within one's own home, but also via the Internet from anywhere, is obvious. Especially in the case of vacation homes, remote control makes sense, for instance to turn on the water heater before arrival, adjust the temperature of the apartment, or simply to check remotely that the oven and all lights have been turned off and the heater is working without problems.

But here again, one should pay attention to security. The systems are directly connected with the Internet and are thus in principle exposed to the same threats as computer systems. As described in Chapter 3.9, it was simply forgotten in the case of various control systems of hotels and companies with web access to change the standard passwords. This made it possible for unauthorised persons to access the systems and control them completely. What appears harmless at first glance may have far-reaching consequences, for instance if the heater is shut off in an empty house in the winter or the alarm system is also controlled by home automation and is deactivated that way.

Also in a different area, we will be confronted in future with *SCADA* systems. The upheavals in the energy sector, especially in view of the phasing out of nuclear energy in the long term, are forcing energy suppliers to identify options for ensuring energy stability, even if less band energy from nuclear power plants and an increasing amount of irregular energy in the form of wind and solar energy will be available. Part of the solution to this problem will be the *smart grid*. In a first step, energy consumption is detected directly at the consumer in order to increase system stability. This information is transmitted to a central office. While energy consumption today is largely based on estimates and experience, it will in future be possible to determine it much more precisely and in that way to guarantee improved system stability. But if these data fall into the wrong hands or such a *smart meter* is hacked, then electricity might for instance be used to determine whether someone is at home, or the electricity bill might be manipulated directly.

In a second step, it is conceivable that devices like dishwashers and washing machines would be connected to the *smart grid* and controlled by it. Consumers would then signal the central office that they would like to activate their washing machine. This would not occur immediately, however, but rather the control centre would decide when is the best time to activate the device in question.

Clearly, such a system would have to be very well protected, since incorrect handling might lead to serious electricity shortages. In the worst case, the entire energy supply might break down.

5.2 Anonymous – the advantages and disadvantages of the open structure

Anonymous has caused a stir in recent months with various operations in cyberspace. The list of victims includes prominent companies such as Sony, the Bank of America, the security firm Stratfor (see Chapter 4.3) or even criminal groups such as the Mexican drug mafia "Los Zetas".

In Switzerland, especially "Operation Payback" drew attention, one of whose attacks was against Postfinance after it blocked the account of WikiLeaks founder Julian Assange. But who exactly is behind Anonymous and its attacks? According to various statements, Anonymous is not an organisation or group per se, with bylaws, applications for membership, and membership dues. Rather, Anonymous is more of an idea or an attitude to life[41]. Support is not tied to a particular form. Every "anon" does what he or she can and believes to be right. On the one hand, this definition has the advantage that the threshold is low to participate in Anonymous, and that the momentum of current discontent with a company or a state can be exploited by initiators before participants in actions think (or are able to think) too much about the consequences. On the other hand, this type of structure also entails risks – including for the movement itself. Since all "anons" decide themselves what they think is right, actions may be announced or carried out that do not necessarily reflect the majority or even overall opinion of Anonymous.

The best example of this was the announcement that Anonymous would attack Facebook on 5 November 2011 – with the goal of encouraging "as many users as possible" to leave Facebook.[42] This of course resulted in a lot of media coverage – but nothing happened on 5 November. The announcement not only led to discussions in the press, but also within Anonymous itself. Other "anons" described the planned attack as the work of a confused lone fighter, and the announcement was called "imaginary", although there in fact would be reasons from the perspective of Anonymous to carry out such an attack. The name of the initiator was subsequently disclosed, which can probably be seen as the worst punishment within Anonymous.[43]

But also in the case of the attack against Stratfor, various motives, denials, and denials of these denials accumulated. After Anonymous initially claimed responsibility for the action under the name "LulzXmas" and called for the stolen credit card data to be used for donations to charitable organisations, a denial began circulating on the Internet, also in the name of Anonymous, followed by a denial of that denial. In yet another statement, the real reasons for the attack were cited as the disclosure of contacts to intelligence services and the armament industry.[44] But especially the Stratfor case illuminates another aspect: Criminals with purely financial motives and without major visions might also hide under the guise of Anonymous. The credit card data were not only used to donate supposedly USD 1 million to charitable organisations; they were also made available on the Internet, where they were freely available to all criminals (and the rest of the world) and could be used for any purpose whatsoever.

[41] http://www.format.at/articles/1131/524/303276_s1/format-chat-anonymous-mitglied-tvxor (as of 23 February 2012).

[42] https://www.taz.de/!81221/ (as of 23 February 2012).

[43] http://www.golem.de/1111/87543.html (as of 23 February 2012).

[44] http://www.n-tv.de/technik/Hacker-Angriff-gibt-Raetsel-auf-article5086791.html (as of 23 February 2012).

The loose ties within Anonymous result in numerous uncoordinated, more or less spectacular attacks. Since, given its structure, Anonymous has no membership, official spokesperson, or other persons responsible for the movement as a whole, in principle anyone can carry out attacks in the name of Anonymous or publish statements. Accordingly, it makes little sense to ask after an attack or the publication of data whether "Anonymous" is responsible. This is also how claims of responsibility and denials should be treated.

5.3 "Good" and "bad" surveillance on the Internet

The analysis of the German law enforcement trojan (colloquially referred to as "federal trojan") by the Chaos Computer Club and the disclosure of the scope of its functionality triggered renewed debates about its use not only in Germany, but also in Switzerland. Additionally, WikiLeaks began to publish numerous documents on 1 December 2011, which are purported to show that private security companies are selling ICT solutions to states with predominantly autocratic governments and lack of respect for human rights. Many of these solutions originate in the field of *lawful interception* and ICT forensics and allow the respective authorities to tap or record the communication of their citizens on the Internet and mobile phones, but also to spy out data on computers.

This debate, which is in fact old but has been rekindled, arises from one of the fundamental problems of the Internet, the networked society, and ICT. The emergence of new options all the time to communicate, to exchange data and information, and to make them available everywhere and always, has consequences: The measures to locate and obtain information, and generally the work of the security authorities of a state, are becoming much more complicated. In the case of judicially ordered tapping of a Skype communication for instance, this development makes the use of ICT solutions necessary, such as third-party programmes on the suspect's computer. In light of the increasing possibilities for communication within a country, especially those states pursuing repressive policies against political dissidents are strengthening central control of the domestic networks and their connections abroad. In some cases, the same ICT products and solutions are used there as they are in seemingly better-functioning states governed by the rule of law. The reason for this is that, at the technical level, the Internet, computers and networks work the same everywhere, and corresponding ICT solutions can be used anywhere, regardless of where these ICT elements are located and what legal framework conditions prevail.

On the legal side, ICT products are not subject to export controls, except for some restrictions governing the trade in crypto solutions. Such controls could also not be implemented in practice. For one, software-based ICT solutions such as those criticised by WikiLeaks are practically always *dual-use goods*, and for another they consist of programme *code* – i.e. they do not exist physically – and can be sent from one place to another at any time. Ironically, such an export regime could only be enforceable worldwide through total control of the entire Internet and its data flows.

In light of the fact that more and more different kinds of processes now take place over the Internet, it is clear that there is demand by countries' security authorities for ICT solutions of one kind or the other. Only in that way can they fulfil their mandate within the framework of the rule of law. There is no bright line as to when such solutions can be lawfully employed or not in the Western understanding of the power of the state. However, every state is free to issue binding rules for its domestic ICT industry governing the trade in ICT solutions, and to provide clear legal rules governing the cases in which such products may be employed by the country's own authorities. In Switzerland, this work has begun or has already been completed within the context of revision of the Federal Act on Postal Service and Telecommunications Surveillance[45] (BÜPF) and other laws in this field.

5.4 Security in the mobile age – How do I protect my smartphone?

As the newest statistics show[46], Switzerland has about four million mobile phones, including 1.5 million *smartphones*[47]. Two operating systems dominate the market worldwide and in Switzerland: Apple iOS with about 50% of the market share of smartphones sold in Switzerland, and Google Android with a market share of about 27%. These two operating systems are also the most popular for tablets.

In this connection, an increasing convergence between the operating systems for mobile devices and the "classic" operating systems for *desktops* can be observed. This is seen in the new Apple operating system Mountain Lion, which includes several iOS functions, as well as the new Windows 8, which has the same graphical user interface in the *desktop* and mobile version[48]. These statistics show that we are in a transitional phase between *desktop* systems and mobile systems. What is the significance of this for security? An analysis of iOS and Android helps illuminate this question:

- The Apple operating system is a proprietary system that works only on the company's own hardware. Unless users manipulate their iOS[49], they can only install applications from the iTunes Store or install in-house applications[50] without the app store if they participate in the iOS Enterprise Program. Anyone can develop applications for iOS. Before they can be placed on the market, however[51], they must first be analysed and accepted by Apple. Consequently, the applications are signed directly by Apple and offered in the iTunes Store. Users are, however, unable to view the rights assigned to an application.
- The Android system, in contrast, is based on an *open source* platform with a Linux core and can be operated on the hardware of a wide range of manufacturers. The main distribution point for applications is the Google Play Store (previously named Android Market[52]) – with a simple click, the user can install applications from any website[53]. Also for Android, anyone can develop applications. There is no verification process as in the case of Apple. Moreover, the developers *sign* the applications themselves. The end user has the possibility of viewing the application's rights (only, however, if the user surfs from the website to the Google Play Store, since the rights are typically not shown directly in the smartphone application).

[45] http://www.admin.ch/ch/d/sr/c780_1.html(as of 23 February 2012).

[46] http://weissbuch.ch/wb11press.html (as of 23 February 2012).

[47] A smartphone is a mobile telephone combining advanced functions, such as an Internet connection or the processing of personal data, with the basic function of a telephone. The other category of modern mobile phones is called "feature phones". These mobile phones have only a few additional functions. Their development is thus not as complex as that of smartphones.

[48] The next Windows 8 Metro appears to have already omitted the Start button, which has always been a favourite of Microsoft users: http://arstechnica.com/microsoft/news/2012/02/discoverability-windows-8-and-the-disappearance-of-the-start-button.ars (as of 23 February 2012).

[49] This operation is called "jailbreaking" in the iOS world.

[50] Thanks to the iOS Developer Enterprise programme, a business can, for instance, develop its own app store: https://developer.apple.com/programs/ios/enterprise/ (as of 23 February 2012).

[51] https://developer.apple.com/appstore/guidelines.html (as of 23 February 2012).

[52] The Android Market was replaced by Google Play Store at 7th March 2012

[53] This procedure is called "sideloading".

Symantec recently published a report[54] on how the two operating systems try to ensure the security of the end user. The report examined the following five main points:

1. **Traditional access control:** For example use of a password to gain access to the phone, or the possibility of having access to the device blocked after a certain period of inactivity.
2. **Origin of the applications:** Of primary interest here is the *digital signature*.
3. **Encryption:** Data encryption if the device is lost or stolen.
4. ***Sandboxing*:** The attempt to isolate the applications in such a way that they only have access to the processes they need.
5. **Rights of the applications:** Applications are only assigned the rights they absolutely need to fulfil their functions.

According to the report, the differences between the two systems are obvious. Briefly put, the significant factor is the origin of the applications. In this regard, there is a clear contrast between the two philosophies. Apple takes responsibility for the security[55] of the applications to be installed. On the other side, the *open source* approach taken by Android allows users to install any kind of application, but without much control or restrictions regarding the functioning or the required rights. One only need look at the first page of the Android Market to find games requiring authorisations that are entirely unnecessary for the purpose of the application. This includes the right to send and receive *SMSs*, to make calls, and to access the personal data stored on the device[56].

Another aspect is that protection from *malware* on a mobile device is very different from the protection one is used to on *desktop* systems. In future, the protection of mobile devices will have to be completely rethought, or the "old" ideas from the *desktop* systems will have to be implemented on mobile devices as well:

- Antivirus:
  On mobile systems, no antivirus protection is distributed with the operating system. On iOS, only Apple can offer such protection, since antivirus programmes must have access to all applications, which however is not granted to installed applications. In general, this is prevented by *sandboxing* and the granting of rights. On Android, the only effective antivirus programmes are subject to payment. Nevertheless, the free application by Creative Apps is the most frequently distributed antivirus app. According to a study by AVTest[57], it does not appear to have detected any single one of 172 tested *viruses*.
- Firewall:
  So far there have been no studies published analysing *firewalls* on mobile devices.
- Updates of the operating system and the applications:
  For devices with unmodified operating systems (i.e. without *jailbreaks* or modified *ROM*), only Apple and some hardware manufacturers implementing Android regularly offer

[54] http://www.symantec.com/podcasts/detail.jsp?podid=b-a-window-into-mobile-device-security (as of 23 February 2012).

[55] At least in one case, namely that of the American researcher Charlie Miller, it was possible to shut down the security of the app store and publish a potentially malicious app: http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (as of 23 February 2012).

[56] An interesting example is that of Uloops, an application for composing music. In the description, the developers indicate that the application has access to the phone's status and identity. It can import a large amount of personal data, including the internal ID of the phone, the model, brand, username, password and e-mail. https://market.android.com/details?id=net.uloops.android&feature=featured-apps#?t=W251bGwsMSwxLDIwMywibmV0LnVsb29wcy5hbmRyb2lkIl0 (as of 23 February 2012).

[57] http://www.av-test.org/fileadmin/pdf/avtest_2011-11_free_android_virus_scanner_english.pdf (as of 23 February 2012).

updates. Most of the hardware manufacturers using the Google system are not willing to do so. Consequently, any vulnerabilities exist until the user buys a new device.

So end users have a difficult choice: Either they decide to trust Apple and to work with a closed system[58] without great "freedoms", or they decide on an *open source* system with all its advantages and disadvantages[59], characterised by openness and few restrictions.

5.5 Attacks on certificate service providers and their impact[60]

The secure use of cryptosystems with public keys ("public key cryptography") hinges on the security of the CSPs and PKIs employed[61]. Accordingly, the security of CSPs and PKIs has always been an issue to be dealt with by security technicians. The focus of interest has been on scenarios involving either forged certificates (using weaknesses in the collision resistance of the cryptographic hash functions employed[62]) or abuse of code signing certificates. In the second case – as the Stuxnet worm showed – such a certificate for instance allows malware to be smuggled into an operating system in the form of digitally signed driver software. The most recent attacks on CSPs have now shown, however, that the compromising of a CSP for the purpose of issuing false certificates constitutes a real threat. Large-scale *Man-in-the-Middle* (MITM) attacks can be carried out with the help of bogus SSL/TLS server certificates. He then has full control over the transmitted data and may also decrypt them and show them in plain text.

Where – as in the cases described above – bogus certificates are issued, two points must first of all be taken into account:

- On the one side, all certificate revocation mechanisms employed on the basis of revocation lists (CRLs and/or OCSP queries) fail for such certificates. A bogus (i.e. falsely issued) certificate is not necessarily blocked and accordingly cannot be recognized as such. In this regard, a way to distinguish authorized (i.e. properly issued) from non-authorized certificates would need to be found.

- On the other side, it has been shown that the (centralized and hierarchical) trust model of ITU-T X.509 is fundamentally problematic. If in this model a CSP or a Root CA recognized as trustworthy is compromised, all entities relying on that CA (in the extreme case, this may be all Internet users) are affected. In terms of security technology, everyone is in the same boat, and the probability that a Root CA is compromised increases with the length of the list.

[58] In addition to the advantages and disadvantages of the iOS architecture and market model, possible surprises such as the sending of GPS position data must be mentioned. Without the user's knowledge, the data are transmitted to Apple during the backup: http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/ (as of 23 February 2012).

[59] Also in this case, other factors in addition to the architecture and the market model must be taken into account. Android lets the provider decide whether to change the operational system or to install applications before selling the phone. This is true for instance of the application Carrier IQ, which is pre-installed on some Android devices. It extensively records the behaviour of the user and notifies it to the provider: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/ (as of 23 February 2012).

[60] Excerpt from the technical report of that name at http://www.melani.admin.ch/dokumentation/00123/01132/index.html?lang=en

[61] In this sense, CSPs and PKIs represent an Achilles heal of public key cryptography.

[62] This point is discussed in more depth in "Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen“ dated 4 August 2010: http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de

After these preliminary remarks, the question arises as to which precautions can be taken to prevent MITM attacks as best as possible under the circumstances. Since only few approaches are available for preventing MITM attacks, one must attempt to make MITM attacks as difficult and complex as possible for the attackers. In this respect, it is vital to discern whether changes can be made to the trust model or not.

- If no changes can be made to the trust model, then it is advisable to work with predominantly empty lists of trustworthy Root CAs or with a selective inclusion of only specific Root CAs. Google began using this option with Chrome version 13 under the term "public key pinning". If the approach is to be generalized to arbitrary domains, then a connection with the Domain Name System (DNS) makes sense.

- If changes can be made to the trust model, then in principle new solutions may be considered. A trust model would make sense in this regard in which compromising would have only local consequences. Such a model would necessarily have to be distributed and support dynamic trust relationships. Researchers at Carnegie Mellon University have shown, for instance, that attacks usually take place locally, and that bogus certificates can therefore be identified in a comparison with geographically distributed notary services.

Like every socio-technical system, a CSP also has weaknesses and vulnerabilities that can be addressed and exploited (in a more or less targeted way) by attacks. The weaknesses and vulnerabilities in this regard refer less to the cryptographic methods and mechanisms employed than to the interfaces with the relevant processes for issuing and outputting certificates. Attacks are conceivable here and – as the recent attacks document – also realizable. Counterfeiters of banknotes can be considered as an analogy: They can either counterfeit banknotes or – what would be more complicated and costly – break into a banknote printing facility and misuse the machines to print regular banknotes. Obviously, while the second option is more difficult to realize, it is all the more lucrative. An analogous attack has now succeeded in the PKI realm, and it is possible and even probable that such attacks and similar ones will succeed again in future. Accordingly, it is worth including such contingencies in the considerations regarding the design of future PKIs.

6 Glossary

.htaccess	.htaccess ("hypertext access") is a configuration file of an Apache webserver in which directory-specific settings can be specified.
404 error page	An error page is a web page displayed when the user clicks on an Internet link that no longer works, for instance, or that calls up a non-existent URL. Most browsers display the standard page supplied by the webserver. Error pages may be individually designed by the site's webmaster.
AcceptPathInfo	Setting in the Apache webserver.
Admin interface or administration panel	The admin interface is a graphical user interface with which an administrator can change settings.
Advanced persistent threat	This threat results in very great damage impacting a single organisation or a country. The attacker is willing to invest a large amount of

	time, money and knowledge in the attack and generally has substantial resources.
Apache webserver	The Apache HTTP Server is an open source, free product of the Apache Software Foundation and is the most used webserver on the Internet.
Backdoor	"Backdoor" refers to a software feature that allows users to circumvent the usual access control of a computer or of a protected function of a computer program..
Backup	"Backup" means the copying of data with the intent of copying them back in the event of data loss.
Base64	Base64 describes a procedure for coding 8-bit binary data (e.g. executable programmes, ZIP files) as a sequence of characters consisting only of readable, code-page independent ASCII characters.
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.
Bot / Malicious Bot	Comes from the Slavic word “robota” meaning work. Refers to a program that automatically carries out certain actions upon receiving the command. So-called malicious bots can control compromised systems remotely and have them carry out arbitrary actions.
Browser	Computer programs mainly used to display Web content. The best-known browsers are Internet Explorer, Opera, Firefox und Safari.
Building management system	A building management system (BMS) is software used to visualise and control a building with building automation. The usual functions of a building management system include the control of lighting and air conditioning systems.
Certificate authority	A certificate authority is an organisation issuing digital certificates. A digital certificate is the cyberspace equivalent of a personal ID, so to speak, and serves to assign a certain public key to a person or organisation. This assignment is certified by the certificate authority with its own digital signature.
Certification service provider (CSP)	See certificate authority.
Code	Program instructions that tell the computer what commands to carry out.

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.
Control system	see SCADA
Cryptosystem	A cryptosystem is a system used for encryption. Cryptography originally referred to the science of encrypting information.
Data retention	"Data retention" means the storage of personal data by or for public authorities, even though the data are not currently needed.
Desktop	A desktop computer, or "desktop", is a computer designed so that it can be used as a workplace computer on a desk.
Dial-Up	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).
DNS-System	Domain Name System .With the help of DNS the internet and its services can be utilised in a user-friendly way, because users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
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.
Driver software	A device driver, or simply "driver", is a computer programme or software module that controls the interaction with connected devices.
Dual use good	"Dual use" is a term primarily used in export control, designating the use of an economic good (e.g. a machine, but also software and technology) for both civilian and military purposes in principle.
Event Viewer	Program that displays the error messages and notices of the Windows operating system.
Exploit	A program, a script or a line of code with which vulnerabilities in a computer system can be used to advantage.

Financial agent	A financial agent works as a legal money broker and thus engages in financial transfers. Recently, this term has been used in connection with illegal financial transactions.
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.
Geo-restrictions	Restrictions for instance in regard to access to websites based on the country assignment of the IP address one uses.
Hard disk	A hard disk is a magnetic storage medium for computers, which writes the data on the surface of a rotating disk.
IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
ITU-T X.509	X.509 is an ITU-T standard for a public key infrastructure for the issuing of digital certificates.
Jailbreak	Jailbreaking is used to overcome the network restrictions on Apple products by using suitable software.
Lawful interception	"Lawful interception" refers to the surveillance possibilities of states in regard to telecommunications, e.g. in the form of voice, text, images and videos.
Live CD	A live CD contains a bootable operating system.
Log file	A log file contains the automatically maintained log of all or specific actions of processes on a computer system.
Malicious Code	Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses. See also Malware.
Man-in-the-middle attacks	Man-in-the-middle attacks (MITM) Attacks in which the attacker infiltrates unnoticed the communication channel between two partners and is thereby able to spy on or even modify their data exchanges.
Open Source	Open source is a range of licences for software whose source code is publically available. Further developments are encouraged by the

	licence.
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.
Public Key Infrastructure	Infrastructure for the management and use of digital certificates.
Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts or deletes data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
Recovery process	The recovery of original data after data loss.
ROM	Read Only Memory. Memory in which data can only be read, but not altered.
Root CA	Central certificate authority
Root certificate	Certificate serving to validate all subordinate certificates.
Router	Computer network, telecommunication, or also Internet devices used to link or separate several networks. Routers are used, for instance, in home networks, establishing the connection between the internal network and the Internet.
Sandboxing	Sandboxing is a technique generating a separated environment on a computer, which can be used to execute untrusted programmes.
SCADA systems	Supervisory Control And Data Acquisition Systeme. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
Screenshot	A screenshot in ICT is the storage of the current graphical content of the screen.
Server	Computer system which provides clients with certain resources or data, such as storage space, services (e.g. e-mail, internet, FTP, etc.).
Sign/signature/digital signature	An electronic signature is data associated with electronic information, where such data is used to identify the signer or creator of the signature and to verify the integrity of the signed electronic

	information.
Smart grid	Smart grids are intelligent (electricity) grids that report data from various devices on the grid (typically meters installed at the user's location) to the operator. Depending on the design, commands may also be issued to these devices.
Smart meter	A smart meter is an energy meter that displays the actual energy use and actual usage period to an energy consumer; the information can also be transmitted to the energy supplier.
Smartphone	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.
Spam	Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L’aggressore tenta di intro-durre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
SSL/TLS server certificate	A digital certificate is the cyberspace equivalent of a personal identification card and serves to assign a specific public key to a person or organisation. This assignment is certified by the certificate authority with its own digital signature.
Symmetric encryption	In contrast to asymmetric encryption, both participants in symmetric encryption use the same key.
Tweet	Messages sent using the Twitter communication platform.
URL manipulation	With certain manipulations of the URL, a server can be made to display pages that are actually blocked.
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).
Virus	A self-replicating computer program with harmful functions that attaches itself to a host program or host file in order to spread.
VoIP	Voice over IP. Telephony via internet protocol (IP). Frequently used protocols: H.323 and SIP.