



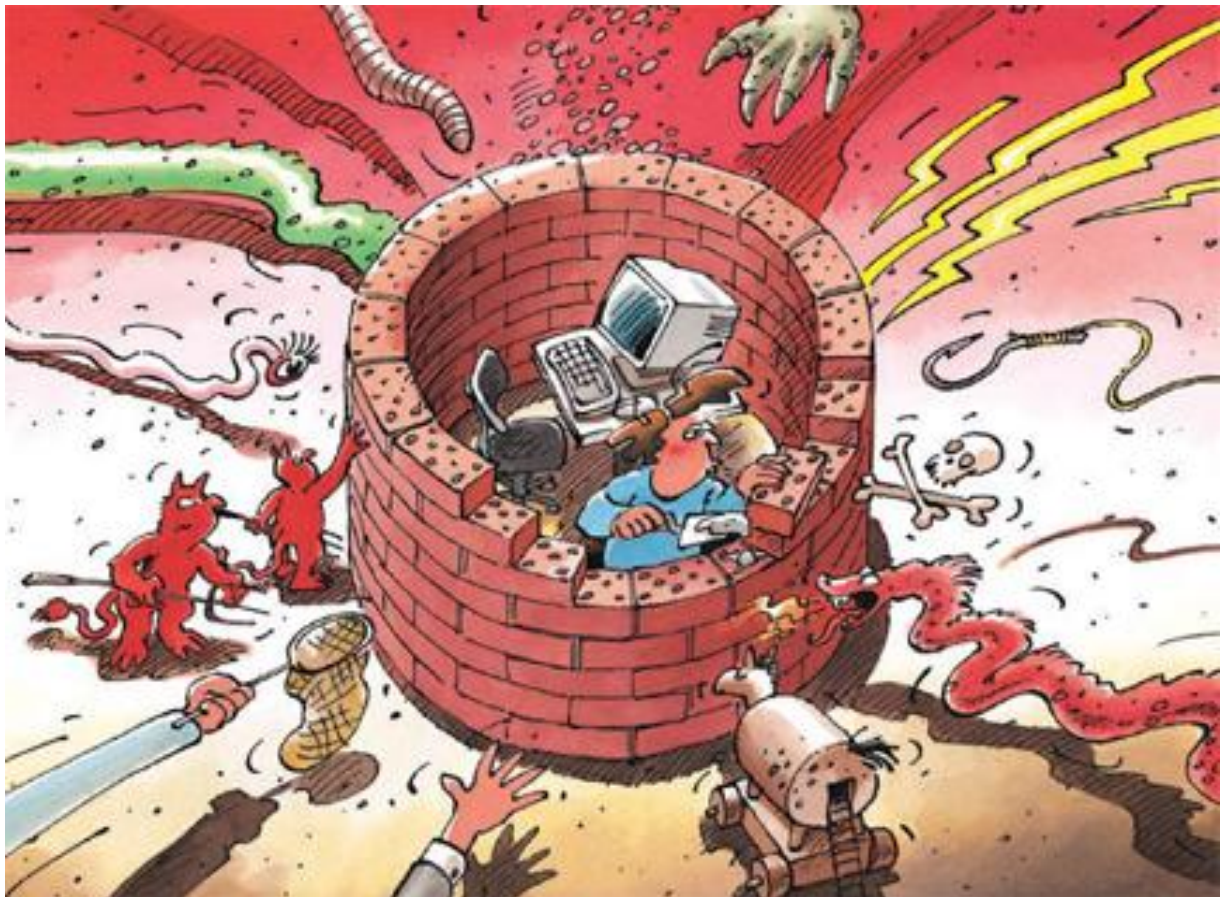
---

# Information Assurance

## Situation in Switzerland and internationally

Semi-annual report 2012/I (January – June)

---



# Contents

<b>1</b>	<b>Focus areas of issue 2012/I</b>	<b>3</b>
<b>2</b>	<b>Introduction</b>	<b>4</b>
<b>3</b>	<b>Current national ICT infrastructure situation</b>	<b>5</b>
3.1	ICT breakdowns in the private and public sectors	5
3.2	E-mail account takeovers – scammers react to measures taken by e-mail providers	6
3.3	Surge of ransom trojans	7
3.4	Voice phishing (vishing)	9
3.5	How phishers obtain e-mail addresses	10
3.6	Phishing e-mails – purported tax refund by the Federal Tax Administration	11
3.7	E-voting incidents	12
3.8	Malware with certificate purportedly issued by Swiss company	13
3.9	Federal Council adopts national strategy to protect Switzerland from cyber risks	14
<b>4</b>	<b>Current International ICT Infrastructure Situation</b>	<b>16</b>
4.1	Iran in the cross hairs? Flame and Wiper	16
4.2	Hactivism in the Middle East	16
4.3	Anonymous announced attack against the Internet – no measurable impact	17
4.4	Protests against ACTA – also on the Internet	18
4.5	Large volumes of passwords and credit card data stolen	19
4.6	Update on SCADA	21
4.7	Establishment of a European Cybercrime Centre	22
4.8	Deactivation of a Zeus botnet	23
4.9	Drive-by downloads spread using web banners	23
<b>5</b>	<b>Trends / Outlook</b>	<b>24</b>
5.1	Conflation of business and private ICT – a security risk?	24
5.2	Cyber conflict in the Middle East	25
5.3	Data theft: attacks against many small and a few large companies	26
5.4	Client communication in the age of phishing	27
5.5	E-voting in Switzerland – experiences so far	30
<b>6</b>	<b>Glossary</b>	<b>31</b>

# 1 Focus areas of issue 2012/I

- **Large volumes of passwords and credit card data hacked**

The first half of 2012 was again characterised by major attacks on well-known companies during which client data – usually usernames and passwords but also credit card data – was stolen. These cases, some of which were very spectacular, are in contrast to the numerous attacks on small businesses and their data that happen every day and are not reported in the media. According to a study by Verizon, more than 75% of attacks target SMEs with fewer than 1,000 employees.

▶ Current situation internationally: [Chapter 4.5](#)

▶ Trends / Outlook: [Chapter 5.3](#)

## **Different variants of phishing**

Phishing attacks are observed on a daily basis in Switzerland. In most cases, these e-mails induce clients to enter their credit card data. As a recent case shows, the scammers automatically comb through Swiss guest books and forums to find valid e-mail addresses to which the phishing e-mails are sent. But also voice phishing attacks, in which scammers pretend to be ICT support staff and ask the victims to give them access to their computers, have been observed frequently in Switzerland for about a year. When criminals use phishing to obtain the e-mail login data of a person, they use the data to send bogus calls for help to all contacts in the compromised e-mail address book.

All these incidents demand greater company sensitivity when communicating with their clients. If certain basic corporate communication rules are disregarded, clients may quickly classify newsletters as supposed phishing e-mails.

▶ Current situation in Switzerland: [Chapter 3.2](#), [Chapter 3.4](#),  
[Chapter 3.5](#), [Chapter 3.6](#)

▶ Trends / Outlook: [Chapter 5.4](#)

## **Cyber conflict in the Middle East**

At the end of May, the complex malware "Flame" was discovered, which was used to attack and spy on organisations in several countries in the Middle East. The technical analysis by security firms uncovered various similarities among Flame, Stuxnet and Duqu.

With the open conflicts that have erupted since the beginning of the Arab Spring, the aggressive and offensive use of ICT resources and the Internet has also increased. Cases regularly become known in which websites are brought down, government or private documents stolen and published, or sabotage malware is employed.

▶ Current situation internationally: [Chapter 4.1](#), [Chapter 4.2](#)

▶ Trends / Outlook: [Chapter 5.2](#)

- **E-voting incidents**

It is clear that in the Internet age citizens expect the state to offer public votes and elections electronically. Nevertheless, there are certain fundamental differences between e-voting and other e-services such as e-banking.

▶ Current situation in Switzerland: [Chapter 3.7](#)

▶ Trends / Outlook: [Chapter 5.5](#)

- **National strategy to protect Switzerland from cyber risks**

On 27 June 2012, the Federal Council adopted the national strategy to protect Switzerland from cyber risks.

▶ Current situation in Switzerland: [Chapter 3.9](#)

## 2 Introduction

The fifteenth semi-annual report (January – June 2012) of the Reporting and Analysis Centre for Information Assurance (MELANI) presents the most significant trends involving the threats and risks arising from information and communication technologies (ICT). It provides an overview of the events in Switzerland and abroad, sheds light on topics in the area of prevention, and summarises the activities of public and private players. Explanations of jargon and technical terms (in *italics*) can be found in a **glossary (Chapter 6)** at the end of this report. Comments by MELANI are indicated in a shaded box.

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

**Chapters 3 and 4** discuss breakdowns and failures, attacks, crime and terrorism connected with ICT infrastructures. Selected examples are used to illustrate important events of the first half of 2012. Chapter 3 discusses national topics; Chapter 4 international topics.

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

## 3 Current national ICT infrastructure situation

### 3.1 ICT breakdowns in the private and public sectors

Breakdowns triggered by incorrect handling or technical failures are one of the most frequent causes of information infrastructure outages. As a rule, critical systems are designed redundantly in order to prevent outages. As events in the past have shown, redundancy generally works well for hardware outages. This is only somewhat true of software breakdowns. Since roughly the same software and configuration run on redundant systems, it is possible that the same problems will arise on the backup system as on the main system, and that the backup system will also crash.<sup>1</sup> Again in the first half of 2012, several breakdowns in Switzerland made the headlines:

#### *IT breakdown in the public administration of the Canton of Bern*

On 8 May 2012, a key component in the network of the public administration of the Canton of Bern failed, bringing down several important systems for more than 24 hours and causing various services to be unavailable. For instance, the driver and vehicle licensing office had to suspend all services. Also affected were the online portal (TaxMe) for accessing and filling out tax returns electronically, the real estate information system (GRUDIS), the geographical data information system (*Geoportal*), data on the water levels of rivers and lakes, and the official compilation of legislation. Data loss was prevented, however.

The malfunction was caused by a software error in the operating system (microcode) of a central memory system. This error also knocked out the existing redundancies of data storage, such as dual system components and data mirroring in a remote data centre.<sup>2</sup>

#### *Coop shops without checkout systems*

On 4 April 2012, all Coop shops in German-speaking Switzerland had problems with their checkout systems. They were unavailable for two hours. The shops remained closed or free croissants were handed out to waiting customers. The breakdown was caused by a faulty software update which had been installed overnight and had gone unnoticed in the subsequent tests.

#### *Delayed start of trading at the Swiss Exchange*

On Friday, 13 January 2012, the Swiss Exchange was unable to begin trading at the usual time. While the error was fixed before the opening hours, the recovery process with all involved parties took some time and the trading couldn't start before noon. While the cause of the malfunction was discovered, the operator of the Swiss Exchange – SIX – did not want to communicate it publically. According to SIX, only a handful of exchange participants were

---

<sup>1</sup> MELANI Semi-annual report 2009/1, Chapter 4.6:  
<http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=en> (as of 31 August 2012).

<sup>2</sup> [http://www.be.ch/portal/de/index/mediencenter/medienmitteilungen.meldungNeu.html/portal/de/meldungen/m/2012/05/20120509\\_1347\\_alle\\_dienstleistungensindwiederverfuegbar](http://www.be.ch/portal/de/index/mediencenter/medienmitteilungen.meldungNeu.html/portal/de/meldungen/m/2012/05/20120509_1347_alle_dienstleistungensindwiederverfuegbar) (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

affected. On grounds of market integrity and fairness, however, the decision was made to suspend all trading.

This was not the first time trading had to be suspended due to technical problems. On 12 November 2009, the Swiss Exchange had to be closed already at 3 p.m. and trading stopped.<sup>3</sup> Despite these incidents, the outage of a stock exchange should be considered an extremely rare event.

These examples clearly show how dependent the private sector – but also the public sector – is on failure-free ICT operations. Already small outages can cause great financial damage. It is important to have solid ICT infrastructure and above all to be able to fix malfunctions as quickly as possible. According to a nationwide study carried out by the ETH Zurich in 2005, a national outage of the entire Internet for one week would cause losses to the economy amounting to CHF 5.83 billion.<sup>4</sup> Since outages can never be ruled out, careful continuity planning is indispensable precisely for such services.

### 3.2 E-mail account takeovers – scammers react to measures taken by e-mail providers

Already for more than three years now, cases have been observed where stolen data is used to access the e-mail accounts of victims. The scammers look around the e-mail account and then write e-mails to all or targeted contacts in the victim's address book. These e-mails are usually bogus calls for help, claiming that the sender is stuck somewhere in a foreign country and that his or her money and passport have been stolen. Finally, the e-mail asks the recipient to send money as quickly as possible:

"I hope you get this in time. Sorry I didn't tell you about my trip to Spain. I'm now in Spain and am in trouble because I lost my wallet."

Image 1: Text of a scam e-mail sent to all contacts of a compromised e-mail account.

The case of Verena Koshy, a politician from Köniz (Canton of Bern), in the first half of 2012 showed that even politicians are not immune to such attacks. Although a person whose e-mail account has been hacked does not suffer a direct financial loss, these incidents are always annoying and cause major inconvenience – especially for people who have a wide network and have saved many contacts. Many addressees received the bogus call for help from Ms. Koshy. If such an incident is noticed, the addressees should be informed and warned as quickly as possible, and the victim should immediately contact the *provider* to take measures to restore account access for the victim. Providers generally react within 24 to 48 hours, after which the scammers no longer have control over the hacked account.

Unfortunately, scammers have also realised that the blocking of accounts and warnings to recipients limit their chances for success. They have taken countermeasures accordingly in recent months and adjusted their approach. While they still steal contact data from the hacked e-mail account, they change a small detail in the sender's address – for instance "Neier" instead of "Meier" – so that the recipient doesn't notice. The attacker sets up this address in advance to perpetrate the scam. Unlike the hacked account, the attacker

---

<sup>3</sup> <http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Technische-Probleme-legen-Boerse-lahm/story/30392767> (as of 31 August 2012).

<sup>4</sup> <http://www.ethz.ch> (as of 31 August 2012).



## Information Assurance – Situation in Switzerland and internationally

continues to have access to the separate account even after measures have been taken and can communicate with the victims indefinitely until the scam is complete.

Another change is that scammers subsequently delete all contacts and all e-mail messages from the hacked accounts. This is an attempt to prevent the actual owner of the account from warning all contacts once access has been restored. This fact is a major inconvenience for the victim, since in most cases no *backup* of the contact list and e-mail messages exists. In some cases, the provider is able to save the data, but in most cases the data is lost forever.

Here are some tips to limit damage in the event of a scam.

1. Create a *backup* of the contacts so that an alternative e-mail address can be used if the account is attacked. This allows contacts to be warned about the fraudulent e-mails as quickly as possible.
2. Select the e-mail provider carefully, especially if the e-mail address is to be used professionally.
3. If a scam occurs, immediately try to regain access to the account. In most cases, the alternative e-mail address will also have been changed, however. If this is not the case, a replacement password can be sent to that e-mail address. But if the alternative address has also been changed, a *recovery process* must be started. For this purpose, most e-mail providers make a *recovery form* available. Here is a non-exhaustive list of the most popular e-mail providers:

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

### 3.3 Surge of ransom trojans

MELANI reported on *ransom trojans* already in the last semi-annual report.<sup>5</sup> *Ransom trojans* are *ransomware* (extortionate *malware*) that block the computer and demand ransom money. This type of trojan surfaced first in Germany in spring 2011 and included the logo of the German Federal Criminal Police Office (BKA). This gave rise to the nickname "BKA Trojan" for the *malware*.<sup>6</sup> This rather unfortunately chosen name of course has nothing to do with the *law enforcement trojan* of the German Federal Criminal Police.

The first Swiss version of this trojan was sent last autumn in the name of the Federal Department of Justice and Police (FDJP). At the beginning of March 2012, another type of *ransom trojan* was circulated, purporting to be from the Cooperative Society of Music Authors and Publishers, SUISA, which serves as the collecting society for copyrights in Switzerland.<sup>7</sup> Since June 2012, a version has also been circulated in the name of the (non-existent) "Cyber

---

<sup>5</sup> MELANI Semi-annual report 2011/2, Chapter 3.5:  
<http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en> (as of 31 August 2012).

<sup>6</sup> See <http://www.bka-trojaner.de> – this website provides information on the various versions (as of 31 August 2012).

<sup>7</sup> <http://www.suisa.ch> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

Crime Investigation Department". This malware even turns on the webcam and displays the victim's image on the blocked computer in a further attempt to intimidate the victim.

The trojan demands payment of a fine, generally via the online payment service Paysafe.

Paysafecard, the provider of the prepaid means of payment used by the scammers in these cases, has reacted to the misuse and now prints a warning message on its Paysafe cards.

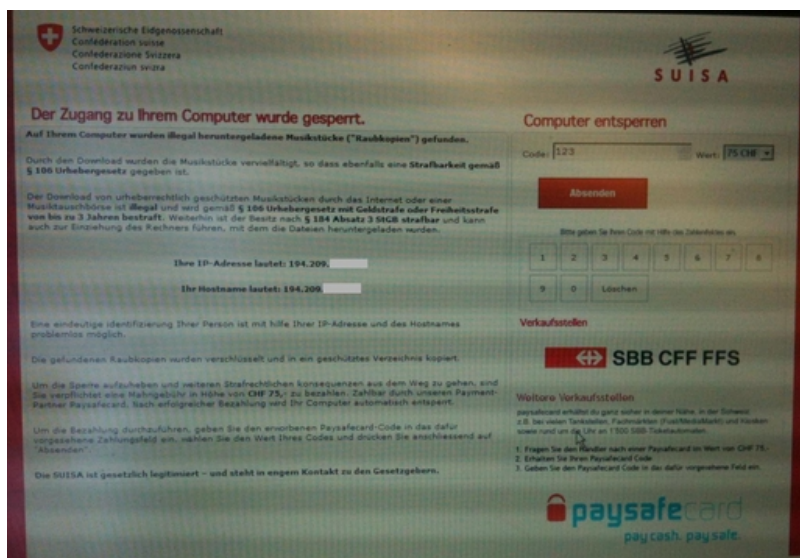


Image 2: Ransom trojan with SUIA logo



Image 3: Ransom trojan with logo of the Swiss Confederation

Since the first cases surfaced in Switzerland, the Reporting and Analysis Centre for Information Assurance (MELANI) has regularly received reports of blocked computers. The infection generally is spread via video portals or websites with multimedia content. It has to be assumed that the infections are carried out using contaminated video files or compromised video players, for instance.

The infection and blocking of a computer is always an inconvenience, especially if the computer is indispensable for the operations of a small business and cannot simply be exchanged. MELANI knows of such cases.

MELANI is also aware of cases where the block can be circumvented easily. If the system is shut down and rebooted without an Internet connection, it has sometimes been possible to circumvent the block.



### 3.4 Voice phishing (vishing)

*Voice phishing* was long non-existent in Switzerland, but cases have been registered more frequently since summer 2011. In its last semi-annual report, MELANI discussed these calls in detail.<sup>8</sup> The approach currently taken by scammers is almost always the same. The victim receives a call from a purported computer support company (usually Microsoft), claiming that the victim's computer has been sending out suspicious messages. To "prove" this, the scammers typically instruct the victims to launch the computer's *Event Viewer*, which displays internal messages of the operating system. Even a perfectly functioning system occasionally generates error messages. Depending on the age and configuration of the computer, the list of error messages in the Event Viewer may be very long even though the system does not have any fundamental problems. The launch of this program is typically used by the "support" callers to present a believable background and scare the victim. The scammers' goal is to convince the callee to download a *remote access tool* providing remote access to the computer. In this way, the scammers obtain full access to the system and the same possibilities of manipulating the system as if they were sitting directly in front of it. Finally, the scammers usually try to sell victims a software license or a service ("system cleaning") and thereby obtain their credit card information.

If the victim has reacted to a telephone call like this and provided credit card data to the scammers, it is especially important to block the credit card immediately.

It is generally difficult to assess what the scammers have done or installed on the computer. If the scammers were given access via a *remote access tool*, then they had the same possibilities of manipulating the computer as if they were sitting directly in front of it (copying/manipulating/deleting data, installing programs, etc., or also establishing a *back door* to access the system at a later time).

If such an incident occurs, it is recommended to have the computer checked by a specialist. But this does not guarantee that any *malware* or other manipulations of the system can be found. The most secure method is to completely delete the computer's hard disk and reinstall the operating system. Personal data should be backed up first, however, so that it is not lost.

After cleaning/reinstalling the computer (or from another computer), the passwords of all Internet services previously used on that computer should also be changed.

#### *Vishing in the name of Swisscom*

In July 2012, an e-mail was circulated in the name of Swisscom. In bad German but better French, victims were told that something was wrong and that their account had been "inhibited" (i.e. blocked). Unlike classic *phishing* e-mails, the message did not ask for usernames and passwords, but rather provided a telephone number to call for additional information. The number with the calling code 0088 belongs to a satellite phone provider. High costs are guaranteed if a call is made. It could not be determined whether victims were asked for their usernames and passwords if they called. Swisscom has blocked those phishing e-mails for their costumers at an early stage.

---

<sup>8</sup> MELANI Semi-annual report 2011/2, Chapter 3.1:  
<http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

**Gesendet:** Dienstag, 10. Juli 2012 01:19

**Betreff:** Sie haben 1 neue Nachricht / Vous avez 1 nouveau message

**Ihr Konto ist gehemmt worden.**

Für mehr Informationen erreichen Sie uns unter der Telefonnummer:  
00881835211648 oder 00881835211650

**Votre compte a été suspendu.**

Pour de plus amples informations, vous pouvez appeler le numéro de téléphone:  
00881835211648 ou 00881835211650

Image 4: E-mails sent in the name of Swisscom in July 2012

### 3.5 How phishers obtain e-mail addresses

There are different ways for e-mail addresses to end up in a spam database. One of the ways is to comb the Internet automatically for valid e-mail addresses published on websites (e.g. forums or guest books, etc.). Once an e-mail address has ended up in a spam database, it is used multiple times by criminals and often sold to other scammers as well.

Operators of forums and guest books play an important role in this regard that is often underestimated and neglected, as most guest books still display e-mail addresses in plain text and can be extracted very easily by criminals using suitable tools.

An analysis of the recipient e-mail addresses of a recent phishing e-mail wave shows that these sources are in fact used. In this case, the e-mail addresses used by the scammers could be matched with entries in guest books on Swiss websites. Some of the guest books turned out to be veritable goldmines for the address collectors. The website of one Swiss musician, for instance, contains more than 2,700 e-mail addresses published in plain text. This has the additional advantage for scammers that these e-mail addresses most probably belong to Swiss citizens or at least people who speak German. With this information, phishing e-mails can be drafted in a more targeted manner, increasing the probability that the attack succeeds.

MELANI recommends the following measures for handling e-mail addresses in guest books and forums:

*On the part of the web administrator*

- In many cases, it is unnecessary to publish the e-mail address since it serves solely as a means of authentication for the website administrator. In such cases, the e-mail address should not be published.
- If publication is necessary so that the owner of the e-mail address can be contacted, do not publish the address in plain text. There are several options, for instance with the help of JavaScript, to prevent the automatic reading of e-mail addresses.
- The most efficient option is to refrain from publishing the address and instead to make a (secure) web form available for contacting the address owner.

On the part of the user

- Give your e-mail address to as few people as necessary and use the address solely for important correspondence.

### 3.6 Phishing e-mails – purported tax refund by the Federal Tax Administration

Using various tricks, attackers try to make the life of security authorities entrusted with preventing *phishing* attacks as difficult as possible. MELANI reported on this already in the last semi-annual report.<sup>9</sup> Another variation is the following approach.

On Monday, 4 June 2012, scammers sent out *phishing* e-mails in the name of the Federal Tax Administration (FTA). The e-mails promised the recipients a tax refund. An *HTML form* was attached to the e-mail. Once the form was opened, the user was asked to enter personal and credit card data. Unlike classic *phishing* e-mails which ask users to click on a link to enter personal and credit card data on a separate phishing page, the *HTML* page in this case was simply included with the e-mail as an *attachment*. Opening the *HTML* page generates it locally on the recipient's computer. When the fields on the form are completed and the user clicks on the "Next" button, the data is sent "directly" to the attacker.

The advantage for attackers is that they do not need a hacked or specially created *web server* for these purposes on which the phishing page would otherwise have to be placed and which of course could be deactivated by security authorities or the hosting provider. All of the phishing website information is simply included in the *attachment*. The only thing still needed is a *PHP mailer*, thousands of which are available unencrypted on the Internet and which can be used to send data to any number of e-mail addresses. Clearly, mailers of this kind are more difficult to block or secure.

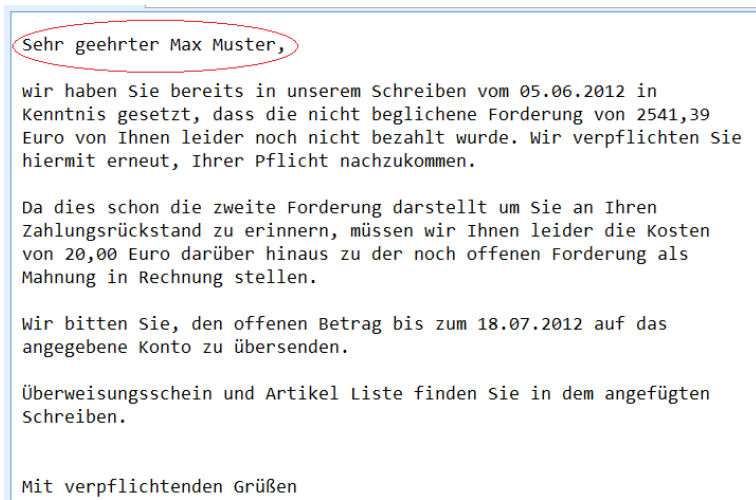


Image 5: Phishing e-mail with attached input screen

<sup>9</sup> MELANI Semi-annual report 2011/2, Chapter 3.4: <http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

For a long time, it was expected that fraudulent e-mails would contain a personal salutation to make a more trustworthy impression on the victim. Surprisingly, this has in fact been observed only in exceptional cases so far. One example using this method was an e-mail wave in summer 2012 where an attempt was made to spread the malware in the *attachment*:



Sehr geehrter Max Muster,

wir haben Sie bereits in unserem Schreiben vom 05.06.2012 in Kenntnis gesetzt, dass die nicht beglichene Forderung von 2541,39 Euro von Ihnen leider noch nicht bezahlt wurde. Wir verpflichten Sie hiermit erneut, Ihrer Pflicht nachzukommen.

Da dies schon die zweite Forderung darstellt um Sie an Ihren Zahlungsrückstand zu erinnern, müssen wir Ihnen leider die Kosten von 20,00 Euro darüber hinaus zu der noch offenen Forderung als Mahnung in Rechnung stellen.

Wir bitten Sie, den offenen Betrag bis zum 18.07.2012 auf das angegebene Konto zu übersenden.

Überweisungsschein und Artikel Liste finden Sie in dem angefügten Schreiben.

Mit verpflichtenden Grüßen

Image 6: Example of an e-mail with malware and personal salutation

In principle, it can be assumed that serious companies will never ask their clients for passwords by e-mail or ask them to verify or update their credit card, account or other personal information. E-mails of that sort are generally sent by scammers. But scammers are always thinking up new scenarios to lure recipients into reacting without thinking. See also Chapter 5.4 on "Client communication in the age of *phishing*".

If you unexpectedly receive suspicious e-mails or messages from unknown senders, do not under any circumstances follow the instructions in the text, do not click on attachments, and do not follow any links. Delete the message instead.

## 3.7 E-voting incidents

Exercising direct democracy is one of the most precious assets of any Swiss citizen. This includes e-voting, i.e. the possibility of casting votes electronically. The advantage is obvious: participation in political decision-making processes such as popular votes is not limited to the opening hours of polling stations and is possible from anywhere in the world.

It is therefore unsurprising that apart from Switzerland, other countries including in particular Norway, Estonia, and France are conducting promising trials with electronic voting.

However, rumours of manipulation can call into question the trustworthiness of e-voting and endanger it for the long term. Already simple attacks such as *DDoS* attacks can have far-reaching consequences and delay a democratic vote or even prevent it. Chapter 5.5 discusses this issue in more detail.

The following examples of incidents took place in connection with e-voting systems in the first half of 2012:

### *Extra vote in Swiss e-vote*

After the federal popular vote on 11 March 2012, it became known that the vote of a citizen living in the Canton of Luzern had erroneously been saved twice owing to a software error. Apparently the error was noticed immediately, and the specialists were able to remove the

## Information Assurance – Situation in Switzerland and internationally

extra vote from the system. According to the press release, there was never a reason to doubt the accuracy of the final results, and voting secrecy had been maintained at all times<sup>10</sup>.

### *Attack against e-voting of the New Democratic Party in Canada*

In the leadership election of the New Democratic Party in Canada, the multi-stage election procedure was conducting using e-voting. Several tens of thousands of party members voted online from home. During the election, however, the servers were attacked using a DDoS, which delayed the process. The deadline for casting votes was extended several times; one of the election rounds even had to be suspended and later resumed. This most likely discouraged numerous eligible voters from participating.

### *Pilot project for online elections in the US capital Washington hacked*

In March 2012, researchers at the University of Michigan wrote that the security function of a pilot project for online elections in the US capital Washington could be cracked very quickly. The researchers claimed that 48 hours after the system had been launched they had gained practically complete control of the election server. They claimed to have been able to change any vote cast and gain access to nearly all of the secret ballot boxes. It took two days to discover the attack, and then only because the researchers had left obvious clues.

### *Constitutional Court of Austria annuls the ordinance on e-voting for Austrian Students' Association (ÖH)*

The Constitutional Court of Austria found the ordinance on e-voting for the Austrian Students' Association (ÖH) election of 2009 to be unlawful and voided it, as it failed to specify in sufficient detail how error-free functioning of the system could be verified. According to the Austrian Ministry of the Interior this decision has no path-breaking meaning, because e-voting for federal elections would first have to be provided for in the constitution. No constitutional majority for such an amendment appears to be on the horizon in Austria.<sup>11</sup>

## 3.8 Malware with certificate purportedly issued by Swiss company

Several versions of the Mediyes<sup>12</sup> malware surfaced between December 2011 and March 2012 with a *key certificate* issued by a company in Central Switzerland called Conpavi AG. On its website, the company claimed it was a partner of the city of Luzern and the Bern University of Applied Sciences for e-government projects.

---

<sup>10</sup> [http://www.ge.ch/evoting/scrutin\\_20120311.asp](http://www.ge.ch/evoting/scrutin_20120311.asp) (as of 31 August 2012).

<sup>11</sup> <http://www.heise.de/newsticker/meldung/Oesterreichs-Verfassungsgerichtshof-hebt-E-Voting-auf-1400214.html> (as of 31 August 2012).

<sup>12</sup> The malware Mediyes is an example of "click fraud malware": It intercepts search engine queries sent by the victim to Google, Yahoo and Bing and forwards them to a server of an ad network.

So that website operators can easily display advertisements on their sites and make money doing so, online ad firms make search functions available that can easily be included on a site. When a visitor searches for a term, an ad message is displayed in addition to the results on the website. If the visitor clicks on the suggested link, the website owner earns money.

This is what the scammers took advantage of, copying search queries to force the display of ads (on a website created especially for that purpose) and clicking on them automatically in the background to make money.



## Information Assurance – Situation in Switzerland and internationally

While Conpavi AG does exist and is entered in the commercial register, its declared aim is to engage in services and trading in the area of pharmaceutical goods. This has little to do with e-government. So is it indeed a bogus company invented by scammers solely for that purpose, as some media reported?<sup>13</sup>

The case does not appear to be that simple. A look at the *Internet archive engine* archive.org shows that the site conpavi.ch appeared in 2002 for the first time.



Image 7: Archive entries on archive.org concerning the company Conpavi

A closer look at the commercial register shows that the company was founded on 20 March 2000 under the name "netauc" and was renamed "conpavi" on 11 December 2001. The purpose of the company was to provide services relating to electronic means of communication, particularly advice on Internet issues for authorities.<sup>14</sup> On 16 June 2009, Conpavi was then transformed into a company offering services and trading in the area of pharmaceutical goods. However, the website of the old company with the old description of services was not removed. This gave criminals a nearly perfect platform to carry out their scams and to obtain *certificates*. Anyone failing to take a closer look might indeed have assumed that the company still existed and worked in the field of *e-government*. Accordingly, it was apparently also possible to convince the certificate authorities to issue a valid *certificate*.

Scammers try all possible ways to make their actions seem as credible as possible to victims. It frequently happens that company names or websites are used for scams after the company has been liquidated. Websites still have good links, and a Google search does not indicate any suspicious activities. Often, scammers also take over the *domain name* once it has been cancelled by the company, or if the domain registration has not been renewed. This gives scammers the opportunity to use the reputation a company enjoyed up to the time of its liquidation or change of name or purpose.

### 3.9 Federal Council adopts national strategy to protect Switzerland from cyber risks

On 27 June 2012, the Federal Council adopted the national strategy to protect Switzerland from cyber risks.<sup>15</sup> The measures supported by the Federal Council include additional staff for MELANI in the FDF and the DDPS starting in 2013. The adopted strategy also takes account of several parliamentary proposals calling for stronger measures against cyber risks.

<sup>13</sup> [http://www.nzz.ch/aktuell/startseite/zuger\\_scheinfirmaauf\\_krummer\\_tour\\_im\\_internet-1.16001018](http://www.nzz.ch/aktuell/startseite/zuger_scheinfirmaauf_krummer_tour_im_internet-1.16001018) (as of 31 August 2012).

<sup>14</sup> <http://www.zefix.admin.ch> (as of 31 August 2012).

<sup>15</sup> <http://www.news.admin.ch/message/index.html?lang=de&msg-id=45138> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

The Federal Council is pursuing the following strategic goals in this regard:

- early identification of threats and dangers in the cyber field,
- improvement of the resilience of critical infrastructures,
- effective reduction of cyber risks, especially cyber crime and cyber sabotage.

The strategy designates the competent federal offices to implement 16 of the measures enumerated in the strategy as part of their basic mandate by the end of 2017. This implementation process is to include partners from public authorities, the private sector, and society. A coordination office in the FDF will verify implementation of the measures as well as the need for further provisions to minimise risk.

National cooperation between the private and public sector as well as cooperation with foreign countries remains a precondition for minimising cyber risks. Mutual exchange of information on a permanent basis is to create transparency and trust. The state should only intervene where public interests are at stake or when acting in accordance with the principle of subsidiarity.

According to the strategy, dealing with cyber risks should be understood as part of an integrated business, production and administration process, in which all players – from the technical to the management level – must be included. Every organisational unit at the political, business and social level bears responsibility for identifying the cyber aspects of their tasks and responsibilities and for addressing or, where feasible, reducing the associated risks in their respective processes. The decentralised structures in the public and private sector are to be strengthened for this purpose, and existing resources and processes are to be used consistently. The on-going combination of technical and non-technical information is necessary to analyse and assess cyber risks comprehensively. These insights should be worked up centrally if possible and provided to players as needed to support their risk management processes.

The strategy identifies cyber risks mainly as a manifestation of existing processes and responsibilities. Accordingly, these cyber risks should also be incorporated into existing risk management processes. The primary goal is to strengthen the information basis concerning cyber risks and awareness thereof among the responsible persons and offices. For this purpose, the Federal Council is mandating the departments to implement the measures at their level and in cooperation and dialogue with cantonal authorities and the private sector. The measures extend from risks analyses to critical ICT infrastructures and greater inclusion of Swiss interests in this area at the international level.

The Federal Council recognises that cooperation between the public and private sector in Switzerland is well established and functions smoothly. With this national strategy to protect Switzerland from cyber risks, the Federal Council aims to strengthen this cooperation in the cyber field and further consolidate the existing foundation so as to minimise cyber risks in a targeted manner. It relies on the existing structures and does without a central steering and coordination body, as has been created in some other countries with less established cooperation among the relevant players. Instead, the information flow and holistic evaluation of available information on cyber risks and threats will be intensified to support public authorities, businesses and operators of critical infrastructure and to disseminate such information as needed. For this purpose, the Reporting and Analysis Centre for Information Assurance (MELANI) is to be strengthened.

## 4 Current International ICT Infrastructure Situation

### 4.1 Iran in the cross hairs? Flame and Wiper

On 28 May 2012, Kaspersky Lab reported the discovery of a very complex *malware* used to attack and spy on organisations in several countries. The functions of this *malware* include collecting information of all kinds. For instance, it can monitor network traffic, log keystrokes, record audio, and even read the address books of nearby cell phones via *Bluetooth* if the phone's Bluetooth connection is active. The *malware*, called "Flame", was active especially in the Middle East. Nearly half of the proven infections were in Iran. Initial versions go back to the year 2006 – accordingly, the espionage network was able to work for more than five years without being discovered. This was possible in part because the attackers always only infected a few dozen systems at a time and deleted Flame after obtaining data from the infected systems. Consistent with this strategy, the attackers shut down the control infrastructure of the espionage network to erase their tracks once the discovery of the *malware* was made public by Kaspersky Lab.

More than 80 *domain names* were registered for the control infrastructure over the duration of the attacks, and servers around the world were used, including in Hong Kong, Vietnam, Turkey, but also Germany, England and Switzerland.

Flame was spread via *USB sticks* and local networks. For the infection via *USB sticks*, the same vulnerability was used as for Stuxnet. Technical analysis by security firms also uncovered various further similarities among Flame, Stuxnet, and Duqu.<sup>16</sup>

A *malware* called "Wiper", which disrupted the communication networks of the Iranian oil ministry in April 2012, read data from those networks, and ultimately also completely deleted hard disks of infected systems. To contain Wiper and as a security measure, the computer systems of the oil ministry and various oil depots were taken off the Internet.

These attacks show once again that espionage attacks are not a sporadic affair, but rather that there is permanent interest in access to systems, data and information, and that the pressure on sensitive data and systems is increasing every day. It is possible for espionage infrastructure to remain undiscovered for years. It must be assumed that other espionage software has already been placed and is either being used in parallel or is being maintained as a replacement should the attack be discovered, in order to continue to tap and sabotage infiltrated systems and networks. See also Chapter 5.2.

### 4.2 Hacktivism in the Middle East

In January, anti- and pro-Israeli hackers engaged in low-level skirmishes. A self-declared Saudi hacker calling himself "0xOmar" published the credit card information of thousands of Israelis, which he had stolen in attacks on the databases of Internet service providers. As a response to this operation, an Israeli hacker named "0xOmer" published data on Saudi citizens. The day after a call by a Hamas speaker to protest against the occupation of

---

<sup>16</sup> See: MELANI Semi-annual report 2010/2, Chapter 4.1:  
<http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=en> und  
MELANI Semi-annual report 2011/2, Chapter 4.2:  
<http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en> (as of 31 August 2012)

## Information Assurance – Situation in Switzerland and internationally

Palestine by attacking Israeli websites, the websites of the Israeli airline El Al and the Israeli stock exchange were disrupted, which was in turn avenged by “hacktivist” attacks against the websites of the stock exchanges of the United Arab Emirates and Saudi Arabia. This again motivated a TV preacher in Kuwait to call for cyber jihad against Israel via Twitter. Several days later, a pro-Israeli hacker published the Facebook access data of several thousand Arabs, which forced Facebook to reset the passwords of the affected accounts. After several further hacks and publications of stolen data as well as denial-of-service attacks on websites, the open hostilities subsided again by mid-February.

These incidents are an example of how political conflicts can be incited also by non-state players or in fact anyone. If a political statement is attached to the publication of data obtained by hacking, this provokes reactions from the camp of political opponents. In this way, hackers can stir each other up. While in this case one of the sides was clearly designated, the other side's selection of targets initially relied on the unconfirmed self-declaration of the first attackers. Over the course of the skirmishes, however, doubts arose concerning the origins of the initiator "0xOmar", so that other Arab states and Iran became targets of pro-Israeli hackers as well. As in the case of state attacks, the problem of attribution arises in the context of hacktivism of this kind. As long as an attacker has not been identified unambiguously, there is a risk of retaliating against the wrong target, drawing a large number of uninvolved persons into the fray.

### 4.3 Anonymous announced attack against the Internet – no measurable impact

On 12 February 2012, Anonymous announced that it would cripple the Internet on 31 March with an attack against the 13 *DNS root servers* to protest against the planned US Stop Online Piracy Act (SOPA), Wall Street, irresponsible politicians, bankers and social evils in general. While the announcement was met with great interest by the media, the attack – as expected – had no measurable impact.

The Domain Name System (DNS) makes it easier to use the Internet and its services by allowing web addresses (*URLs*) to be entered instead of *IP addresses*. Without *DNS servers*, the Internet still works, but *IP numbers* would have to be entered instead of *URLs*. Uppermost in the hierarchy are the *root servers*, which serve as the highest authority for information concerning *top-level domains* (e.g. .com, .net, .ch).

Since the *DNS root servers* are essential for the smooth functioning of the Internet, various security measures have been implemented. For instance, the 13 *DNS root servers* are not simply 13 individual servers. In total, 259 servers are operated by various providers in different countries.

The "*DNS amplification attack*" method described by Anonymous in this case exploits the fact that name servers respond to small query packets with very large packets in certain situations. Theoretically, a 60-byte-long query might provoke a response of more than 3,000 bytes. In the attack, these large responses are directed to the *DNS root servers* in order to overload and cripple them. However, these servers have enormous capacities for dealing with peak loads. This ensures that the *DNS* would still work even if two thirds of the root servers were to be disabled. Additionally, an outage of the *DNS root servers* would only have an impact if it were sustained for a long time, since many providers store *DNS* queries locally in order to reduce network traffic. The *DNS root servers* are also monitored continuously. If an anomaly is detected, the malicious traffic to the *DNS root servers* would immediately be blocked. The last major attack took place in 2007 against 2 of the 13 *DNS root servers*. Since the others functioned smoothly, there were no noticeable consequences in that case either.

An attack against the Internet does not fit the modus operandi of Anonymous, which has for instance repeatedly declared that it will not attack media. An attack affecting all Internet users would probably be counterproductive for Anonymous, causing it to lose sympathisers. To carry out such an attack, prior tests of the purported tool would also be necessary, as well as a large number of volunteers. As already was the case in the announced attack against Facebook in November 2011, various Anonymous activists dissociated themselves from the call.

The loose affiliation with Anonymous results in a series of uncoordinated, more or less spectacular announcements and attacks. Since, given its structure, Anonymous has no membership as such and there are no official speakers or other persons responsible for the whole movement, in principle anyone can publish messages in the name of Anonymous and generate media interest.

### *Anonymous taps conference call of Scotland Yard and FBI*

Activists affiliated with Anonymous were able to tap a confidential conference call of the London police Scotland Yard and the US federal police FBI. Anonymous apparently managed to intercept an e-mail containing the access data for the conference call. The activists published the content of the conference call on YouTube and elsewhere. Apart from many incidental topics, the conference call also discussed details concerning ongoing investigations of Anonymous and LulzSec, such as the dates of planned arrests. In addition to the conference call audio file, Anonymous also published the e-mail containing the access data for the call. Criminal proceedings have been initiated.<sup>17</sup>

## 4.4 Protests against ACTA – also on the Internet

At the beginning of 2012, there were vehement protests in several countries against the planned ratification of the ACTA treaty. The Anti-Counterfeiting Trade Agreement (ACTA) is a planned multilateral trade agreement under international law. The participating countries want to use ACTA to establish international standards against product piracy and copyright violations.

These protests, with the goal of scuttling the ACTA treaty, took place mainly in the form of traditional demonstrations, which reached their climax on the pan-European day of action on 11 February 2012. But protest actions were also observed on the Internet, some of which are mentioned here (without a claim to completeness):

### *Czech Republic*

In the Czech Republic, 27,000 datasets regarding members of the governing party ODS were stolen and published. In addition to private addresses, the datasets contained the telephone numbers of the party members. On 6 February 2012, ratification of ACTA in the Czech Republic was suspended until further notice.

### *Poland*

Several websites of the Polish government were temporarily disabled by *DDoS* attacks. The Polish branch of Anonymous and the hacker group "Polish Underground" are said to be behind these attacks. Some of the activists also unmasked the website of the municipality of

---

<sup>17</sup> <http://www.spiegel.de/netzwelt/web/anonymous-attacke-hacker-veroeffentlichen-fbi-gespraech-mit-scotland-yard-a-813224.html> (as of 31 August 2012).



## Information Assurance – Situation in Switzerland and internationally

Kraszewnik<sup>18</sup> and left a message behind. Also in Poland, the government has decided to suspend ratification of ACTA.

### *United States*

As part of the protest actions against ACTA, Anonymous apparently also hacked several websites of the US Federal Trade Commission, FTC. Seven sites were apparently affected by the attack – but not the main site.

### *Greece*

Hackers of the Anonymous movement attacked the website of the Greek Ministry of Justice on Friday, 3 February 2012, in protest against austerity measures, but also against Greece's participation in the ACTA treaty. For four hours, texts to this effect were displayed on the ministry's website. The hackers gave the government two weeks to abandon the ACTA treaty; otherwise new attacks would be launched.

### *Slovenia*

The Slovenian branch of the Anonymous hacker group temporarily disabled several websites as part of the protest actions against ACTA, including the site of the leading government party SDS and of other parties. Ratification was suspended on 7 February 2012.

The protests were less pronounced in Switzerland. In part, this is likely also due to the fact that Switzerland offers its citizens the tools of referendum and initiative to influence policymaking. Although there were minor demonstrations in Zurich, no major demonstrations or even attacks on the Internet as seen in other European countries were observed. Although Switzerland participated in the preparation and negotiation of ACTA, the Federal Council announced on 9 May 2012 that it would not sign the treaty for now.

The protests against the ACTA treaty are a further example of how protests continue to move into virtual space. But they also show the great sensitivity of citizens to Internet issues. Any restriction and regulation is met with considerable scepticism, since the Internet is still associated with a free and sometimes lawless zone.

## 4.5 Large volumes of passwords and credit card data stolen

The first half of 2012 was again characterised by major attacks on well-known companies, in which client data – usually usernames and passwords but also credit card data – was stolen.

For instance, it became known in the week of 4 June 2012 that more than 6 million *SHA-1 hash* values of passwords of the online professional network LinkedIn were published in Internet forums. *SHA-1* is a globally widespread cryptographic hash function that generates a 160-bit hash value (checksum) from any given message. Often, the password can be reconstructed from this hash value. Many passwords have already been published in plain text. Although the published documents do not include the associated e-mail addresses (which serve as a username), it must be assumed that this data has also been stolen and is being held by the attacker.

---

<sup>18</sup> <http://www.kraszewnik.pl/> (as of 31 August 2012).

Just a few hours after the incident became known, phishing websites already surfaced asking users to "verify" their LinkedIn passwords.

### *Database breach of Amazon subsidiary Zappos*

Unknown hackers gained access to the data of 24 million registered US customers of the Amazon subsidiary Zappos and also stole the password hashes of the customers. Fortunately, only the last four digits of customer credit cards were saved in the attacked database. According to information provided by the company, the perpetrators were unable to access the servers containing additional payment data and complete credit card numbers.<sup>19</sup>

### *Attack against credit card data of Global Payments*

The credit card processing service Global Payments was not as fortunate. More than 1.5 million datasets of credit card numbers are said to have been stolen. Apparently, the data theft was in the context of a hacker attack against a New York taxi company.<sup>20</sup> The attackers were able to gain access to the administrator account of that company and read credit card data for several months. This data was not used immediately, however, but rather the scammers collected it to use at a later time. In this way, they prevented detection of the theft and any countermeasures that might have diminished their gains.

### *450,000 usernames and passwords stolen from the Yahoo! Contributor Network content platform*

Yahoo became the victim of a hacker attack in the first half of 2012. Nearly 450,000 usernames and passwords of the Yahoo! Contributor Network content platform<sup>21</sup> were stolen and published on the Internet by the hacker group D33Ds Company. According to Yahoo, a vulnerability in the company's computer system was exploited; Yahoo says the vulnerability was fixed immediately. According to the hacker group D33Ds Company, the database was neither well-secured nor were the saved passwords encrypted. The attack was intended as a wake-up call for the database administrators responsible.

### *50,000 Twitter usernames and passwords surface*

On 9 May 2012, more than 50,000 usernames and passwords of Twitter accounts likewise surfaced. Twitter subsequently promised to reset the passwords of the affected accounts. It is still unclear where the data came from and who published it. Apparently the quality of the data was not very high, since it contained double entries, accounts that had already been blocked, and fake accounts.<sup>22</sup>

### *GMX accounts hacked*

The e-mail provider GMX reported that GMX accounts had been broken into in at least 3,000 cases. Originally it was assumed that the attacks were *brute force* attacks. This approach is not very useful for online services, however, since an attack of that magnitude would be noticed very quickly. Much more probable is that the attackers were in possession of usernames and passwords. GMX confirmed that usernames and passwords were entered in a very targeted way. It is not known how the passwords were stolen. The passwords may, however, have been stolen in a different context – i.e. from other service providers – and

---

<sup>19</sup> <http://online.wsj.com/article/BT-CO-20120116-706917.html> (as of 31 August 2012).

<sup>20</sup> <http://blogs.gartner.com/avivah-litan/2012/03/30/new-credit-card-data-breach-revealed/> (as of 31 August 2012).

<sup>21</sup> [http://www.focus.de/digital/internet/datenbank-muehelos-geknackt-hacker-veroeffentlichen-zugangsdaten-von-450-000-yahoo-nutzern\\_aid\\_781269.html](http://www.focus.de/digital/internet/datenbank-muehelos-geknackt-hacker-veroeffentlichen-zugangsdaten-von-450-000-yahoo-nutzern_aid_781269.html) (as of 31 August 2012).

<sup>22</sup> <http://www.spiegel.de/netzwelt/web/twitter-passwoerter-im-netz-a-832171.html> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

then "tried out" with the GMX accounts.<sup>23</sup> Since many people still use the same password for all services on the Internet, this suspicion is not unfounded.

According to Firehost, attacks against websites using *SQL injections* rose by 69% between April and June 2012.<sup>24</sup> An *SQL injection* tries to send manipulated commands to a database. Generally, this approach exploits vulnerabilities or poorly programmed interfaces which verify the sent commands inadequately or not at all. This makes it possible to spy out client data, manipulate online shops, or simply destroy entire databases. A successful attack, the loss of client data, and the associated loss of reputation can quickly cost a lot of money and even ruin a company. As always, it helps to keep the website software updated and to protect it from external attacks.

It has become indispensable to use different passwords for different online services. This improves security enormously, even if these passwords must be recorded somewhere (on paper) for the user to remember them.

## 4.6 Update on SCADA

In January 2012, a group of security service providers published vulnerabilities in components of industrial control systems. This caused unease among both manufacturers and operators: The discoverers of the vulnerabilities had not informed the manufacturers in advance so that the gaps could have been closed prior to publication. They were communicated directly to the public. This approach was criticised by numerous sides.

On the one hand, the discoverers wanted to show the operators of critical infrastructures how easily SCADA systems can be compromised. On the other hand, the action was apparently intended as a lesson for the manufacturers. Apparently the group had already learned how manufacturers knew about certain vulnerabilities for years, but instead of fixing them quickly, delayed publication and updates for as long as they could.<sup>25</sup> To be fair, it must be noted that updating SCADA systems is not comparable to updating personal computers. Updates to control systems always give rise to the risk of malfunctions, which may have serious consequences.

The difference from ordinary computer systems is firstly that manufacturers so far have little experience fixing vulnerabilities, and secondly that operators rarely update their software components. This is because in the case of continuously running processes, updates are possible only during certain maintenance windows. Moreover, the impact of *patches* on the overall process can often be tested in advance only to a very limited extent. The principle of "don't touch a running system" applies to the extent that disruptions and outages can very quickly incur high costs.

Originally SCADA systems had only a few similarities with traditional ICT: they were isolated from the computer networks, employed proprietary hardware and software, and used their own protocols for communicating with the central computer. This has changed fundamentally in recent years, since comparatively inexpensive devices with integrated interfaces to

---

<sup>23</sup> <http://www.zeit.de/digital/datenschutz/2012-07/gmx-passwort-account> (as of 31 August 2012).

<sup>24</sup> <http://www.heise.de/newsticker/meldung/Deutlicher-Anstieg-der-SQL-Injection-Angriffe-1651041.html> (as of 31 August 2012).

<sup>25</sup> <http://www.heise.de/security/meldung/Sicherheitsexperten-setzen-Hersteller-von-Industriesteuerungen-unter-Druck-1418292.html> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

Internet protocol have been available. While these components usually do not (yet) have a connection to the Internet, it is still possible for *malware* to enter the separated systems via infected laptops or *USB sticks*. Since *SCADA* components are not designed to support security elements such as *firewalls* and *antivirus software*, attackers encounter sufficiently low barriers once they are in the network.

### *Possible attack against US track system*

According to a report by the US Transportation Security Administration (TSA), a track system in the north-west of the United States was disrupted on 1 December 2011, apparently triggered by two unknown accesses from non-US IP addresses. This resulted in delays of 15 minutes. One day later, a second access is reported to have occurred, but caused no disruption. It was not disclosed who or what was behind these attacks. The Department of Homeland Security stated, however, that a targeted attack could be ruled out. The data of the three IP addresses involved was made available to other transport companies in the US and Canada.<sup>26</sup>

### *Implants with weaknesses*

The following example shows that serious consequences can be expected not only in the case of successful attacks against large systems, but that attacks against small systems may even have life-threatening consequences: in a recent study, security experts examined the risks of medical implants. Not surprisingly, pacemakers for instance were shown to have a significant security risk. Everyone is familiar with the warnings for people with pacemakers regarding devices with strong electromagnetic radiation. In one test, the researchers irradiated a defibrillator implant with radio waves, with the result that the implant was shut down. Other frightening weaknesses were also found, however. For instance, *WiFi* links used for the update function contain weaknesses that can be exploited. In the worst case, this leads to deactivation of the device (such as in the case of insulin pumps), with all the resulting health consequences.<sup>27</sup>

## 4.7 Establishment of a European Cybercrime Centre

On 28 March 2012, the European Commission recommended the establishment of a new European Cybercrime Centre hosted by Europol, the European police office headquartered in The Hague. Europol already coordinates the work of national police authorities throughout Europe in the field of cross-border organised crime, and it promotes information exchange among the national police authorities.

The centre is to focus on combating cybercrime in Europe and is scheduled to begin operations on 1 January 2013. The centre is to compile information and experiences, support criminal investigations, and promote solutions and cybercrime awareness throughout the EU.

---

26

<http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/> (as of 31 August 2012).

27

<http://www.pcwelt.de/news/Sicherheitsrisiko-Medizinische-Implantate-als-Zielscheibe-fuer-Hacker-5708296.html> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

Additionally, the centre will build up a community of experts from all branches of society for the purposes of combating cybercrime and child pornography more efficiently.<sup>28</sup>

With the steady increase in communication via Internet and the rising commercial uses of the Internet, fraud and other offences on the Internet have also risen. Investigations regularly involve hundreds of victims in different parts of the world. The traces left by the perpetrators usually lead to several countries and accordingly different jurisdictions. Investigations of this scope and complexity can no longer be solved exclusively by individual national police forces, and traditional, time-consuming mutual legal assistance quickly reaches its limits of efficiency. No criminal offences are as international as cybercrime. Effectively combating Internet crime requires a jointly coordinated and cross-border approach. This is precisely the starting point of the European Cybercrime Centre, which aims to provide additional support.

### 4.8 Deactivation of a Zeus botnet

Together with financial service providers, the Information Sharing and Analysis Center (FS-ISAC), the Electronic Payments Association (NACHA) and the IT security specialist Kyrus, Microsoft went to New York district court and obtained a search warrant executed by US Marshals on 23 March 2012 in two office buildings in the states of Pennsylvania and Illinois. Several web servers were seized. They were suspected of being used in connection with a Zeus botnet. To make the search possible in the first place, Microsoft took unprecedented legal steps: in cooperation with organisations from the financial sector, a civil lawsuit was initiated against the operators of the Zeus botnet instead of a criminal prosecution. The first suits were filed against unknown persons. Then in July, Microsoft published two names associated with the Zeus botnet. Yevhen K. and Yuriy K. have already been arrested in the UK.<sup>29</sup>

The focus of this approach was not to destroy the botnet. A botnet of Zeus's complexity cannot simply be shut down. Rather, the goal was to burden the operators of these networks with work and costs – in the hope that its operation would no longer be considered profitable.

However, the search did not meet with an exclusively positive response. For example FoxIT, a security service provider from the Netherlands, have made some critical remarks about this Microsoft operation.<sup>30</sup>

### 4.9 Drive-by downloads spread using web banners

In mid-May 2012, *malware* was spread using a vulnerability in the *OpenX* web banner software on the website [www.wetter.com](http://www.wetter.com). It is not known how long this infection was active on the site of [wetter.com](http://www.wetter.com). Visitors to the site may have been infected with *malware* without their knowledge. CERT.at knows that different variants of *malware* were spread that way,

---

<sup>28</sup> <https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417> (as of 31 August 2012).

<sup>29</sup> <http://www.golem.de/news/botnet-microsoft-nennt-zwei-mutmassliche-betreiber-von-zeus-1207-92930.html> (as of 31 August 2012).

<sup>30</sup> <http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/> (as of 31 August 2012).



one of which was a *ransom trojan (ransomware)*.<sup>31</sup> On *ransom trojans*, see also Chapter 3.5 and MELANI Semi-annual report 2011/2, Chapter 3.5<sup>32</sup>.

Website infections are currently the most popular vector for spreading *malware*. Central servers that make content available to different websites play a key role in this regard. Especially in the case of online advertisements, but also statistics services, a single act of compromise may have far-reaching consequences.

How software is handled plays an important role for suppliers of Internet ads, but also other content. Here again, all programs must always be kept updated. In the end, it is especially true in the case of such services that a website can only be as secure as its weakest link. And the weakest link is often software included in the website that is offered by third parties and hence beyond the website operator's control.

## 5 Trends / Outlook

### 5.1 Conflation of business and private ICT – a security risk?

While a strict distinction used to be made between private and professional life, this boundary has become fluid: on the one side, companies expect employees to be available also outside office hours or to work evenings (from home) when there is deadline pressure, and on the other side employees use ICT in the office also for private purposes. For instance, they access private e-mails or engage in social networking. In addition, the call for the most modern devices is omnipresent also in the workplace. Why should employees make do with a company cell phone without additional functions if they use the most recent *smartphone* in their private lives? If a company does not react, employees will sooner or later use their private *smartphones* also for company tasks or otherwise develop ways to harmonise their workflow with their needs and desires. That this means an additional challenge for ICT officers at companies is obvious. Where computers are used no longer only in the (controlled) company network, but also outside the workplace, this gives rise to new risks.

Further risks arise when data is exchanged between private and company computers, for instance using a *USB stick* or CD. Experience shows that *USB sticks* are very often used by attackers as a transmission path for targeted attacks to enter the company network. The attacker infects the (poorly protected) private computer of an employee and then uses an external storage medium to sneak into the company computer without being detected. What aggravates the situation is that investigations are much more difficult when a private computer is involved, since there is generally no standardised logging of computer and network activities. While in the case of targeted *malware* attacks using company e-mail, for instance, the possibility exists of verifying after the fact whether an e-mail has arrived and been opened, this possibility usually does not exist in the case of private networks.

---

<sup>31</sup> <http://www.cert.at/warnings/all/20120516.html> (as of 31 August 2012).

<sup>32</sup> See: MELANI Semi-annual report 2011/2, Chapter 3.5:  
<http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

This development illustrates the importance of an integrated approach to security. Not only the classic ICT security questions arise, but rather also organisational questions: Who has access to what data? Do employees know which data may be removed from the company network? What devices may be brought into the company and connected there? In security zones, does it suffice to block USB ports, or do cell phone cameras also have to be banned? The general question arises whether company devices should in fact be distributed relatively broadly and also made available for private use. While all this may lead to greater administrative effort for a company, at least it ensures control of the devices and the applications running on them, since they still belong to the employer and are subject to its control.

While technical security mechanisms are indispensable, they cannot offer 100% protection. Simply protecting computers and networks on which information is stored is not enough; the focus should be on protecting the information itself. This entails better information and data management, information classification, and so on. It also requires a clear assessment of the risks, entailing that the security of distribution channels, access privileges, and storage locations are adjusted to the actual value of the information. Not every channel or storage location is equally secure, and not all documents in a company are equally sensitive. In many cases, ICT is understood in principle as a cost factor, and accordingly regarded by management purely as a logistics and support function. ICT – as part of the information assurance process – must however necessarily be integrated into the corporate and strategic risk management process, in light of its critical factors. Information assurance is thus a further integrated component of the strategic risk management and security concept, at the same strategic level as the protection of buildings and persons, financial controlling, and so on.

## 5.2 Cyber conflict in the Middle East

With the beginning of the Arab Spring and the fall of the first governments, documents and other proof were made public showing that some Arab states had used high-quality technologies from the West to engage in Internet surveillance of their regime critics. Even those states in which only few or no riots broke out are said to employ programs and infrastructures to monitor communications as widely as possible. Business for such ICT solutions is booming, and as already reported in the Semi-annual report 2011/2<sup>33</sup>, this is a complex issue that does not permit an overly simplified black-and-white perspective. But various incidents in different centres of crisis and conflict in the Middle East show that there is a much broader range of ICT players and resources going far beyond communication surveillance.

For instance, the Stuxnet *malware* and its auxiliary modules impressively demonstrated the effectiveness of ICT-based means if they are developed with sufficient resources and covered by the state for use in sabotage and espionage. As described in Chapter 4.2, even non-state players participate virtually in conflicts in the Middle East. It is difficult to assess who exactly is behind the protest movements in question, to what extent they enjoy more than simply ideological support from the state, and how they incite each other to action. They make use of the entire spectrum of data theft, denial-of-service attacks, and the very popular virtual defacements. But also on the organisational and propagandistic side, the advantages of the Internet are utilised. For instance, activists of all backgrounds organise themselves via Facebook, Twitter and suchlike, or they upload cell phone videos and photos to the Internet

---

<sup>33</sup> See: MELANI Semi-annual report 2011/2, Chapter 5.3:  
<http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

in order to support their statements and demands; in such cases, the real context can hardly be reconstructed in a comprehensive or meaningful way.

It is thus no surprise that many different ways are tried to infiltrate not only the e-mail accounts of opponents, but also social network groups, in order to obtain information on planned activities and the identities of the persons involved as well as other useful data. Already before the Arab Spring, for instance, actions became known in which regime critics living abroad were inundated with targeted ICT attacks. But also the members of authoritarian regimes and their relatives may be harassed by activists or foreign intelligence services, as the example of the publication of Bashar al-Assad's iTunes purchases shows.<sup>34</sup>

The growing demand for (centralised) surveillance technologies, ICT sabotage, the use of propaganda image materials, and the discrediting of individuals on the basis of stolen personal e-mails are a result of the use of all available ICT resources and methods by one party or the other in a region marked by many years of tension and instability.

Not only since the Arab Spring has the Middle East been marked by unrest, crises and all kinds of conflict potential. With the outbreak of demonstrations and riots, some of these underlying conflicts entered a new stage, or old difficulties that previously had been suppressed have now surfaced in public. Not only since these incidents and eruptions has ICT been employed in the Middle East, whether in the fields of communication, (centralised) surveillance of such communication, SCADA systems, or support of production and business processes. With the open conflicts erupting since the beginning of the Arab Spring, the aggressive and offensive use of ICT resources and the Internet has increased.

Cases regularly come to light in which websites are brought down, documents of the state or of individuals are stolen and published, or malware is used for purposes of sabotage. All of this is in addition to the flooding of various Web 2.0 services with messages, videos, and fragments of information on the apparent situation on the ground – though both sides to a conflict use these techniques and it is often impossible to verify or reconstruct what really happened. What aggravates all of this is that ICT-based resources are often relatively cheap, have a long-range effect, and thus are attractive for everyone involved.

In this sense, the cyber conflict carried out on several levels in the Middle East is primarily a concomitant of the real conflicts and realities on the ground. Accordingly, incidents in this connection should not be seen as isolated events, as they are often portrayed in the media, but rather should be understood as embedded within an overall context permitting a comprehensive assessment of what has occurred and what is presented and reported.

### 5.3 Data theft: attacks against many small and a few large companies

Again and again, attacks against client data of major companies, and especially credit card data, make the headlines. In addition to recent incidents described in Chapter 4.5 one might recall the numerous attacks in the past: for instance the loss of client data by Sony last year; the incident involving the Anglo-American department store chain TJX in 2005, in which systematically more than 45 million credit card datasets were stolen over the course of 1½ years; or the incident involving the credit card processing service Heartland in 2009.

---

<sup>34</sup> <http://www.guardian.co.uk/world/2012/mar/14/assad-itunes-emails-chris-brown> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

A study by the American security firm Verizon<sup>35</sup> using data of the US Secret Service and the Australian, Dutch and Irish police from the year 2011 showed, however, that attacks against major companies make up only a small share. Of the 855 reported incidents with a total of 174 million compromised datasets, only the smallest part of the incidents concerned large companies. While admittedly some of these cases were very spectacular, they contrast with numerous attacks on small companies and their data, which occur every day under the radar of the media. In more than 75% of the cases, the attacks are against SMEs with fewer than 1,000 employees.

While large companies prepare well for cyber risks and in most cases have an ICT security team and a CSO, this awareness is still lacking among many smaller companies. Many companies still handle client and credit card data with a considerable lack of sensitivity. What good do secure orders using https do, if the data are then saved without encryption on the computer?

Some criminals ruthlessly exploit this by looking for the path of least resistance and identifying the "easiest" targets. Often, automated attack methods are employed, which search systematically for known weaknesses and misconfigurations on websites or in databases in order to steal the data. Instead of attacking a large company, it may indeed be more profitable for criminals to attack many different small companies with less effort but also lower gains, i.e. fewer datasets.

Large companies should not think themselves safe, however. For some criminals with greater technical know-how and good skills, greater effort may pay off over time. In the field of espionage, the term *advanced persistent threat* (APT) has become popular in this regard and is used primarily for state players without a direct financial benefit. But if the gains make sense in the end, then a targeted, highly professional attack prepared over the course of months may be worthwhile for criminals. Unlike state espionage, however, the financial motive predominates here.

## 5.4 Client communication in the age of phishing

"No serious company will ever ask you for your username and password by e-mail." This is the standard answer given by MELANI when people report an e-mail and are unsure if it is actually from the company it claims to be from. This statement, which initially sounds simple, sometimes poses certain challenges to companies in the age of electronic client communication, however. How should a company communicate with clients so that they do not think it is a fraudulent e-mail? And even more importantly: careless client communication by a company may also have a negative impact on client behaviour regarding fraudulent e-mails.

### *eBay client verification*

The following example illustrates the dilemma many companies face:

eBay sporadically sends e-mails to verify membership if a user has not logged into an account for a long time. This is clearly a necessary procedure, since otherwise many unused accounts would accumulate on eBay over the years.

Although the message does not directly ask the user to enter username and password, the e-mail does immediately give rise to scepticism among many recipients who are aware of the

---

<sup>35</sup> <http://securityblog.verizonbusiness.com/category/ask-the-data/> (as of 31 August 2012).

## Information Assurance – Situation in Switzerland and internationally

phishing problem, especially if – as in the following case – the client account was recently used for an auction.

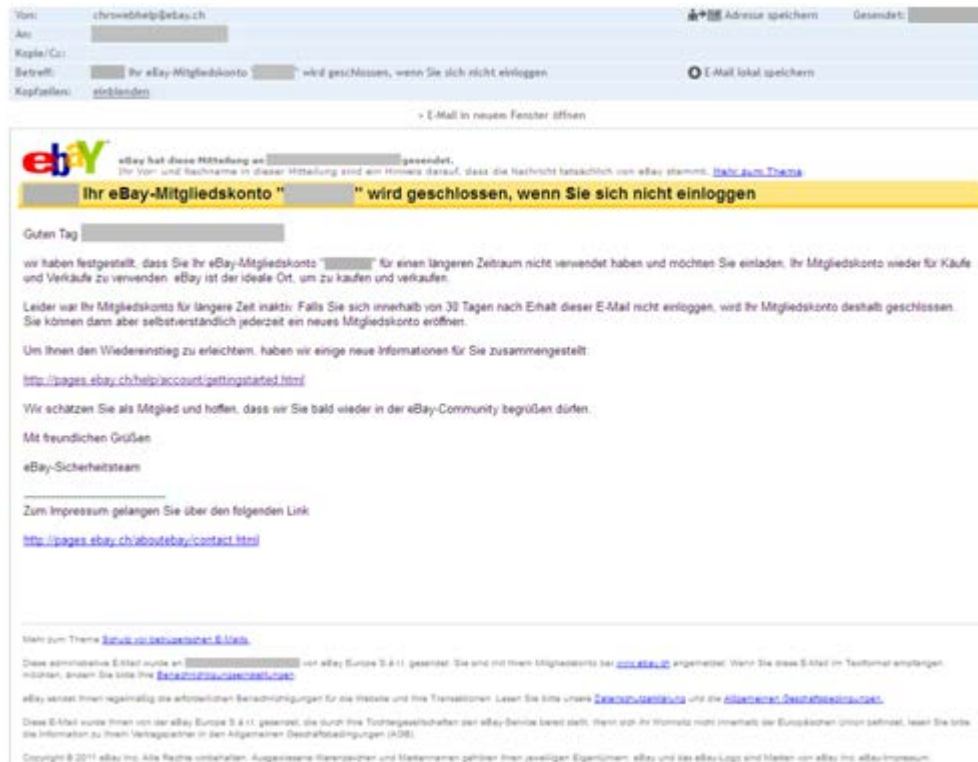


Image 8: E-mail from eBay to verify clients

### *Change of PayPal's terms and conditions*

Another case resulting in reports to MELANI was a change in terms and conditions sent out by PayPal at the end of June by e-mail. Although the e-mail did not contain a link to the login page, the fact that users did not expect to receive an e-mail from PayPal gave rise to uncertainty.

### *Newsletter from Switzerland Tourism*

An e-mail from Switzerland Tourism sent on 31 May 2012 also resulted in enquiries to MELANI. The links contained in the e-mail did not refer to domains of Switzerland Tourism, but rather to a different Swiss server named "crm.stnet.ch". The links were very complicated and long, which caused recipients to have MELANI verify the authenticity of the e-mail.



## Information Assurance – Situation in Switzerland and internationally

Betreff: Mit allen Wassern gewaschen

Falls der Newsletter nicht korrekt dargestellt wird, klicken Sie hier [http://crm.stnet.ch/crm/service/nlweb?bpid=\[REDACTED\]&language=de&chk=iSXR06ASZf](http://crm.stnet.ch/crm/service/nlweb?bpid=[REDACTED]&language=de&chk=iSXR06ASZf) .

[http://crm.stnet.ch/content/campaign\\_data/content/804302666/Headerde.jpg](http://crm.stnet.ch/content/campaign_data/content/804302666/Headerde.jpg)  
[http://crm.stnet.ch/content/campaign\\_data/content/980099386/Mainimage.jpg](http://crm.stnet.ch/content/campaign_data/content/980099386/Mainimage.jpg)  
[http://crm.stnet.ch/content/campaign\\_data/content/804302666/juerg-foto-Sommer.jpg](http://crm.stnet.ch/content/campaign_data/content/804302666/juerg-foto-Sommer.jpg)

Grüezi [REDACTED]

Freuen Sie sich auf Ferien, die prickeln. Unser Reiseland steht diesen Sommer ganz im Zeichen des Wassers. Sprühen Sie sich mit [http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Fempfehlungen%2Fstaadtereisen%2F470108%2F1&chk=3f7xlXXD1W&ganame=Newsletter+05%2F2012\\_CHdefr](http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Fempfehlungen%2Fstaadtereisen%2F470108%2F1&chk=3f7xlXXD1W&ganame=Newsletter+05%2F2012_CHdefr) oder geheimnisvoll mit [http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Ferlebnisse%2Fwandern.html%3F3D255278&chk=6VAZ5FLJaD&ganame=Newsletter+05%2F2012\\_CHdefr](http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Ferlebnisse%2Fwandern.html%3F3D255278&chk=6VAZ5FLJaD&ganame=Newsletter+05%2F2012_CHdefr) in einer atemberaubenden Tour. Haben Sie das Beste herausgepickt.

Finden Sie uns im Netz

[http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.facebook.com%2FMySwitzerland&bpid=\[REDACTED\]](http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.facebook.com%2FMySwitzerland&bpid=[REDACTED])  
[http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Ftwitter&lid=4&chk=D6xD9RVRAR&ganame=Newsletter+05%2F2012\\_CHdefr](http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Ftwitter&lid=4&chk=D6xD9RVRAR&ganame=Newsletter+05%2F2012_CHdefr) <http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.youtube.com%2Fmyswitzerland&lid=5&chk=2DeDD32Te2> [http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.flickr.com%2Fphotos%2Fswitzerland\\_tourism%2F&lid=6&chk=XXWjH0FADF](http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.flickr.com%2Fphotos%2Fswitzerland_tourism%2F&lid=6&chk=XXWjH0FADF)  
Viel Genussreiches wartet auf Sie. Lassen Sie sich erfrischen von unseren Ideen rund ums Element Wasser!

[http://crm.stnet.ch/content/campaign\\_data/content/804302666/juerg.gif](http://crm.stnet.ch/content/campaign_data/content/804302666/juerg.gif)

Jürg Schmid, Direktor Schweiz Tourismus

Image 9: E-mail from Switzerland Tourism with links to the domain stnet.ch

### *Re-registration for MELANI newsletter*

Even MELANI is not immune to problems of this sort. Since the MELANI newsletter was migrated to the information portal of the federal government in June 2012 and it was not possible for technical reasons to transfer the database containing the registered e-mail addresses, all MELANI newsletter subscribers were informed that they would have to re-register in order to continue receiving the newsletter.

Such a venture is difficult and has to be planned carefully. MELANI tried to solve this problem by announcing the procedure in an advance e-mail and by defining the precise time the e-mail would be sent out. The e-mail was sent using pure text format and contained only a single link which, like earlier newsletters, led to the MELANI domain. New subscribers were at no time asked to enter their password (but rather to choose a new one). The home page of the MELANI website also clearly referred to the e-mail distribution. Despite this approach, reactions were forthcoming – though the number was limited. Responding quickly to questions from clients during and after newsletter distribution is also a useful way to keep uncertainty to a minimum. Nevertheless, there was potential for improvement also in this case, for instance by using a link in the e-mail to an encrypted page (https).

The following points should be observed when sending out newsletters:

- Send e-mail in text format where possible.
- Send newsletter e-mails as regularly as possible.
- Limit the use of links in the e-mail and link only to the company's own domain. If possible, use links to encrypted pages (https) and communicate this to the recipient.
- Do not link to websites asking the user to enter username and password or other data.
- Mention the newsletter on the home page of the company website or link the information directly, so the recipient has the option of entering the main address manually and clicking on the newsletter there.
- Address clients by first and last name where available.



## 5.5 E-voting in Switzerland – experiences so far

In the year 2000, the project Vote électronique for casting votes electronically was launched in Switzerland. The first pilot trial took place in 2003 in a small commune in the Canton of Geneva, where a manageable number of voters had the option of casting their votes electronically at the communal level. This first pilot trial met with a huge response internationally and was also mentioned in renowned newspapers in Switzerland and abroad.

Since this first trial, the Federal Council has approved more than 100 trials in federal popular votes. The 115th trial of electronic voting is scheduled for the federal popular vote on 25 November 2012. If the numerous additional trials at the communal and cantonal level as well as several tests during elections are included, the total number is much higher.

Despite this large number of trials, there has been only minor incidents with very small impacts (see example in Chapter 3.7). But is Swiss e-voting really that secure? The following brief analysis will investigate this question.

Currently only a limited number of eligible Swiss voters may use electronic voting. While access has meanwhile been extended to Swiss living abroad, for various reasons it is still unlikely that an erroneous trial with Vote électronique would affect the final result:

- The size of the electorate is chosen so that even if results are close, it can be assumed with high probability that a partial or total failure of the electronic system would have no impact on the final result. So far, mainly Swiss nationals living abroad make use of electronic voting.
- The electronic ballot boxes must always be closed at Saturday on the week-end of the physical ballot. This measure gives voters the opportunity to cast their votes physically at a polling station if, for instance, a total failure of the electronic systems occurs (e.g. owing to a nationwide collapse of Internet connections or a successful DDoS attack).

In addition to these organisational measures, numerous technical measures are implemented to guarantee the principles enshrined in the Federal Act on Political Rights and the Ordinance on Political Rights (one person one vote, anonymity of vote, confidentiality of vote).

But what happens if a large share of the population uses this service? Especially if e-voting is used nationwide, above measures will no longer work or only to a limited extent:

- An attack against the electronic ballot box is certainly unlikely: the votes cast are kept encrypted until they are counted. The relatively short period in which electronic voting is possible makes it unlikely that even a massive *brute force* attack would be sufficient to decrypt and falsify the votes in time. Even a successful attack would probably not influence the voting outcome: the existing limits (at most 10% of the federal electorate may vote electronically) are chosen such that the final result would not be affected even if the e-voting system failed completely or the electronic votes were manipulated.
- Nevertheless, it can of course not be ruled out that an attack against one of the *Vote électronique* systems might be possible at some time. Conceivable for instance would be a *DDoS* attack against the electronic systems, preventing Swiss nationals living abroad from casting their vote on time.

**Information Assurance – Situation in Switzerland and internationally**

- But the greatest problem are certainly insecure input devices (client systems) combined with the inability to trace and prove votes. Many attack possibilities (vectors) currently relevant to Internet banking might also target e-voting directly or even in a simplified form. The security measures – transaction authentication and monitoring procedures – used for Internet banking do not work here. Accordingly, the threat situation is high, and the client represents the Achilles heel of e-voting.<sup>36</sup> If it is possible for an attacker to install *malware* on the computer of the voter, he can manipulate the vote anyway he wants. Malicious code smuggled into the browser can for example change a parameter value "Yes" into the parameter value "No" even before it is encrypted and sent to the e-voting server. The malicious code might also manipulate the security image sent back by the e-voting servers after it has been decrypted, so that the voter does not detect the manipulation. Such an attack scenario is especially serious if it occurs nationwide and a large number of votes can be manipulated.<sup>37</sup> Modern e-voting technologies, such as "verifiability", make it possible to detect such attacks in time, however.

"Verifiability" serves to detect manipulations of votes. If, for instance, a virus on a voter's computer changes a vote, then the voter can detect the manipulation using a verifiable system. In a first step, verifiability can for example be implemented by displaying a code for each ballot proposal (or candidate) on the computer screen for the voter after the vote has been sent. The voter then compares this code with personal codes that have been sent as part of the voting materials. Since the codes are different for each ballot proposal (or candidate), the virus does not "know" which code to display in order to trick the voter.

The major difference between e-voting and e-commerce lies in the error tolerance of the systems. While a certain percentage of scams can be tolerated in the case of electronic services and companies also pay for them – after all, companies also save money by offering e-services – in the case of voting the result have to represent the will of the electorate. Anything else would diminish citizens' trust in democracy.

The expansion of the number of electronic voters has to be combined with the introduction of the "verifiability".

## 6 Glossary

Antivirus Software	Virus scanner (anti-virus) software protects your data from viruses, worms or Trojan horses.
Attachment	An attachment is a file sent along with an e-mail.
Backdoor	"Backdoor" refers to a software feature that allows users to circumvent the usual access control of a computer or of a protected function of a computer programme.
Backup	"Backup" means the copying of data with the

<sup>36</sup> <https://www.e-voting-cc.ch/index.php/de/workshops/workshop09/programm09/87> (as of 31 August 2012).

<sup>37</sup> [http://data.rrb.zh.ch/appl/rbzhch.nsf/0/C12574C2002FAA1FC1257942004EB439/\\$file/Evaluation\\_E-Voting\\_Z%C3%BCrich.pdf](http://data.rrb.zh.ch/appl/rbzhch.nsf/0/C12574C2002FAA1FC1257942004EB439/$file/Evaluation_E-Voting_Z%C3%BCrich.pdf) (as of 31 August 2012).

**Information Assurance – Situation in Switzerland and internationally**

	intent of copying them back in the event of data loss.
Bluetooth	A technology for wireless communication between two terminals and which is mainly used in mobile phones, laptops, PDAs and input devices (e.g. computer mouse).
Brute force attack	Attack method in which all potential solutions/passwords are tried out until the right one is found.
DDoS attacks	Distributed denial of service attacks A DoS attack where the victim is simultaneously attacked by many different systems.
Digital certificate	Verifies the affiliation of a public key to a topic (person or computer).
DNS	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).
DNS amplification attack	A denial of service attack (DoS) that exploits publicly accessible DNS servers and uses these as amplifiers.
DNS root server	Root name servers, or simply root servers, are servers for resolving names at the root of the Internet's domain name system. The zone of the root servers covers names and IP addresses of all name servers of all top-level domains.
Domains	The domain name (e.g. www.example.com) can be resolved by the DNS (Domain Name System) into an IP address, which may then be used to establish network connections to that computer.
E-Commerce	E-commerce is the generic term in the Internet economy for electronic commerce.
E-government	E-government means the simplification and execution of processes by using digital information and communication technologies between state, communal and other authorities as well as between institutions and citizens/businesses.
Event-Viewer	Program that displays the error messages and notices of the Windows operating system.
Firewall	A firewall protects computer systems by monitoring incoming and outgoing connections and rejecting them if necessary. A personal

## Information Assurance – Situation in Switzerland and internationally

	firewall (also called a desktop firewall), on the other hand, is designed to protect a stand-alone computer and is installed directly on it.
Geoportal	Web portal that makes geographic information available.
HTML	HyperText Markup Language Pages for the World Wide Web are written in HTML. This allows to determine the properties of the web page (e.g. page representation, links to other sites, etc.). Because HTML is made up of ASCII characters, a HTML page can be edited using a normal word processing programme.
Internet archive engine	Internet service that archives copies of all/many websites on the Internet at certain intervals and makes them available. This means that old sites which otherwise would no longer be reachable can still be seen.
IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
Law enforcement trojan	Software used by the police during criminal investigations, for instance to tap VoIP conversations.
Malicious Code	Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses.
MD5 hash function	Algorithm converting any text into a numeric sequence of always the same length. Hash functions are used in three areas: <ul style="list-style-type: none"> <li>- Cryptography.</li> <li>- Database systems. Database systems use hash functions to search efficiently within large databases.</li> <li>- Checksums. A hash value can be assigned to every file. An altered hash value indicates a manipulation.</li> </ul>
OpenX	OpenX is an open source software providing ad banner management.
Patch	Software which replaces the faulty part of a programme with a fault-free version. Patches are used to eliminate security holes.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their

**Information Assurance – Situation in Switzerland and internationally**

	victim's good faith and helpfulness by sending them e-mails with false sender addresses.
PHP mailer	PHP program sending text using an e-mail function. PHP is a scripting language used mainly to create dynamic websites or web applications.
Ransom trojan	Malware that blocks the computer and demands a ransom from the owner.
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.
Remote Administration Tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
SCADA systems	Supervisory Control And Data Acquisition Systeme. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
SHA	Secure Hash Algorithm. The term "SHA" describes a group of standardised cryptological hash functions that calculate an unambiguous hash value for any kind of electronic data.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
Spoofing	In the IT field, spoofing means various ways to manipulate computer networks in order to conceal one's identity.
SQL-Injection	SQL injection refers to the exploitation of a vulnerability in connection with SQL databases, resulting from insufficient verification of the variables to be transmitted. The attacker attempts to inject his own database commands, in order to change the data as desired or to gain control over the server.
Top-Level-Domains	Every name of a domain on the Internet consists of a sequence of character strings separated by periods. The term "top level domain" refers to the last name in this sequence, constituting the highest level of the name resolution. If the full domain name of a computer or website is

## Information Assurance – Situation in Switzerland and internationally

	de.example.com, for instance, the right-most member of the sequence (com) is the top level domain of this name.
URL	Uniform Resource Locator The web address of a document. It consists of protocol name, server name, path and document name (e.g.: http://www.melani.admin.ch/test.html).
USB Memory Stick	Small high capacity data storage devices, connected to a computer via the USB interface.
Voice phishing	Type of fraud in which the victim is called by telephone and induced to divulge access data.
WLAN	WLAN stands for Wireless Local Area Network.