Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

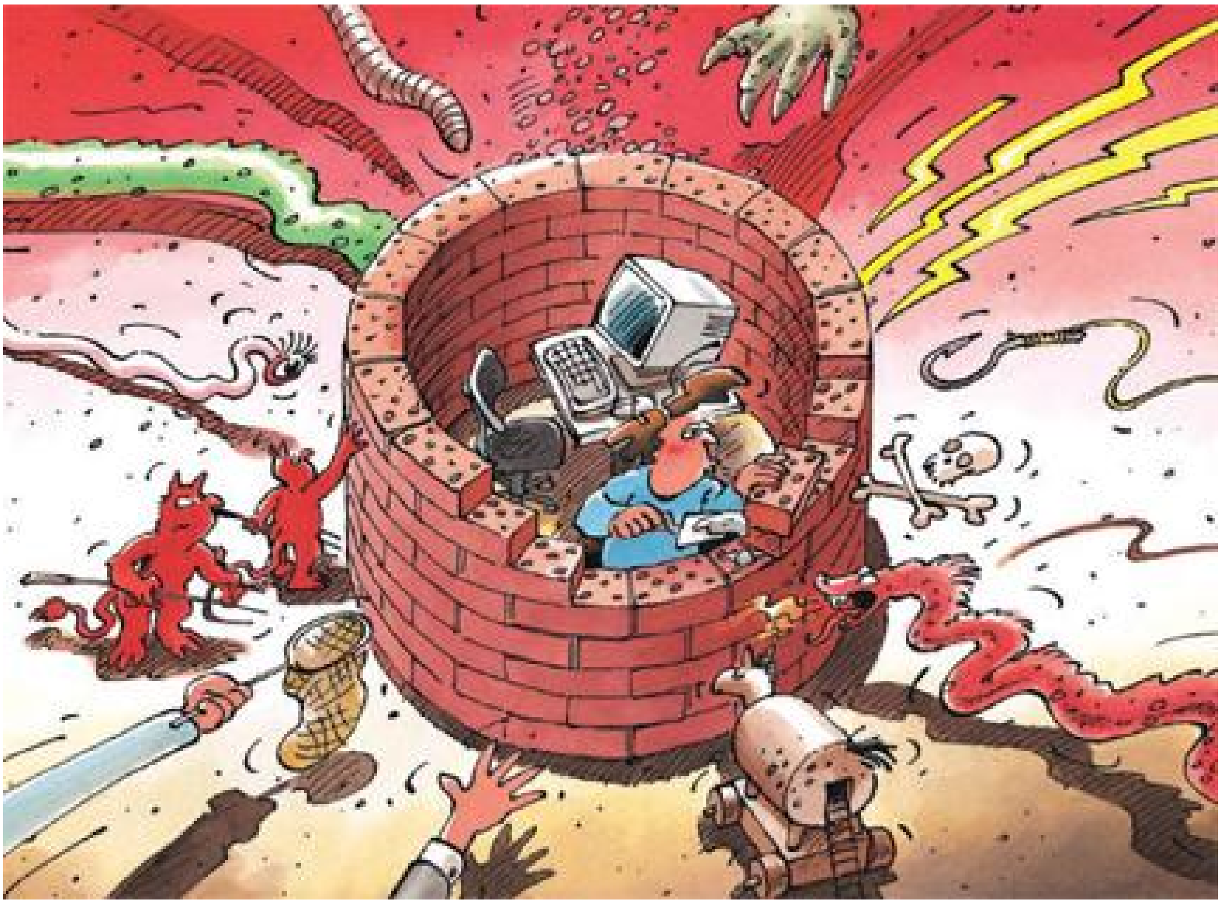
Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

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

Information Assurance

Situation in Switzerland and internationally

Semi-annual report 2012/II (July-December)



Contents

1 Focus areas of issue 2012/II

- **Phishing on the rise**
  Classic *phishing*, i.e. sending e-mails with the intent to trick the victim into divulging personal data in some way, is on the rise. Attackers are mainly targeting credit card data. Alongside the rather simple and widespread form of credit card *phishing*, a new modus operandi has emerged, however, also targeting Swiss e-banking clients in the second half of 2013.

  ► Current situation in Switzerland: Chapter 3.1

- **DDoS – massive attacks against various US banks**
  Attacks against the availability of websites, i.e. distributed denial of service (DDoS) attacks, are meanwhile among the main threats to networks. DDoS attacks, some of them massive, have been reported against various US banks since September 2012. Other attacks against availability have also made the headlines.

  ► Current situation in Switzerland: Chapter 3.6
  ► Current situation internationally: Chapter 4.2

- **Cyber conflict in the Middle East – update**
  As part of investigations of the "Flame" *malware*, the Russian anti-virus software manufacturer Kaspersky Lab discovered a further example of *malware* christened "Gauss". Gauss is the first known case where sophisticated, allegedly state-sponsored spy software exhibits the typical characteristics of an online banking trojan. Most of the infected devices were in Lebanon, followed by Israel and the Palestinian territories.

  The Saudi state oil company Saudi Aramco was crippled by *malware* infections. Shortly afterwards, the Qatari gas producer RasGas also had to separate its office network from the outside world. Although there is no official confirmation, various experts assume that RasGas was attacked by the same *malware*. Western experts speculate the attacks are part of efforts by Iran, whose energy exports have come under heavy pressure due to international sanctions, to prevent an increase of oil and gas production by Arab states.

  ► Current situation internationally: Chapter 4.1, Chapter 4.2

- **Dependency on ICT in daily life – always and everywhere**

  For several years already, not only computers and servers have been affected by cyber attacks. Every IT system can become a target for hackers. Breaking into electronically secured hotel doors is only one of many examples. The dependency of today's society on ICT is very multifaceted.

  ► Current situation in Switzerland: Chapter 3.4
  ► Current situation internationally: Chapter 4.3, Chapter 4.6

- **Regulation versus freedom – how to make the Internet secure?**
  To this day, the Internet is not regulated by the state and is largely governed as a free space via technical standards and administrative guidelines (referred to as policies). On the other side, there is a strong coalition of countries advocating Internet regulation to expand their state control to cyberspace and to strengthen their sovereignty.

  ► Current situation internationally: Chapter 4.9
  ► Trends/Outlook: Chapter 5.3

2 Introduction

The sixteenth semi-annual report (July-December 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 second 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 Phishing – current trends

Classic *phishing*, i.e. sending e-mails with the intent to trick the victim into divulging personal data in some way, is on the rise. Attackers are mainly targeting credit card data. Alongside the rather simple and widespread form of credit card *phishing*, *voice phishing* attacks have also emerged, however, targeting Swiss e-banking clients in the second half of 2013. Unlike e-banking *malware*, such attacks require only minimal technical infrastructure and can also be carried out by attackers without sophisticated technical know-how. In most cases, a computer and/or telephone will suffice.

3.1.1 Combined phishing/voice phishing attacks

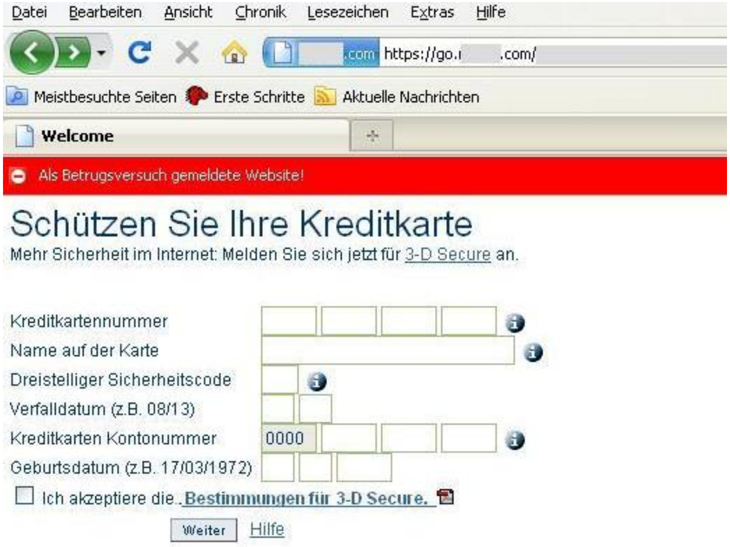
Since autumn 2012, a new modus operandi has been observed in *phishing* attacks in Switzerland: *phishing* e-mails are sent out, claiming that the financial institution has installed a new security system to protect e-banking accounts. According to the e-mail, a bank employee will soon contact the victim by phone to discuss and complete the process. For this purpose, victims are asked to provide personal data including their telephone number.

The victims are then called by the scammers – a new approach in Switzerland – and asked to divulge their password and second security element, supposedly for the purpose of improving security. Victims are for instance asked to enter a code in the card reader and report the result to the attacker. With this information, the scammer can log into the e-banking account and transfer money. If *transaction signing* is required to make the transfer, the process is repeated and the scammer again asks the victim for the transaction signature. The phone call sounds professional and is often even in Swiss German.

3.1.2 Phishing pages also with https

It has long been expected that attackers would start using *phishing* pages with encryption (https pages). In the autumn of 2012, several *phishing* waves did indeed link to encrypted pages. URLs beginning with https:// *(hypertext transfer protocol secure)* indicate that the information entered on the corresponding pages will be transmitted with encryption.

However, no special *certificate* is used, but rather simply the *certificate* of a hacked website. This cannot yet be considered a trend, however, since the cases have been isolated so far.


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
[redacted].com https://go.[redacted].com/
Meistbesuchte Seiten Erste Schritte Aktuelle Nachrichten
Welcome
Als Betrugsversuch gemeldete Website!

Schützen Sie Ihre Kreditkarte

Mehr Sicherheit im Internet: Melden Sie sich jetzt für 3-D Secure an.

Kreditkartennummer
Name auf der Karte
Dreistelliger Sicherheitscode
Verfalldatum (z.B. 08/13)
Kreditkarten Kontonummer 0000
Geburtsdatum (z.B. 17/03/1972)

□ Ich akzeptiere die Bestimmungen für 3-D Secure.

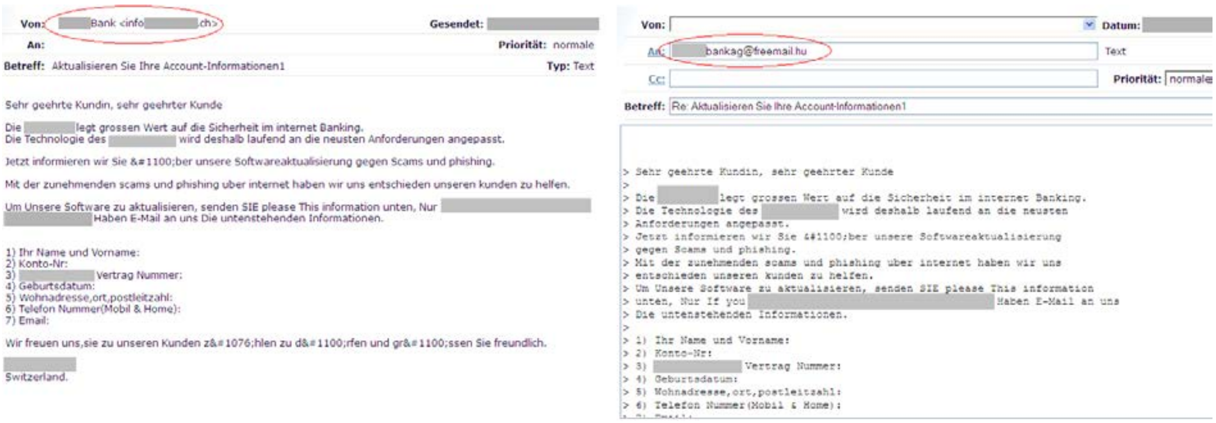
Weiter Hilfe

Figure 1: Phishing page with encryption

3.1.3 Phishing e-mails increasingly also without phishing page

As already reported in the last MELANI semi-annual report[1], *phishing* scammers are also trying to obtain victims' data even without classic *phishing* pages saved on a webserver. Two methods have established themselves in this regard: the first involves attaching a *phishing* page to the e-mail as an HTML form. When opened, the HTML page is built up locally on the recipient's computer. If the form fields are completed and the "Next" button is clicked, the data is sent "directly" to the attacker.

The second method is even simpler. Here, the form is simply integrated into the e-mail. Other than an e-mail address set up for the fraud, nothing else is required. The attackers also take advantage of the fact that for every e-mail, a special reply address can be defined that deviates from the visible sender address. Accordingly, the visible sender address may be the official address of a financial institution, and only once the reply button is clicked can the user see where the e-mail is actually being sent.



Von: [redacted]Bank <info[redacted].ch>
Gesendet: [redacted]
An:
Priorität: normale
Betreff: Aktualisieren Sie Ihre Account-Informationen1
Typ: Text

Sehr geehrte Kundin, sehr geehrter Kunde

Die [redacted] legt grossen Wert auf die Sicherheit im internet Banking.
Die Technologie des [redacted] wird deshalb laufend an die neusten Anforderungen angepasst.

Jetzt informieren wir Sie &#1100;ber unsere Softwareaktualisierung gegen Scams und phishing.

Mit der zunehmenden scams und phishing uber internet haben wir uns entschieden unseren kunden zu helfen.

Um Unsere Software zu aktualisieren, senden SIE please This information unten, Nur [redacted] Haben E-Mail an uns Die untenstehenden Informationen.

1) Ihr Name und Vorname:
2) Konto-Nr:
3) [redacted] Vertrag Nummer:
4) Geburtsdatum:
5) Wohnadresse,ort,postleitzahl:
6) Telefon Nummer(Mobil & Home):
7) Email:

Wir freuen uns,sie zu unseren Kunden z&#1076;hlen zu d&#1100;rfen und gr&#1100;ssen Sie freundlich.

[redacted]
Switzerland.

Von:
Datum: [redacted]
An: [redacted]bankag@freemail.hu
Text
Cc:
Priorität: normale
Betreff: Re: Aktualisieren Sie Ihre Account-Informationen1

```
> Sehr geehrte Kundin, sehr geehrter Kunde
>
> Die [redacted] legt grossen Wert auf die Sicherheit im internet Banking.
> Die Technologie des [redacted] wird deshalb laufend an die neusten
> Anforderungen angepasst.
> Jetzt informieren wir Sie &#1100;ber unsere Softwareaktualisierung
> gegen Scams und phishing.
> Mit der zunehmenden scams und phishing uber internet haben wir uns
> entschieden unseren kunden zu helfen.
> Um Unsere Software zu aktualisieren, senden SIE please This information
> unten, Nur If you [redacted] Haben E-Mail an uns
> Die untenstehenden Informationen.
>
> 1) Ihr Name und Vorname:
> 2) Konto-Nr:
> 3) [redacted] Vertrag Nummer:
> 4) Geburtsdatum:
> 5) Wohnadresse,ort,postleitzahl:
> 6) Telefon Nummer(Mobil & Home):
```

Figure 2: Phishing e-mail with prepared reply address. The e-mail appears to be from the info address of a Swiss bank, but the reply is sent to an address with a free e-mail service in Hungary.

[1] MELANI Semi-annual report 2012/1, Chapter 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 28 February 2013).

For the attacker, both methods have the advantage that the attacker does not need a hacked or specially established webserver where the *phishing* page would normally be placed. Law enforcement authorities or hosting providers can deactivate such webservers relatively quickly once they become known.

3.1.4 First Swiss domain deleted by MELANI at Switch

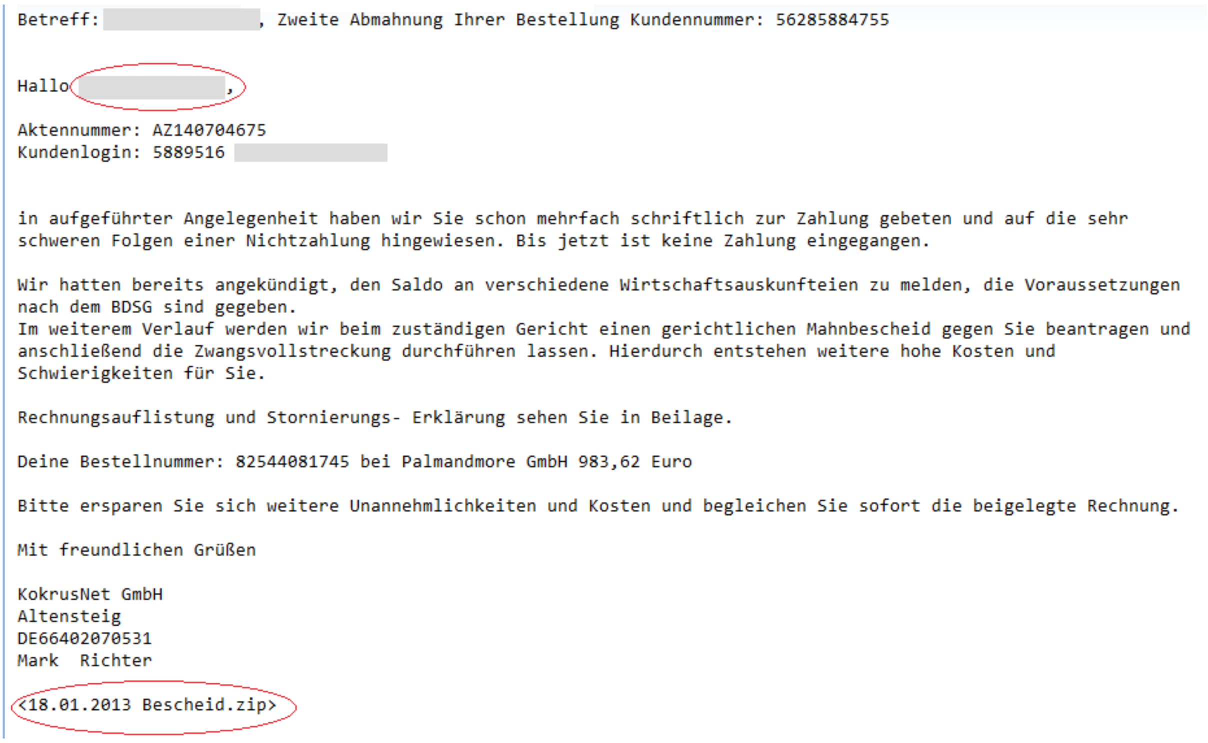
To combat the abuse of Swiss Internet addresses and to defend against acute dangers for Internet users, the revision of the Ordinance on Addressing Resources in the Telecommunications Sector (TSRO, SR 784.104; entry into force 1 January 2010) included a new article. According to the new provision, the ".ch" registry (SWITCH) must block domain names and cancel the respective assignment to a name server if an authority recognised by the Federal Office of Communications (OFCOM) for the purpose of combating cybercrime applies for the block, or if there is justified suspicion that the domain name is being used unlawfully. Unlawful purposes include obtaining sensitive data using unlawful methods (i.e. phishing) or spreading malicious software (i.e. malware) via the domain. SWITCH can take this measure of its own accord to defend against threats and maintain the block for 5 days. SWITCH has already availed itself of this possibility numerous times, especially to protect visitors to hacked websites. The Reporting and Analysis Centre for Information Assurance (MELANI) now had to use this power for the first time itself.

In December 2012, a *phishing* page with a Swiss Internet address was reported to MELANI. The domain was set up exclusively for the purpose of phishing and was not – unlike in many other cases – a hacked website on which scammers usually place the *phishing* page in a subdirectory. MELANI thereupon decided to extend the block, which SWITCH had already imposed for 5 days, by a further 30 days and at the same time to have SWITCH carry out a verification of the holder. Since this verification was not responded to, the domain was permanently deleted.

3.2 Bogus invoices with malware

For several months now, an increasing number of e-mails with bogus senders have been in circulation referring to a (bogus) order, delivery, or invoice. Every week, MELANI receives several such reports. By announcing payment reminders, subsequent costs, and possible lawsuits, the senders try to build up a threat and thereby trick the recipient into opening the attachment to get more information. In these cases, however, the attachment contains *malware*, generally within a zip file.

In the cases known to MELANI, these e-mails are personalised, i.e. include the first and last name of the recipient. Personalised addressing of fraudulent e-mails appears to be on the rise, since it creates a more trustworthy impression.



Betreff: [redacted], Zweite Abmahnung Ihrer Bestellung Kundennummer: 56285884755

Hallo [redacted],

Aktennummer: AZ140704675
Kundenlogin: 5889516 [redacted]

in aufgeführter Angelegenheit haben wir Sie schon mehrfach schriftlich zur Zahlung gebeten und auf die sehr schweren Folgen einer Nichtzahlung hingewiesen. Bis jetzt ist keine Zahlung eingegangen.

Wir hatten bereits angekündigt, den Saldo an verschiedene Wirtschaftsauskunfteien zu melden, die Voraussetzungen nach dem BDSG sind gegeben.
Im weiterem Verlauf werden wir beim zuständigen Gericht einen gerichtlichen Mahnbescheid gegen Sie beantragen und anschließend die Zwangsvollstreckung durchführen lassen. Hierdurch entstehen weitere hohe Kosten und Schwierigkeiten für Sie.

Rechnungsauflistung und Stornierungs- Erklärung sehen Sie in Beilage.

Deine Bestellnummer: 82544081745 bei Palmandmore GmbH 983,62 Euro

Bitte ersparen Sie sich weitere Unannehmlichkeiten und Kosten und begleichen Sie sofort die beigelegte Rechnung.

Mit freundlichen Grüßen

KokrusNet GmbH
Altensteig
DE66402070531
Mark Richter

<18.01.2013 Bescheid.zip>

Figure 3: Example of a bogus invoice with personalised form of address and *malware* (Bescheid.zip) in the attachment.

3.3 Control systems open on the net – also in Switzerland

The security of industrial control systems is not only a matter of discussion for security experts, but also increasingly so for the media.[2] According to the US Industrial Control Systems *CERT* (ICS-CERT), which issued a warning in this regard at the end of October[3], attacks against such systems have been on the rise. The background of the warning is that more and more tools are being offered that allow attackers to identify and penetrate such systems. Special knowledge is not needed. The best-known tool in this regard is certainly the search engine "SHODAN", which has existed already for several years, searches the Internet for *SCADA* systems, and was already discussed in a previous semi-annual report[4]. Using this search engine, ICS-CERT was able to find more than 500,000 systems. Apart from SHODAN, other tools exist such as the Every Routable IP Project (ERIPP).

On the other side there is a large number of operators of industrial control systems that so far have focused primarily on functional stability and less on safety from manipulation. This may also be because many do not even know whether the systems are really connected to the Internet. Additionally, many manufacturers hardcode universal passwords in the application so that the manufacturer can access the systems even if the access data is lost. These emergency passwords have the advantage that stable operation of the devices is possible even if the password is lost, but naturally they also offer a certain attack vector. Another case became public in August 2012 through security researcher Justin W. Clarke. In the proprietary operating system Rugged OS, which is used for applications such as power

[2] http://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/report-februar-102.html (as at 28 February 2013).

[3] http://ics-cert.us-cert.gov/index.html (as at 28 February 2013).

[4] MELANI Semi-annual report 2011/2, Chapter 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en (as at 28 February 2013).

plants and traffic monitoring, Clarke found a hardcoded, secret *RSA key*. If this key is known, the encrypted network traffic can be decrypted and tapped. ICS-CERT subsequently issued a warning in this regard.[5]

Another problem was identified by Phil Kernick, an Australian security expert. In virtually all *SCADA* incidents he investigated, *malware* had been used. But the *malware* was not targeting SCADA systems specifically. Instead, it was for instance conventional e-banking *malware*. As a consequence of this infection, the systems' operation was no longer stable, and the systems crashed from time to time. This can have serious consequences in the case of SCADA systems. The cause is usually that control networks and office networks are not strictly separated. Also the possibility of connecting USB storage devices or third-party mobile computers (e.g. by employees or external contractors) is often problematic, since the necessary user policies and/or technical obstacles are usually missing.

In principle, machines should be connected to the Internet only where absolutely essential for operations. These systems must of course be sufficiently protected with firewalls and strong passwords. To prevent the spread of *malware* from office computers to SCADA systems, these two networks should be separated from each other.

After MELANI reported already in its Semi-annual report 2011/2 how the search engine SHODAN could be used to find 34 vulnerable systems in Switzerland, such systems were also identified in 2012. These systems were either not protected at all or only with a standard password that should have been changed when operations began. While these potential targets are as a rule not classified as sensitive, the fact that the default password was not changed when installing the control system connected to the Internet is a serious violation of basic principles of IT security. The possibility of, for instance, accessing the heating or air conditioning network of another business and manipulating it could potentially have serious consequences.

Furthermore, the partial integration of other company-internal administrative applications such as accounting software and the like, and the possibilities of accessing them, open up additional potential for abuse. In principle, industrial control systems should not be connected to the Internet. If doing so is absolutely essential, special care must be taken.

3.4 Traffic light breakdown in Vaud

An IT breakdown in the traffic guidance system of the canton of Vaud resulted in traffic obstructions and kilometres of congestion along the motorway between Lausanne and Chexbres on 16 July 2012. At 4 p.m., the traffic surveillance section of the Vaud police noted technical problems. Shortly thereafter, the system stopped working, and traffic signals jammed. In the Flonzaley tunnel, the left lane was blocked and could no longer be freed, resulting in a 15-kilometre tailback. After a technician intervened manually, the traffic between Lausanne and Chexbres slowly began to return to normal again from 7:30 p.m. The IT breakdown was only fixed at 1:40 a.m., however.

Additionally, transmission of the alarms in the tunnels of the Vaud motorways was interrupted. If there had been a fire or an accident, the emergency system in the tunnels

[5] http://ics-cert.us-cert.gov/pdf/ICS-ALERT-12-234-01.pdf (as at 28 February 2013).

would not have worked. While surveillance cameras continued to transmit images, they could no longer be moved. For this reason, police officers were posted at important points.[6]

Although this incident was a breakdown, not an attack, it shows how multifaceted the dependency of today's society on ICT is. More and more ICT systems are being employed also for road traffic signals, in order to manage an increase in traffic without changing the infrastructure. Such systems are designed so that they shut down when they malfunction, or all signals are switched to a blinking amber light. This is intended to rule out a situation where everyone on the road has a green light, leading to accidents.

3.5 Breakdown at Ricardo

On 28 October 2012, the online auction site ricardo.ch had severe IT problems. An error in the database entailed that about one third of its users were unable to bid for several hours. As a consequence, products were generally sold at significantly less than their value, since the auctions were completed as planned despite the glitch, but bids were no longer possible. In an auction, the last few minutes are known to be the most lucrative. Ricardo.ch subsequently made clear that offers concluded during the breakdown "would in all cases have to be sold to the buyer at the best bid achieved".

Two weeks later, and probably also after various user protests, the statement above was revised. According to ricardo.ch, it had been assumed that the affected offers would automatically be extended in time, which however was not the case for all offers. Ricardo.ch now communicated that in such cases, the seller was in principle not bound by the contract, and affected sellers could contact customer service[7]: As an act of courtesy Ricardo has refunded their customers in some cases with higher sums of money.

Like virtually all companies, ricardo.ch excludes liability for technical problems. In most cases, the risk is therefore borne by the client. Accordingly, the general terms and conditions of ricardo.ch state that the company is liable only for grossly negligent or intentionally caused temporary unavailability of the website, failure of individual or all website functions, or malfunctions of the website. In particular, ricardo.ch is not liable in the case of slight negligence for technical problems due to which the offers or bids are accepted or processed with a delay or incorrectly.[8] Where incidents do occur, especially if money is at stake, the general terms and conditions are usually faced with public pressure. Especially because of the threat of damage to their reputation, companies often are accommodating and do not insist on the general terms and conditions in such cases.

[6] http://www.vd.ch/autorites/departements/dse/police-cantonale/medias/communiques-de-presse/articles/disfonctionnement-reseau-informatique-gerant-la-signalisation-routiere-sur-les-autoroutes-vaudois/ (as at 28 February 2013).

[7] http://blog.ricardo.ch/2012/11/teilausfall-von-ricardo-ch-am-28-oktober-2012/ (as at 28 February 2013).

[8] http://www.ricardo.ch/ueber-uns/Portals/ch-ueber-uns/Docs/downloads-pdf-de/AGB_DE.pdf (as at 28 February 2013).

3.6 DDoS attack against Inside Paradeplatz

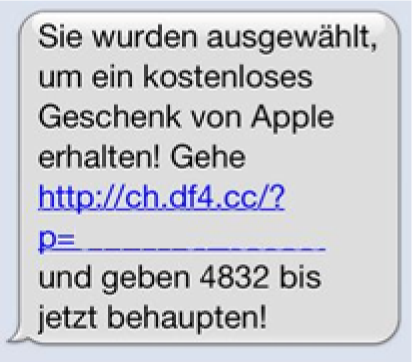
Twice within three months, the website "Inside Paradeplatz" was shut down with a *distributed denial of service attack* (DDoS attack). Already in June, unknown attackers targeted the website and sent thousands of queries per second to the website, so that it was temporarily no longer available. The same happened again at the beginning of September, but lasted much longer than the first attack, which was over after one and a half days. Additionally, the personal website of the operators was apparently also compromised at the same time as the second attack, placing a *drive-by infection* on it. According to the website owner, a corresponding warning to this effect was displayed, if the site was searched via Google and clicked on.[9] According to him, the aim was to prevent information from being disseminated by a different channel. These facts indicate that the attack was targeted. It is very complex to determine who the perpetrator is in such cases, however, since the traces of the attack are concealed.

DDoS attacks are meanwhile one of the main threats to networks. A selection of DDoS attacks abroad can be found in Chapter 4.2. Nevertheless, the attack above is striking and tends not to correspond to the usual DDoS attacks. Especially the fact that the private site of the operator was also attacked in order to place a *website infection* leaves room for speculation. The reason cited by the website owner that the attacker used the website infection to prevent information from being disseminated by a different channel, is only partially plausible. This is because the private site could likewise simply have been targeted with a DDoS attack, if the goal had been to prevent the dissemination of information.

One can speculate about other purposes, for example that the attacker in this case wanted to infect targeted computers belonging to persons in the environment of the operator with *malware*, in order to obtain information. Among persons in the environment of the operators, the probability is especially great that they will first go to the private website of the operator to find out why the official site is no longer working.

3.7 A gift from Apple or a potential fraud?

In November 2012, a *SMS* text message in bad German was circulated, claiming that the recipient had received a gift from Apple. In light of the high reporting rate to MELANI, this SMS was likely sent on a large scale. The SMS contained a winning code and a link. The domain names were always constructed according to the same pattern, each of them containing the *top-level domain* ".cc".

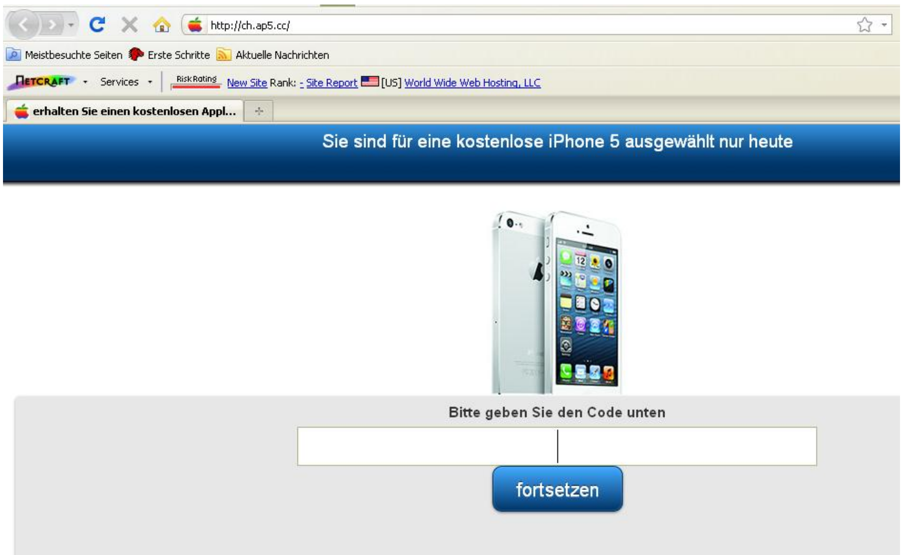


Sie wurden ausgewählt, um ein kostenloses Geschenk von Apple erhalten! Gehe http://ch.df4.cc/?p=______________ und geben 4832 bis jetzt behaupten!

Figure 4: SMS with supposed winning notification

[9] http://insideparadeplatz.ch/2012/08/28/inside-paradeplatz-im-visier-von-hackern/ (as at 28 February 2013).

To receive the free iPhone 5, the code which was contained in the SMS supposedly had to be entered on the indicated website. An analysis showed that any number whatsoever could be entered, and the user would then be linked to another page. Even this fact alone makes the SMS appear suspicious, indicating that the entire operation was only a pretext to entice the recipient into doing something.


http://ch.ap5.cc/
Meistbesuchte Seiten
Erste Schritte
Aktuelle Nachrichten
NETCRAFT
Services
Risk Rating
New Site Rank: - Site Report [US] World Wide Web Hosting, LLC
erhalten Sie einen kostenlosen Appl...

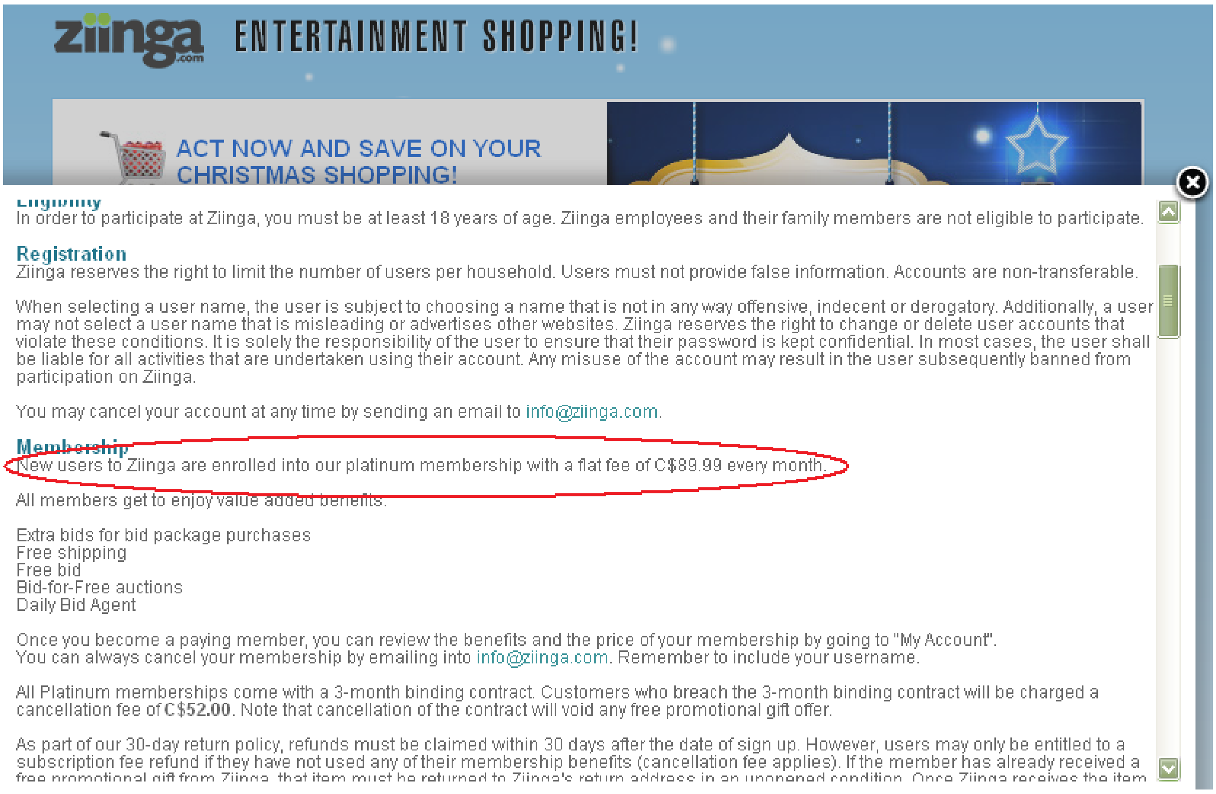
Sie sind für eine kostenlose iPhone 5 ausgewählt nur heute

Bitte geben Sie den Code unten

fortsetzen

Figure 5: Page on which the supposed winning code was to be entered

After entering the winning code, the user was redirected to the website of a company named "Ziinga". This company offers so-called entertainment shopping, in concrete terms it is an auction platform. On this page, victims are asked to enter their last and first name, e-mail address and gender, and to accept the general terms and conditions. Victims may certainly think this is plausible, since they might still believe they have won an iPhone. By accepting the general terms and conditions, however, the victim becomes a apparently a platinum member at the price of $89.99 a month as seen on Figure 6.



Eligibility

In order to participate at Ziinga, you must be at least 18 years of age. Ziinga employees and their family members are not eligible to participate.

Registration

Ziinga reserves the right to limit the number of users per household. Users must not provide false information. Accounts are non-transferable.

When selecting a user name, the user is subject to choosing a name that is not in any way offensive, indecent or derogatory. Additionally, a user may not select a user name that is misleading or advertises other websites. Ziinga reserves the right to change or delete user accounts that violate these conditions. It is solely the responsibility of the user to ensure that their password is kept confidential. In most cases, the user shall be liable for all activities that are undertaken using their account. Any misuse of the account may result in the user subsequently banned from participation on Ziinga.

You may cancel your account at any time by sending an email to info@ziinga.com.

Membership

New users to Ziinga are enrolled into our platinum membership with a flat fee of C$89.99 every month.

All members get to enjoy value added benefits.

Extra bids for bid package purchases
Free shipping
Free bid
Bid-for-Free auctions
Daily Bid Agent

Once you become a paying member, you can review the benefits and the price of your membership by going to "My Account".
You can always cancel your membership by emailing into info@ziinga.com. Remember to include your username.

All Platinum memberships come with a 3-month binding contract. Customers who breach the 3-month binding contract will be charged a cancellation fee of C$52.00. Note that cancellation of the contract will void any free promotional gift offer.

As part of our 30-day return policy, refunds must be claimed within 30 days after the date of sign up. However, users may only be entitled to a subscription fee refund if they have not used any of their membership benefits (cancellation fee applies). If the member has already received a free promotional gift from Ziinga, that item must be returned to Ziinga's return address in an unopened condition. Once Ziinga receives the item

Figure 6: General terms and conditions of Ziinga (as of 30 November 2012)

Ziinga is also mentioned on Wikipedia. The neutrality of the article is disputed, but it still offers some indications of what is going on. The hidden publication of the membership fee in the general terms and conditions has repeatedly been criticised[10]. While the membership can be cancelled retroactively at any time, a cancellation fee of GBP 28 or USD 52 is required. In this case, however, Ziinga distanced itself from the sent SMS message and ruled out a connection. The question remains, however, who other than Ziinga would have had an interest in sending the SMS. It could not be determined who actually sent the SMS. *Malware* was not found on the indicated pages.

Another motive for sending the SMS might also have been to verify valid mobile phone numbers. Every sent link was in fact unique and contained a code that could be used to derive the mobile phone number in question. When recipients clicked on the link, they signalled to the sender that the mobile phone number was operational. If the query additionally is coupled to entry of an e-mail address, then it is even possible to associate the mobile phone number with the e-mail address. Such data could then in turn be used for targeted *phishing* attacks or resold to interested groups.

3.8 Phone phreaking – old scam on the rise[11]

The first practices of *phreaking* occurred already with the rise of automatic switching stations of telephone companies, reaching their peak in the 1970s to mid-1990s. The invention of *phreaking* is attributed to a person with the nickname "Cap'n Crunch". The goal was to gain access to telephone systems in order, for instance, to make calls for free. *Phreaking* affects landlines and recently also *VoIP* systems of private individuals, as well as telephone systems of companies of all sizes. If the attack succeeds, telephone systems can be abused for various forms of fraud.

Criminals gain access to a telephone system especially through maintenance software, which is often protected only with a standard *PIN*. But perpetrators also often are able to hack telephone systems that are well secured and maintained. To conceal their identity and make themselves difficult to trace, perpetrators may use a form of *spoofing*. *Spoofing* conceals one's own calling number and simulates a different phone number instead. The technology and standard PINs for this purpose can be found on the Internet.

Under the most common modus operandi, premium-rate numbers are used. Premium-rate numbers are services going beyond telephony, which however must be paid via the telephone subscription. 0900 numbers in Switzerland are an example. Using this variant, the perpetrator gains access to the telephone system of a company as a first step. Thanks to this control, perpetrators are then able to connect the phone lines with a premium-rate number they have established. So that the company does not notice the intervention too quickly, attacks are carried out outside business hours. Since the perpetrators must occupy a large number of the company's phone lines, the probability that the fraud will be noticed is significantly higher during business hours. The main attack is often preceded by smaller attacks. Abuse of the premium-rate number is generally set up in countries where it is difficult to trace the perpetrators.

Another variant affects online payment systems. Cards with online credit are sold by various outlets such as kiosks and petrol stations. Using *spoofing*, the perpetrators pretend to be

[10] http://en.wikipedia.org/wiki/Ziinga#Controversy (as at 28 February 2013).

[11] This article is based on a report by fedpol, the Federal Office of Police, which was kindly made available to MELANI.

calling from a service number of the company issuing the online credit for the cards and get in touch with individual sales outlets. The employees believe they are talking to a representative of the card issuer, so they divulge the codes and information of cards with online credit. The perpetrators then immediately cash in the credit on the Internet. This makes it impossible to prevent the damage. For this form of phone *phreaking*, the perpetrators need insider knowledge. Firstly, they must know the correct service number of the company, and secondly, they must have knowledge of the technical processes and also be familiar with the support procedures.

Hacked *VoIP* systems can also be used to carry out *vishing* attacks (see Chapter 3.1).

To commit phone *phreaking*, special technical knowledge is necessary. While detailed instructions are available on the Internet, perpetrators must nevertheless always be able to respond to new security precautions and adjust their approach, which may at times require programming processes. In order to penetrate phone systems even when they are well secured and protected, additional detailed information on the organisation, processes and employees of a company is necessary, which often requires insider knowledge. But phone *phreaking* should be expected to become increasingly simple in future and also cover new areas. For instance, there is a risk that *smartphones* will increasingly be affected – hacking of *smartphones* can also be referred to as *phreaking*. The control gained by hacking mobile phones can be exploited by criminals for instance in order to use *SMS* services subject to a fee.

3.9 Second pan-European "Cyber Europe 2012" exercise – again with Swiss participation

On 4 October 2012, more than 500 cyber specialists took part in the second pan-European cyber security exercise, "Cyber Europe 2012". The heart of the exercise was communication and coordination at the international and European level to improve the robustness of critical information infrastructures. Cyber Europe 2012 was a milestone for strengthening cooperation, preparedness and responsiveness in the event of a pan-European cyber security crisis.[12]

Cyber Europe 2012 had three objectives:

- Test effectiveness and scalability of standard procedures for public authorities' cooperation in Europe.
- Explore the cooperation between public and private stakeholders in Europe.
- Identify gaps and challenges on how large-scale, cross-border cyber incidents could be handled more effectively in Europe.

29 EU member states and EFTA countries (European Free Trade Association) took part in the exercise; 25 of these countries (including Switzerland) took part actively in the exercise, while the remaining four were present as observers. Additionally, various EU bodies also participated. In total, 339 organisations with a total of 571 individual participants were involved. In accordance with a recommendation and unlike the previous exercise, Cyber Europe 2010, this time stakeholders from the private sector also took part. In Switzerland, these were two companies each from the telecommunications and financial sectors. As the

[12] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_DE_TRA.pdf (as at 28 February 2013).

exercise was designed, however, cooperation among stakeholders in the public and private sector was limited to the national level, while the public sector cooperated also across borders.

The focus of the exercise scenario was on large-scale network incidents in Europe, affecting all participating countries. The scenario assumed that attackers had joined together for a massive cyber attack against Europe, primarily using *DDoS* attacks against electronic services. For instance, eGovernment and financial services (e-banking, etc.) were affected. These network incidents represented a challenge for participants from both the public and the private sector and required cross-border cooperation.

Cyber Europe 2012 was an opportunity to explore, understand and evaluate existing European cyber-security cooperation mechanisms. The exercise also strengthened cooperation among the participants.

Experiences and insights:

- All participating countries were fully engaged in the exercise phase. During the exercise many bilateral and multilateral interactions at the international level took place.
- Having a set of standard procedures and communication tools helped to provide situational awareness during the simulated cyber-crisis.
- Vulnerabilities were identified in the operational procedures, however, notably in terms of scalability due to the large number of participating countries.
- Familiarity of the involved entities with the standard procedures is crucial for building a fast and effective response capability across Europe.
- In Switzerland, contacts with the private sector participants were well established. The large volume of information and the handling, however, represented a challenge.
- Appropriate, stable and up-to-date communication infrastructures and tools are critical to ensuring smooth and effective cooperation.
- Cyber Europe 2012 helped to build trust between countries, which is key to successful and timely risk mitigation activities during real cyber-crises. The exercise fostered both new and existing relationships.

4 Current international ICT infrastructure situation

4.1 Cyber conflict in the Middle East – update

4.1.1 Gauss: Online banking trojan meets spy software

In its investigations on the *malware* "Flame"[13], Russian anti-virus software manufacturer Kaspersky Lab discovered a further example of *malware*, which was christened "Gauss". It is

[13] On Flame, see MELANI Semi-annual report 2012/1, Chapter 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 28 February 2013).

striking that the architecture, module structure, code base, and communication forms with the *command & control server* are very similar for Flame and for Gauss. In light of these similarities, it is natural to conclude that the same authors are behind these two *malware* programs.

According to reports, Gauss had been active since September 2011 and was likely able to spy on tens of thousands of computers until it was discovered in June 2012. Most of the infected devices were in Lebanon, followed by Israel and the Palestinian territories.

Gauss's functions include harvesting the Internet passwords, online bank account information, *cookies* and special configuration data of the infected computers. The *malware* was programmed so as to facilitate especially the gathering of data associated with Lebanese bank accounts.

Gauss is the first known case where sophisticated, allegedly state-sponsored spy software exhibits the typical characteristics of an online banking trojan. Unlike the known online banking trojans of criminal Internet scammers, the corresponding function in Gauss does not trigger bank transactions to the financial detriment of the users, but rather spies on what bank transactions are carried out with the infected computer.

4.1.2 Shamoon: Espionage and sabotage at oil and gas companies

On 15 August 2012, computers in the office network of the Saudi state oil company Saudi Aramco were crippled by a *malware* infection. The *malware*, named "Shamoon", had gathered information on files from the infected systems and forwarded it to the attacker before deleting the files and overwriting the *master boot record (MBR)*. In this way, the affected computers were rendered inoperable and had to be reinstalled. According to information from Saudi Aramco, more than 30,000 computers in the company network were infected – but this did not impact oil production and trading. The affected devices could all be repaired.

Shortly afterwards, the Qatari gas producer RasGas had to separate its office network from the outside world. Although there has been no official confirmation, various experts assume that RasGas was also targeted by Shamoon.

The described functionality of Shamoon is reminiscent of the *malware* "Wiper" discovered in the spring 2012[14], which was active in Iran. An analysis of Shamoon indicates, however, that the authors are not the same.
The effort necessary for this attack was substantial, which makes it likely that a state was involved, or at least that a state supported the perpetrators. Various western experts in fact speculate that the attacks are part of efforts by Iran, whose energy exports have come under heavy pressure due to international sanctions, to prevent an increase of oil and gas production by Arab states.

[14] On Wiper, see MELANI Semi-annual report 2012/1, Chapter 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 28 February 2013).

4.1.3 Hacktivism in connection with the Middle East

In addition to the two spectacular attacks mentioned above, several smaller attacks in connection with the Middle East took place in the second half of 2012 as well. Here is a selection:

- In August, the blog platform of the news agency Reuters was attacked twice and the Twitter account @ReutersTech once. The goal in each of these attacks was to spread propaganda and erroneous news on events in the Middle East.

- Also in August, targeted e-mails were sent to Syrian dissidents, asking them to download a supposed security program named "Anti Hacker" to protect them from malicious attackers. The program concealed spy software, however.[15]

- A group of (self-declared) Pakistani hackers protested the controversial film "Innocence of Muslims" in September by defacing various websites. In mid-November, this group especially also targeted Israeli websites. At the time, "Operation Israel" was also being carried out by Anonymous. This operation was launched when the Israeli government declared its intention to cut telecommunications connections with the Gaza Strip.

- Anonymous "declared war" against the Assad regime in Syria, since that regime had cut Internet connections abroad.[16]

- A hacker group took over several user accounts of the Israeli Vice Prime Minister and used it to spread pro-Palestinian propaganda. This was apparently not part of Anonymous's "Operation Israel", however, but was an independent act of solidarity with Palestine.

- Because of warnings of a large-scale attack against the Israeli police using *malware*, police computers were temporarily separated from the Internet as a precaution. Officers were sensitised to refrain from connecting USB devices to their police computers. The internal computer system of the police was always operational, however; only e-mail communication with the authorities was temporarily not possible.

- The International Atomic Energy Agency (IAEA) reported an attack, in which personal contact data of scientists was gathered and placed on the Internet. The attackers threatened to publish additional sensitive information if the attacks against Iranian nuclear scientists continued – in recent years, several scientists in Iran have been killed in attacks for which the Iranian government holds Israel and the United States responsible.

- The security firm Symantec discovered the computer worm "Narilam", which appears to have mainly targeted companies in Iran. The analysis indicates that this *malware* was not intended to spy, but rather to carry out targeted attacks against economically relevant (e.g. accounting) databases and to change or delete datasets.[17]

Speculation is certainly possible regarding the respective authors of these attacks. It will likely be difficult to prove, however, whether ultimately state organisations, patriotic hackers,

[15] https://www.eff.org/deeplinks/2012/08/syrian-malware-post (as at 28 February 2013).

[16] http://www.youtube.com/watch?v=olZzqa6nwos; http://www.youtube.com/watch?v=xdmlPhWIAuw (as at 28 February 2013).

[17] http://www.symantec.com/connect/blogs/w32narilam-business-database-sabotage (as at 28 February 2013).

or sympathisers of a certain group are behind the attacks and from whom the perpetrators received what kind of support.

4.2 DDoS attacks – motives, perpetrators and victims

Attacks against the availability of websites, i.e. *distributed denial of service (DDoS)* attacks, are employed for different purposes in the cyberworld. We have already reported on them in previous semi-annual reports.[18] In the beginning, attacks were primarily simple acts of vandalism. In the meantime, motives have changed, however. For instance, DDoS attacks are being observed as tools for revenge, for damaging competitors, for protection rackets, or for politically motivated attacks. While smaller DDoS attacks generally stay hidden and do not become public, there are always also major DDoS attacks with the goal of achieving substantial (media) attention. Websites and webservers are the preferred targets for this purpose. But also mail servers, *DNS* servers, *routers*, *firewalls* and other kinds of Internet services may be affected. In the second half of 2012, the attacks against US banks certainly constituted a new kind of attack. But also other attacks against availability made the headlines:

4.2.1 DDoS attacks against US banks

Denial of service (DDoS) attacks, some of them massive, have been reported against various US banks since September 2012. The targeted banks include Bank of America, Citigroup, Wells Fargo and others. So far, no data theft has been reported, but there were frequently problems accessing the affected banks' websites.

At times, the data volume of the attacks was more than 60 GB/s. Since the beginning of the attacks, numerous sources have suspected that the attacks come from Iran, and not from criminal circles there, but rather from the state, or at least that they are being supported or tolerated by the state. An article in the New York Times, for instance, mentions that unnamed persons in the US government assume that Iran is the cause of the attacks.[19] However, there has been no proof of this theory so far. To date, only the facts that the attacks last a long time and are difficult to contain indicate that there might be a connection with a government. Admittedly, proof is difficult to find in such cases, and experience shows that it must also be treated with caution, since both sides have a considerable political interest. Iran has always categorically denied involvement in these attacks.

Various analysts assume that the attacks are a result of the economic embargo of the United States against Iran and should be considered a retaliatory measure. The group Izz ad-Din al-Qassam Cyber Fighters, which claimed responsibility for the attacks already at the outset, cited the dissemination of the Muhammad video as a justification.[20] There are also speculations that hacktivism might be used to conceal other motives in these cases.[21]

[18] See also MELANI Semi-annual Report 2010/2, Chapter 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=en (as at 28 February 2013).

[19] http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=1& (as at 28 February 2013).

[20] http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 (as at 28 February 2013).

[21] http://blogs.techworld.com/war-on-error/2013/01/iran-v-usa---the-worlds-first-cyberwar-has-started/index.htm (as at 28 February 2013).

Attacks have also been perpetrated from Swiss computers. Generally, webservers with a relatively large bandwidth were involved, which were compromised especially for this purpose by the attackers. The operators of these webservers were notified by the Reporting and Analysis Centre for Information Assurance (MELANI).

According to statements by the US banks, the DDoS attacks have continued, but their consequences are meanwhile less serious. The outages caused by DDoS apparently declined in the first weeks of January, although the attackers announced new massive attacks again at the beginning of the year. Observers see this as proof that the financial institutions have meanwhile improved their ability to successfully defend against the attacks.[22] The traffic statistics of 13 leading US institutions in January 2013 showed site availability of 97%, while availability of only 95% was achieved during the first phase of the attacks. (1% of a day is equivalent to approximately 15 minutes).

Apart from the technical preparations, organisational and communicative measures in particular must be taken for a DDoS attack. What and how a company communicates is without a doubt a decisive factor. A communication strategy can be seen as a first measure against the effects of DDoS attacks. Careless communication, in contrast, may also be a trigger of a (further) DDoS attack. The risks and consequences of communication to the general public must therefore be assessed in advance.

Technical precautions are certainly a second crucial factor. It is much easier to take precautions before an attack occurs than once the company infrastructure is already under attack. This is the case especially for companies whose existence depends largely on online services or sales. Normally, the upstream provider has the experience and possibility to make appropriate solutions available to defend against DDoS attacks.

The measures mentioned above naturally apply especially to critical information infrastructures. If a DDoS attack affects an entire economic sector or even crosses sectors, information exchange among companies is extremely important. This makes it possible to prevent or at least cushion the attacks. MELANI assures such information exchange for the operators of critical infrastructures in Switzerland.

4.2.2 DDoS attack against German electricity supplier

The webservers of the German power grid operator "50 Hertz Transmission" were the victim of a DDoS attack for several days. The company connects nearly one third of Germany to the power grid. However, the electricity supply was not interrupted at any time by the attack, since the attacker did not target the control systems (*SCADA*), but rather "only" the webservers of the company. E-mail communication was also affected and interrupted by the attack. 50 Hertz reacted by disconnecting the servers from the network.

According to media reports, thousands of *IP addresses* from Eastern Europe and especially Russia were used for the attack.[23] Whether the perpetrators are really from that region or whether someone simply rented a botnet from there is just as unclear as the motive for this attack.

[22] http://www.bankinfosecurity.com/are-banks-winning-ddos-battle-a-5434 (as at 28 February 2013).

[23] http://www.welt.de/wirtschaft/energie/article111369975/Russische-Hacker-attackieren-Stromnetzbetreiber.html (as at 28 February 2013).

Economic pressure is increasingly leading to standardisation of systems; not only individual components, but entire substations are being operated by remote control and without staff. In most cases, however, administrative and control networks are still strictly separated. But universal use of the same network technology is increasingly tempting companies to combine their business and control networks in order to simplify administrative processes. The different demands on security precautions and the possibilities available in this regard must in all cases be taken account of, however.

Additionally, it should be noted that especially in the case of power suppliers, not only an attack on control systems can have consequences for stability of the power grid; also systems supplying information for the maintenance of grid stability may be essential. Especially these systems are increasingly connected with the administrative network and accordingly constitute a possible point of attack.

4.2.3 DDoS attack against Swedish government servers and banks

At the beginning of October, DDoS attacks on several Swedish companies and authorities were reported. In addition to banks, the targets included the websites of the Swedish train operator SJ, the news agency TT and military servers. It is suspected that the attacks were in response to Sweden's request for extradition of Julian Assange. Only three days later, Swedish servers were again targeted by a DDoS attack. This time, the focus was on the Swedish central bank, the Swedish parliament, and the national security service Säpo. These DDoS attacks were announced by Anonymous. They were motivated by the protest against the Swedish justice authorities, who had previously cracked down on platforms permitting the download of films and other content using *BitTorrent*.

4.2.4 Attacks against DNS infrastructure

Increasingly, DNS infrastructure is also the focus of attacks. With the help of the *domain name system (DNS)*, the Internet and its services are made user-friendly by permitting *URLs* (e.g. www.melani.admin.ch) to be entered instead of *IP addresses*. At the top of the hierarchy are the root servers, which are responsible as the highest instance for information regarding *top-level domains* (TLDs, e.g. .com, .net, .ch). In addition to these TLD name servers, every provider also runs DNS servers, which provide interim storage for the top-most DNS information and make it available to (the computers of) its clients.

Between 3 and 6 September 2012, Deutsche Telekom dealt with a massive attack on this DNS infrastructure. The attack was successfully repelled, however. No limitation of name resolution was observed.

At the beginning of 2013, SWITCH was also affected by an attack on its DNS infrastructure. This attack was also repelled.[24] This was the first time that the CH-TLD infrastructure was attacked. This *DNS amplification attack* did not target the CH infrastructure, however. It was only a means to an end to attack webservers in the United States. The described "DNS amplification attack" method exploits the fact that name servers in some cases respond to small request packets with very large packets. Theoretically, a 60-byte request may generate a 3,000-byte response. These large responses are then redirected to the actual targets. Using this trick, the attackers require a smaller attack infrastructure (botnet) to generate a large data flow.

[24] A detailed analysis of this attack will follow in MELANI Semi-annual report 2013/1

DDoS attacks are among the main threats to networks. Not necessarily the number of attacks is increasing, but rather they are growing in complexity. Increasingly, attacks against DNS protocols are also being observed.[25] In its blog, SWITCH writes that the DNS protocol is currently the most frequently abused protocol for DDoS attacks. Furthermore, *authoritative DNS servers* are now being used more and more, rather than publicly accessible *DNS resolvers,* as used to be the case.[26]

4.3 Vulnerability in POS terminals

Until now, the focus of attackers in regard to credit card terminals, or *POSs (points of sale),* has mainly been on classic *skimming* methods, which attach additional hardware to the terminal in order to read the magnetic strip and the *PIN*. This modus operandi has also been used in Swiss shops.[27] A new vulnerability published by German security experts Thomas Roth and Karsten Nohl of SRLab at the beginning of July 2012 now draws attention to an additional danger.

The security experts found a critical vulnerability in the "Hypercom Artema Hybrid" card terminals of the manufacturer Verifone. The card reader is attacked using a *buffer overflow* in the *network stack*, allowing the application processor to be taken over. In this way, the attacker gains access to the terminal via the network and is able to control the entry field and display and intercept the PIN and the magnetic strip data. A potential attacker thus no longer needs to gain direct access to the device: access via *TCP/IP* to the terminal suffices. This does not necessarily require physical access to the company network. The attacker may for instance also gain access by smuggling *malware* onto the computer of an employee. It is of course even easier if the card terminal is accessible directly from the Internet, i.e. uses a *public IP address*.

Local attacks directly at the unit are also possible using the serial interface and the JTAG-interface. If JTAG is used, one operates beyond the software-level and the processor is directly accessed. That's the reason why this vulnerability can't be completely resolved through a single software update. [28]

The Reporting and Analysis Centre for Information Assurance (MELANI) was informed early on about this vulnerability. It forwarded the information to the companies in Switzerland responsible for operating these terminals. The companies in turn were able to take appropriate countermeasures.

[25] http://www.all-about-security.de/security-artikel/applikations-host-sicherheit/applikationen-web-services/artikel/14953-ddos-angriffe-bleiben-groesste-gefahr-fuer-netzwerke/ (as at 28 February 2013).

[26] http://securityblog.switch.ch/2012/12/04/ddos-angriffe-durch-reflektierende-dns-amplifikation-vermeiden/ (as at 28 February 2013).

[27] MELANI Semi-annual report 2011/1, Chapter 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=en (as at 28 February 2013).

[28] http://www.golem.de/news/verifone-ec-kartenterminals-in-deutschland-gehackt-1207-93144.html (Stand: 28. Februar 2013).

4.4 Attacks against EU institutions

According to US news agency Bloomberg, a group of Chinese spies is alleged to have hacked into the IT system of the European Council. This group, referred to as "Byzantine Candor", is alleged to have intercepted e-mails of Herman Van Rompuy and other high EU officials. The Bloomberg article also states that the hackers are connected with the Chinese People's Liberation Army and that all of this had been uncovered only thanks to a US group of university professors, entrepreneurs, and ICT security experts. Apart from the European Council, at least 20 companies had become victims of the hackers. All of these victims had in common that they had technology China could use to gain economic competitive advantages. The EU has not commented on these attacks.

According to Bloomberg, Byzantine Candor is only one of many examples that should be considered a veritable Chinese cyber espionage industry.

Reports on similar incidents have been increasingly common over the past two years (see especially MELANI reports 2011/1 and 2011/2)[29]. The alleged espionage activities of "Byzantine Candor" and their possible connections to the Chinese army were already discussed by several media outlets in December 2010, after Wikileaks published a secret US dispatch from 2008 in this regard. The dispatch described how espionage activities from China had multiplied in recent years. In February 2013, US security firm Mandiant published a report attributing numerous espionage activities in recent years, mainly against US companies, to the Chinese army unit 61398.[30] The Chinese authorities categorically deny the existence of this kind of state-sponsored cyber espionage.

4.5 Opening of the CERT of the European Union and the European Cybercrime Centre (EC3)

The *CERT* (Computer Emergency Response Team) of the European Union began its work on 11 September 2012 after a one-year pilot phase followed by an evaluation. Its core responsibility is to protect EU institutions from cyber attacks. CERT-EU is made up of ICT and security experts from the most important EU institutions. Its mandate also includes cooperating with the CERTs of the EU member states and various security firms. The EU Commission has been a victim of several cyber attacks in recent years[31] [32], illustrating the need for such an institution.

[29] See MELANI Semi-annual report 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=en (as at 28 February 2013).
See MELANI Semi-annual report 2011/2: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en (as at 28 February 2013).

[30] This topic will be discussed in detail in the next MELANI Semi-annual report 2013/1.

[31] See MELANI Semi-annual report 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 28 February 2013).

[32] See MELANI Semi-annual report 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=en (as at 28 February 2013).

The European Cybercrime Centre (EC3) opened in the premises of Europol in The Hague on 11 January 2013. EC3 is conceived as a contact office at the EU level for combating cybercrime. According to EU Commissioner for Home Affairs Cecilia Malmström, EC3 offers the EU far more options for combating cybercrime and serves to protect a free, open and secure Internet. MELANI report 2012/1[33] contains a detailed description of the centre and its competences.

4.6 Open sesame: Electronic door locks in hotels

In July 2012, a 24-year-old hacker at the Black Hat conference in Las Vegas demonstrated to those present how certain electronic door locks in hotels can easily be unlocked. The method involves using the programming connector, which apparently is located unsecured in the hotel lock, to find the security keys that are stored uncoded in the door lock's control chip. According to media reports, this vulnerability can apparently be found mainly in the code locks manufactured by Onity.

Based on this example, another hacker proposed an especially effective implementation of this method to the audience. On his blog, he explained all the details for manufacturing a device that can be used to break into a hotel room "protected" by an electronic system. The device has the size and shape of a pen and accordingly can be easily transported inconspicuously.

The door locks can only be updated by changing the *circuit boards*. The costs are not covered by the manufacturer, however, and must be paid by the hotels themselves. As an alternative, the manufacturer offers a free option using a cap claimed to prevent access to the programming connector. More than 4 million door locks are said to be affected worldwide.[34]

Apparently, this vulnerability has been known for quite some time. Since the discoverer feared that authorities and intelligence services were now also aware of the vulnerability, he decided to make it public.

For several years already, not only computers and servers have been targeted by cyber attacks. Any IT system can be attacked by hackers. Breaking into an electronically secured hotel door is only one of many examples illustrating this fact. When designing products protected by an electronic identification procedure, this risk must be systematically taken into account.

Access to a hotel room can give unauthorised persons access to confidential data. It doesn't matter if this data is contained on a laptop, a *USB* stick or paper. The case described above illustrates an entirely different aspect of the problem and shows that it is imperative for companies to define how employees must handle sensitive data on business trips. This includes raising the awareness of employees and taking appropriate precautions (e.g. encrypted storage of information on data carriers) before the trip begins.

[33] See MELANI Semi-annual report 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 28 February 2013).

[34] http://www.t-online.de/computer/sicherheit/id_58856082/hacker-knacken-hotel-tueren-binnen-sekunden.html (as at 28 February 2013).

4.7 Devices connected to the mobile network – large variety and minimal security awareness

Security experts are increasingly also focusing on the mobile network. In July 2012, a German researcher provided evidence for the potential security gaps of the network and the devices connected to it.[35] With the help of a *RIPE*-based query, the researcher first looked for *IP addresses* assigned by operators to devices connected with the mobile network. He was then able to use a simple port scanner to compile a wide range of information. A first insight from these experiments is that there is a huge variety of devices on the mobile network: *GSM/GPRS routers*, cameras, *smart meters* (energy consumption meters), *barcode scanners*, traffic guidance systems, etc. The German researcher was even able to obtain localisation information for devices several times without having to identify himself first. He did not attempt to log into the devices and control them remotely.

The goal of the demonstration was to draw attention to potential consequences of the large number of devices on the mobile network and to illustrate how easily they can be identified. This can tempt people with dishonest intentions to search for vulnerabilities in order to gain control of the devices. These persons could then access devices used in private, public, or even industrial domains.

More and more frequently, even critical devices are being connected via GSM/GPRS to reduce costs, including *SCADA* systems, credit card terminals, or cash dispensers.

4.8 App Stores

The leading smartphone content providers worldwide have created virtual shops for their own client to buy a wide range of applications (apps). The question of course arises what the advantages and disadvantages of these platforms are in terms of security.

App Store iOS

The App Store iOS is the platform launched by Apple in 2008. To access the Apple market, i.e. to offer apps in the store, a manufacturer must necessarily undergo Apple's internal review processes.[36] Apps are permitted in the Apple shop only after that analysis has been performed. The purpose of this process is in particular to review the functioning of the application. If the criteria established by Apple are not met, the app is not published. Many of these criteria concern the security of the end-user's device. For instance, an application is not published if it installs and executes additional program code, has access to protected data, or forwards such data to third parties without prior consent.

In the case of the App Store iOS, end-users fully entrust their security to Apple. But how effective is this solution? Malicious applications appear only rarely in the Apple system. In some rare cases, the review processes were circumvented. The most notorious case is probably that of Charlie Miller, a researcher whose application was reviewed and accepted by Apple. It violated the basic rule that no additional code should be downloaded and executed[37]. After Miller's become public, Apple withdrew his developer's licence. Recently,

[35] http://www.heise.de/security/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html (as at 28 February 2013).

[36] https://developer.apple.com/appstore/guidelines.html (as at 28 February 2013).

[37] http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (as at 28 February 2013).

Mike Lee, a former Apple employee, talked about Apple's review structure in an interview[38]. Lee believes the team employed by Apple to analyse the applications is understaffed. Moreover, testing so many apps is a monotonous and uninteresting task for many reviewers. This is true of the (often pornographic) content and of the fact that many apps are copies or updates of already existing apps. The monotonous work can lead to careless errors, as was the case for the app "Find and Call" (Trojan:iOS/Fidall). This app was able to steal contact lists and forward them to a server.

Play Store (Android)

As already mentioned in a previous semi-annual report[39], Google pursues a different policy in terms of applications. In this case, security is mainly delegated to the end-user. In return, this policy allows users to download Android applications from any website. They do not necessarily have to use the official Google shop, Play Store. Nevertheless, Google's goal is to offer its clients secure applications when they visit the Google platform. At the beginning of 2012, Google therefore introduced the "Bouncer" system. This system automatically analyses all applications of the Play Store and searches them for malicious code. In July, however, two researchers – the Charlie Miller already mentioned above and Jon Oberheide – showed that it is possible to trick "Bouncer" and infect an Android smartphone using a prepared app[40].

Google is trying to balance security and flexibility: On the one hand, it wants to offer Android users a service that is as open and flexible as possible, which of course attracts criminals. On the other hand, Google also wants to offer end-users the greatest possible security.

Amazon Appstore (Android):

In the first half of 2011, Amazon launched its own Android Appstore. Additionally, Amazon began to market its own tablet for this purpose at the end of 2011. This newest-generation tablet runs the modified Android 4.0 system, "Ice Cream Sandwich", which has access exclusively to Amazon's virtual shop. After the launch of the Appstore, experts expressed some security concerns. The main criticism was that Android users accessing the store without an Amazon tablet must select the option "Allow Installation of Applications from Unknown Sources" in order to even use the Amazon Appstore. This relaxes the download restrictions, creating the possibility for potentially malicious apps of any kind to be downloaded from untrustworthy websites. According to the F-Secure report for the second quarter of 2012[41], most malicious applications for Android were discovered on "parallel markets" to Google Play Store. In the same quarter, F-Secure discovered the first drive-by download for Android. Another surprise is the report by security firm TrustGo, which after an analysis of 2.2 million apps in a total of 187 markets concludes[42] that Play Store and Amazon Appstore are ranked only fourth and fifth in terms of security. The five "most dangerous" virtual Android shops, according to this report, are all in China.

In closed systems such as Apple's, the security of the end-user is in the hands of the manufacturer. The advantage is that the complex security tasks have been entrusted to a company that should have the requisite possibilities and knowledge. As already mentioned, malicious applications are very rare in Apple's system. The disadvantage is that clients of the

[38] http://www.businessinsider.com/heres-why-it-really-sucks-to-be-an-app-reviewer-for-apple-2012-7#ixzz1zaB9ki4H (as at 28 February 2013).

[39] MELANI Semi-annual report 2011/2, Chapter 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en (as at 28 February 2013).

[40] http://jon.oberheide.org/files/summercon12-bouncer.pdf (as at 28 February 2013).

[41] http://www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf (as at 28 February 2013).

[42] http://www.trustgo.com/images/en-GB/trustgo_q4_mobile_mayhem.pdf (as at 28 February 2013).

App Store must trust Apple completely, and that they cannot control the actual occurrences in their own system.

On the other hand, the security system of the Play Store has already been attacked successfully, and as mentioned above, Amazon requires its own users to change their security settings so that applications from outside the original market can be downloaded. Criminals place their malicious apps on the various Android markets or websites and hide them as legitimate applications. There are thousands of malicious programs circulating on the various markets. Even if the Android user has the necessary information to assess the rights needed for the applications, this possibility is used only rarely. For the common user who wants to install an app as easily and quickly as possible, the security aspect is secondary. This aspect must also be taken into account by the market operator, who after all wants to achieve a high level of security.

4.9 Reporting requirement for hacker attacks and network control – for and against

Some countries such as France, the United States and Germany have announced that they will prepare legal initiatives to introduce a reporting requirement for serious cyber attacks. According to the cyber strategy of the European Union (EU), the European Commission likewise wants a uniform reporting requirement to make the Internet more secure for companies offering public services of national importance. Already since adoption of the EU Telecoms Package, telecommunications providers in the EU are subject to a reporting requirement.

This approach is opposed mainly by private businesses, Internet service providers and industry, since they fear that a report would have a negative impact on their companies and lead to reputation damage. The administrative effort is considered to be very high. It has to be clarified in detail what precisely should be considered an attack or vulnerability. In principle, companies and operators of critical infrastructures prefer cooperation with the authorities to be needs-based and voluntary.

The advantages and disadvantages of reporting requirements and voluntary information exchange are being hotly debated in several countries. On the one hand, the establishment of voluntary data exchange is a process based on trust, which can accordingly take a long time. Immediate successes are rare. But once such a partnership has been established, the information exchanged is generally of a higher quality than under a reporting requirement. On the other hand, a reporting requirement by definition results in information flow from the outset. But such information is governed by a narrow legal framework that leaves authorities and companies little leeway. The danger that information may flow, but not generate a significant benefit, can therefore not be ruled out. Experience also shows that the discussions during preparation of a reporting law take a lot of time, especially regarding what information must be reported at what level of detail and in what form.

No general statement can be made as to which alternative is better. This depends very heavily on the structure and size of the country in question. Since a large country also has more stakeholders and companies, it is certainly a greater challenge to establish a relationship of trust. In Switzerland, voluntary information exchange within the framework of a public-private partnership (PPP) has become established over the past few years.

5 Trends/Outlook

5.1 Browser vulnerabilities – two-browser strategy and other options

It has now become standard practice to regularly, and best of all automatically, download security updates of operating systems and applications. Nevertheless, *0-day* vulnerabilities frequently do occur, i.e. vulnerabilities for which no security update exists. Almost every day, vulnerabilities of this sort surface in a wide range of applications. Internet *browsers* are likewise not immune to them. Depending on the seriousness of the known vulnerability, it may make sense to switch to a different browser, at least temporarily, until the vulnerability has been resolved by the manufacturer.

What is trivial for the private domain can lead to serious problems in the business world. Unlike in the case of private computers, it is not always that simple to switch to an alternative browser in the case of business computers – for instance if no two-browser strategy has been implemented. This is often the case, so that the responsible ICT division only has to maintain a single browser.

If a serious vulnerability occurs, private or even confidential data may be at risk. It therefore makes sense, both at home and in the business world, to prepare for an emergency, in order to switch to an alternative browser as quickly as possible.

The following possibilities are conceivable in the business world. The list is not exhaustive:

Comprehensive installation of two browsers on all workstations
All workstations in a given company are supplied with at least two browsers. In an emergency, the employees can be instructed to no longer use the affected browser until informed otherwise. This may also be steered using the *proxy* by denying Internet access to the affected browser. This solution is relatively cost-intensive, however, since several browsers have to be maintained and it is not always clear for the user which browser can be used when.

Selective installation of at least two browsers
Workstations that absolutely have to access the Internet are supplied with several browsers. If one of the browsers is affected by a vulnerability, Internet access can be denied. Access to the Internet is then only possible with an alternative browser. This solution has the serious disadvantage that, in the event of an emergency, part of the staff temporarily has no access to the Internet. Even though this may not have a major impact on work, the affected users may feel patronised or disadvantaged.

White list
All divisions of a company notify their ICT division of those *URLs* that must be accessible even in the event of an emergency. These URLs are then entered on a "white list". If a vulnerability occurs, all URLs are blocked that are not included on the white list. With this measure, alternative browsers can be dispensed with. The risk of damage is minimised, since only specific URLs are reachable. Nevertheless, a certain risk persists. It must be possible to install security updates quickly, so that the temporary blocking of URLs not on the white list can be lifted as soon as possible.

Whichever option is chosen for private and business ICT: it is an illusion to believe that alternative browsers are more secure. Sooner or later, vulnerabilities occur with every browser. Just because no known vulnerability exists in a certain browser, that does not mean that the browser is 100% secure. Users should therefore always use the Internet with the necessary care and common sense.

5.2 Overview of cyber strategies

So far, more than 20 countries have published extensive cyber security strategies. Most countries consider threats from cyberspace to be one of the greatest challenges of the 21st century and, as a consequence of increasing cyber incidents (e.g. Stuxnet, Duqu, Flame, and Ghostnet), are integrating cyber security into their national security policy strategies (e.g. France, the Netherlands and the UK).

In all cyber strategies, the use of information and communication technologies (ICT) is defined as a driver of economic progress and social prosperity. At the same time, increasing the robustness of critical infrastructures and minimising cyber risks are described as national priorities.

Cyber as a horizontal task
Coordination of official activities at a political-strategic as well as technical-operational level is seen as key. This is because overcoming cyber risks is understood as a horizontal task, and different authorities and stakeholders must now also cover cyber aspects as part of their core mandate. To ensure this, some countries have established cyber defence centres (e.g. Germany and the Netherlands).

Public-private partnership
Since the bulk of public infrastructure services are in private hands, cooperation between the public and private sector is essential. In most strategies, the need is recognised to intensify and institutionalise this cooperation. Many cyber strategies are based on the consideration that cyberspace should not be made more secure using regulations and state intervention in the market, but rather on a voluntary basis through stronger cooperation (e.g. Switzerland, the UK and the Netherlands).

International cooperation
Effective minimisation of cyber risks also requires stronger international cooperation. This realisation is reflected in all cyber strategies. However, only few countries describe in detail how cooperation at the international level can and should be improved and institutionalised. One exception is the United States, whose cyber strategy is expressly international. With the London Conference on Cyberspace initiated in 2011, the UK is also promoting an international dialogue to define international codes of conduct for cyberspace. International organisations (such as the European Union, the G8, the United Nations and the Organization for Security and Co-operation in Europe) also play an important role in the development of codes of conduct. Both Germany and Australia are advocating a joint early-warning system and the establishment of contact points for communication in a crisis.

With the adoption of the National strategy for Switzerland's protection against cyber risks, Switzerland is increasingly emphasising cooperation between public and private stakeholders in dealing with cyber risks. The public-private partnership (PPP) approach is not new for Switzerland, given that state authorities have been supporting the information assurance process for critical infrastructures on a subsidiary basis since the privatisation of various public services, such as the telecommunications sector. The Reporting and Analysis Centre for Information Assurance (MELANI), which was established in 2004, informs the operators of critical infrastructures of incidents and threats in cyberspace, thus making a contribution to corporate risk management. MELANI's structure is also comparable to the cyber defence centres established in other countries. Compared with some of the efforts in this direction taken by other countries, the cooperation and mandate of MELANI go even further.

This cooperation between public authorities and the private sector has proven itself and functions smoothly. With the National strategy for Switzerland's protection against cyber risks, the existing decentralised structures are strengthened. Compared with other countries, Switzerland is doing without the establishment of a central steering and coordination body.

5.3 Regulation versus freedom – how to make the Internet secure?

The Internet, which started as an American military research project under the Advanced Research Projects Agency (*ARPA*), has established itself as an information and service platform, evolving from a purely scientific network into a commercially used infrastructure of superlatives. This rapid development can be seen in the number of Internet users: while only about 500,000 people used the Internet in 1991, the number is now about 2.5 billion. It is estimated that by 2020, up to 5 billion people – approximately 60% of the world’s population – will have an Internet connection.

To this day, the Internet is not regulated by the state and is largely governed as a free space via technical standards and administrative guidelines (referred to as policies). The non-governmental bodies Internet Corporation for Assigned Names und Numbers (ICANN) and the Internet Society (ISOC) further develop these technical and administrative policies and facilitate the cooperation of governments, the private sector, academia and civil society in administering the Internet. Western governments support this multistakeholder governance model and believe it is useful in ensuring freedom of information.

On the other hand, there is a strong coalition of countries advocating Internet regulation in order to extend their state control to cyberspace and to strengthen or to ensure their sovereignty.

The World Conference of the International Telecommunication Union (ITU) – a specialised agency of the United Nations – held in Dubai at the end of 2012 envisaged expanding the International Telecommunication Regulations (ITRs), which apply to cooperation in voice telecommunications, to the Internet. The fact that 55 of 144 states did not sign this expansion, even though Internet administration is not covered specifically but at most by way of interpretation, illustrates the disunity of the international community regarding the distribution of powers with regard to Internet administration.

The influence of global companies such as providers of software, search engines and social websites, but also the music and film industry, should not be underestimated. These companies have a great interest in a development of the Internet that supports their areas of business. These companies lobby against regulations that cost money or diminish their market opportunities, but on the other hand they also lobby in favour of regulations that are lacking.

5.4 Traces on the Internet – what data users divulge when visiting a website

Information is the new currency on the Internet. This phrase is heard increasingly often with regard to the gathering of information on the Internet. Steadily improved programs and increasingly large computing power make it possible to provide constantly improving qualitative analysis of large data volumes, which can accordingly also be commercialised better. In such cases, individuals disappear in the flood of data, but many people using electronic devices on a daily basis still ask themselves what data is being collected about them and for what purpose that data is processed and stored.

Many online providers are especially interested in user behaviour in order to display advertisements that are as specific as possible and to measure their success. The best-known example here is certainly Google, which employs users' search queries to "personalise" the displayed advertisements. Companies displaying ads earn money when a user clicks on a link. So it is financially worthwhile for them to target and tailor the ads to the user. Banner ads are generally not displayed on the webpage itself, but rather are displayed as a page within the page (i.e. as an *IFrame*). At the same time, the IFrame of the advertising company includes small scripts that collect data such as the IP address, *domain*, *browser*, local time and operating system.[43] The more pages that contain banner ads and hence also information collectors, the more precise the user profiles can be made. However, the user must of course be recognised on the different sites. To ensure this, *cookies* are used. Cookies are in principle not a bad thing, but rather are used to assign personal settings to the user so that the setting does not have to be reconfigured each time the user visits the site or different pages of a site. But ad companies quickly discovered this technique for themselves and incorporated it into their banner ads.

In a study published in the Wall Street Journal in August 2010, 50 of the most popular sites were visited. Afterwards, the test computer had stored 3,180 tracking cookies, most of which were from advertising companies. The information from the cookies is refined with other information, such as the place of residence, in order to establish a profile of the user that is as precise as possible.[44]

Other than the IP address, this information is still more or less anonymous. But this changes when companies are able to compare the user profiles with personal data. In this context the Facebook Like button is often brought up. Analogously to web banners, the Facebook buttons found on various sites can be used to establish a user profile. Even before the user has clicked on the Facebook button, data is transmitted to Facebook.[45] If the user is logged into Facebook at the same time, Facebook would be able to attribute the page directly to the person. Also cookies with a long validity of up to 2 years are used so that this attribution can be made even after the visit.

In addition to the data supplied in the background, there is also the data entered on purpose such as on Facebook, Xing or other social media platforms. All users should of course be conscious of what kind of data they want to enter and what not. There is a risk, however, that the data entered in the background is associated with the data entered on purpose.

New technologies invariably also give rise to new desires. Since surfing the web is moving more and more from "normal" computers to smartphones, advertisements are also increasingly displayed location-specifically. Accordingly, *GPS* data will in future play an ever greater role. A first step is the announcement by the mobile provider Telefonica that it will use location data commercially. At the beginning of October 2012, Telefonica established its

[43] http://de.wikipedia.org/wiki/DoubleClick (as at 28 February 2013).

[44] http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html (as at 28 February 2013)

[45] http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html (as at 28 February 2013).

"Telefonica Dynamic Insight" division. This company is responsible for the preparation and analysis of information – including location data from telecom providers – which can then also be used commercially. With the help of this data, it would for instance be possible to predict the flow of people depending on the weather, the day of the week and the time of day. Such information could then be used by businesses to make personnel available and purchase goods or by local authorities to control flows of people.

Smartphone *apps* will become increasingly important. Precisely in this area, however, there is still a low level of transparency regarding which data is transmitted to the manufacturer. New technologies such as face recognition will also awaken interest in the advertising sector. The challenge for every individual of deciding what personal data may be processed or even passed on to third parties and what not (self-determination over personal information) is unlikely to become easier in future.

Most people now know that they should tread carefully with personal data on the Internet. However, a lot of other data about surfing behaviour is collected in the background, usually with the purpose of displaying suitable advertisements, i.e. to earn as much money as possible.

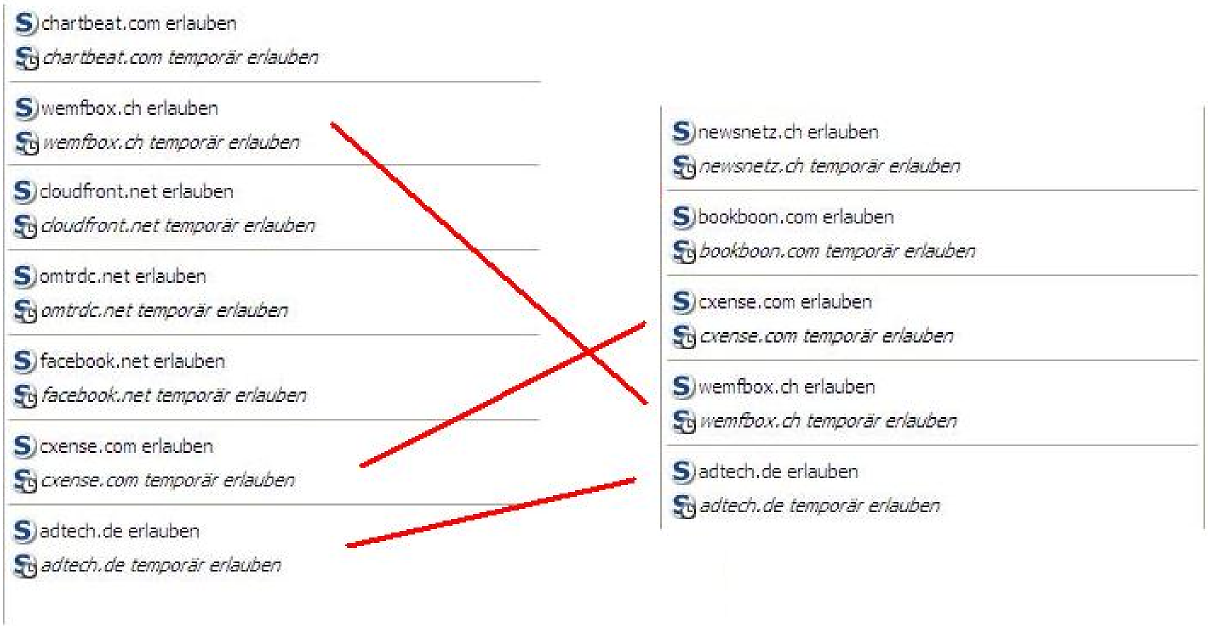
To prevent companies from receiving information about one's surfing behaviour, browser manufacturers make appropriate settings available. A first restriction is achieved by blocking cookies from third parties and advertisers. This setting can be adjusted along with other privacy settings in every browser. Firefox and Internet Explorer (the exact version numbers can be seen here[46]) also offer the "do not track" option, which can additionally be activated and which tells a website by way of an "*opt-out*" that no surfing profile should be compiled. The Firefox add-on "Ghostery"[47] should also be mentioned, which uses a blacklist to prevent tracking attempts as far as possible. However, this and other methods do not offer 100% assurance that no data will be collected or associated with other data.

5.5 Third-company data on business websites – a security problem?

Advertising is displayed on many websites. Only in rare cases are these ads generated by the company itself, however, but rather they are produced and managed by a third company (see also Chapter 5.4). Other than advertising, there is of course other content generated not by the companies themselves, but by external suppliers. This may include statistical services or a service displaying news or stock market quotes. In these cases, not only an image is displayed, but generally a fully functioning page within a page (*IFrame*) with all the same rights as the main page. Especially news portals use this function, since they depend on being able to display news from different sites.

[46] http://ie.microsoft.com/testdrive/browser/donottrack/default.html (as at 28 February 2013).

[47] http://www.ghostery.com/ (as at 28 February 2013).



chartbeat.com erlauben
chartbeat.com temporär erlauben
wemfbox.ch erlauben
wemfbox.ch temporär erlauben
cloudfront.net erlauben
cloudfront.net temporär erlauben
omtrdc.net erlauben
omtrdc.net temporär erlauben
facebook.net erlauben
facebook.net temporär erlauben
cxense.com erlauben
cxense.com temporär erlauben
adtech.de erlauben
adtech.de temporär erlauben

newsnetz.ch erlauben
newsnetz.ch temporär erlauben
bookboon.com erlauben
bookboon.com temporär erlauben
cxense.com erlauben
cxense.com temporär erlauben
wemfbox.ch erlauben
wemfbox.ch temporär erlauben
adtech.de erlauben
adtech.de temporär erlauben

Figure 7: URLs of third companies publishing content and using JavaScript on the websites of two Swiss newspapers. For this figure, the program NoScript was used, which blocks and indicates third-party sites using JavaScript.

Figure 7 shows various third-party content displayed on the websites of two Swiss daily newspapers. Both sites receive advertising content from third companies. In some cases, the same companies and servers are responsible for delivering the data. These servers accordingly play an important role. Compromising such a server can have far-reaching consequences and in the worst case infect a considerable share of the computers of the Swiss population. In the last years, there have been several smaller incidents of this type. In mid-May 2012, for instance, a banner ad on wetter.com distributed *malware*[48]. Swiss companies too have already been affected by such incidents and unknowingly distributed *malware* on their websites via third-party banner ads.

Apart from all the advantages and cost savings made possible by the centralisation of web content, every company should also be aware of the associated risks. In addition to the threat of *malware* infections on website visitors' computers, an incident may also lead to a loss of trust in the company.

It is imperative to define already in advance how to respond in the event of compromised content of third-party suppliers. Does the company have access to the third-party content, and can it influence and suppress it in emergencies? Most importantly, the contacts with the ICT security divisions of the third companies should be clarified in advance, so that the right people can be contacted quickly in an emergency and appropriate countermeasures can be introduced.

5.6 Trust in the supply chain

At the end of April 2012, it became known that Sunrise would outsource the operation and maintenance of its mobile and landline network to Huawei for the next five years. Since 1 September 2012, Huawei has consequently taken over all operational responsibility from

[48] MELANI Semi-annual report 2012/1, Chapter 4.9: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 28 February 2013).

Sunrise. At the beginning of February 2013, Swisscom also entered into a partnership with the Chinese provider. The eight-year contract covers fibre optic expansion until just before the building (fibre to the street, FTTS). In this connection, the question arises whether the penetration of foreign companies into national telecommunications markets could endanger national security – especially as regards access to sensitive information or even possible sabotage of the information infrastructure.

Although there is no knowledge of such incidents so far, naturally it can never be ruled out entirely that the involvement of foreign telecommunications providers in the establishment or operation of Swiss telecommunications networks might be exploited by foreign intelligence services. However, telecommunications companies with worldwide contracts have no interest in deliberately exposing themselves to such schemes. If such a case were to become known, it might result not only in a loss of trust and damage to reputation, but also penalties such as prohibition of access to certain markets.

Possible influence by some state can never be ruled out entirely, especially as the external political environment can change at any time. Since many such devices have *firmware*, it is also possible to place *malware* even at a later date. Trust in a manufacturer can be contrasted with the option of control, but this entails expensive and time-consuming *source code* analysis and security tests for every product and every firmware update. The right solution is probably somewhere in the middle. Risk and vulnerability analysis are among the basic elements of any corporate strategy. Companies should thus focus less on the country of origin of the manufacturer, but rather on the possibilities of including further security measures downstream, irrespective of the device used.

6 Glossary

Advanced Research Projects Agency Network (ARPANET)	ARPANET was originally commissioned by the US Air Force and developed by a small research group headed by the Massachusetts Institute of Technology and the US Department of Defense. It is the predecessor of today's Internet.
App	"App" (an abbreviation of "application") generally refers to any type of application programme. In common parlance, the term now generally refers to applications for modern smartphones and tablet computers.
Authoritative DNS server	An authoritative name server is responsible for a zone. Its information about this zone is therefore considered authoritative.
Barcode scanner	A barcode scanner or reader is a data gathering device that can read and transmit different barcodes. The barcodes are recognised either purely optically or with red or infrared light.
BitTorrent	BitTorrent is a collaborative file sharing protocol that is especially suited to the fast distribution of large data volumes.
Browser	Computer programmes mainly used to display Web content. The best-known browsers are Internet Explorer, Netscape, Opera, Firefox und Safari.
Buffer overflow	Buffer overflows are one of the most common vulnerabilities in current software, which can also be exploited via the Internet.
Circuit board	A circuit board is a carrier of electronic components. It serves to mechanically attach and electronically connect components. Nearly every electronic device has one or more circuit boards.
Command & Control Server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called command & control server.
Computer Emergency Response Team (CERT)	Computer Emergency Response Team CERT (also CSIRT for Computer Security Incident Response Team) refers to a team that coordinates and takes measures relating to incidents in IT significant to safety.
Cookie	Small text files stored by a web page when viewed on the user’s computer. For example, with the assistance of cookies, user preferences for a web site may be stored. However, cookies can also be abused to compile an extended user profile about one's surfing habits.
Defacement	Unauthorized alteration of websites.

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 resolver	DNS resolvers are simply constructed software modules installed on the computer of a DNS participant that can access the information of name servers. They form the interface between the application and the name server.
Domain	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.
DoS attacks	Denial of service attacks. Have the goal of causing a loss of a specific service to users or at least to considerably restrict the accessibility of the service.
Drive by infection	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
Firewall	A firewall protects computer systems by monitoring incoming and outgoing connections and rejecting them if necessary. A personal firewall (also called a desktop firewall), on the other hand, is designed to protect a stand-alone computer and is installed directly on it.
Firmware	Instructions stored in a chip to control a device (e.g. a scanner, graphics card, etc.). Firmware, as a rule, may be modified by upgrades.
General Packet Radio Service (GPRS)	General Packet Radio Service is a packet-oriented service for data transmission that is used in GSM (mobile communication) networks.
Global Positioning System (GPS)	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
Global System for Mobile Communications (GSM)	The Global System for Mobile Communications (previously Groupe Spécial Mobile, GSM) is a standard for fully digital mobile networks, mainly used for telephony, but also circuit-switched and packet-switched data transmission and short messages.

Hypertext Transfer Protocol Secure (https)	Hypertext Transfer Protocol Secure (HTTPS) is a communication protocol on the World Wide Web to make data tap-proof.
IFrame	An IFrame (also inline frame) is an HTML element used to structure websites. It is used to integrate external web contents into one's own website.
IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
Malicious Code	Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses. See also Malware.
Master boot record (MBR)	The master boot record is the first data block (512 bytes) of a storage medium. The MBR contains information describing the structure of the data carrier and optionally a programme that launches an operating system in one of the partitions.
Network stack	In data transmission, the network stack is a conceptual architecture of communication protocols.
Opt-out	Opt-out is a marketing procedure providing automatic inclusion in a distribution list, where the client has the opportunity only after the first distribution to request removal from the list.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with false sender addresses.
Phreaking	Phreaking is the term for “manipulation of telephone equipment”.
PIN	A personal identification number (PIN) is a number for authenticating oneself to a machine.
Point of sale (POS)	A POS terminal (in Switzerland: EFT/POS terminal) is an online terminal for cashless payments at points of sale.
Proxy	A proxy is a communication interface in a network. It works as a mediator, receiving queries on the one side and making a connection on the other side via its own address.
Public IP address	IP address that is reachable directly and from every point on the Internet.
Réseaux IP Européens (RIPE)	The Réseaux IP Européens Network Coordination Centre (RIPE NCC) is a regional Internet registry responsible for assigning IP address ranges and AS

	numbers in Europe, the Middle East and Central Asia.
Router	Computer network, telecommunication, or also Internet devices used to link or separate several networks. Routers are used, for instance, in home networks, establishing the connection between the internal network and the Internet.
RSA encryption	Short for Rivest-Shamir-Adleman encryption. A public-key encryption algorithm introduced in 1978. RSA is an asymmetric algorithm.
SCADA systems	Supervisory Control And Data Acquisition Systeme. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
Skimming	"Skimming" refers to a man-in-the-middle attack that illegally spies out credit card or banking card data. Skimming is used to obtain card data by reading data off magnet stripes and copying them to counterfeit cards.
Smart Meter	A smart meter is an energy meter that displays the actual energy use and actual usage period to an energy consumer; the information can also be transmitted to the energy supplier.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
Short Message Service Service (SMS)	Short Message Service Service to send text messages (160 characters maximum) to mobile phone users.
Source code	In computer science, "source code" refers to the text of a computer program written in a programming language that is readable for humans.
Spoofing	In information technology, "spoofing" refers to various deception attempts in computer networks to conceal one's own identity.
Top Level Domains	Every name of a domain on the Internet consists of a sequence of character strings separated by periods. The term "top level domain" refers to the last name in this sequence, constituting the highest level of the name resolution. If the full domain name of a computer or website is de.example.com, for instance, the right-most member of the sequence (com) is the top level domain of this name.
Transaction signing	Additional security element in e-banking. When a client makes a payment order, a code is sent to the client's cell phone by SMS, for instance. Only after entering the code in the e-banking system does the bank execute the payment.
Transmission Control Protocol /	Transmission Control Protocol / Internet Protocol

Internet Protocol (TCP/IP)	(TCP/IP) is a family of network protocols, also referred to as the Internet protocol family because of its great importance for the Internet.
Uniform Resource Locator (URL)	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).
Universal Serial Bus (USB)	Serial bus (with a corresponding interface) which enables peripheral devices such as a keyboard, a mouse, an external data carrier, a printer, etc. to be connected. The computer does not have to be switched off when a USB device is unplugged or plugged in. New devices are for the most part automatically identified and configured (depending on the operating system).
Voice phishing	Voice phishing is a form of Internet scam, derived from the word "fishing" and the method of VoIP telephony used.
Voice over IP (VoIP)	Telephony via internet protocol (IP). Frequently used protocols: H.323 and SIP.
Zero day exploit	An exploit which appears on the same day as the security holes are made public.