MELANI Reporting and Analysis Centre for Information Assurance

INFORMATION ASSURANCE

THE SITUATION IN SWITZERLAND AND INTERNATIONALLY

SEMI-ANNUAL REPORT 2005 / II

In collaboration with:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Issue 2/2005 (July to December 2005)

Table of contents

1 Introduction ... 5

2 Current situation, threats, and risks ... 6

2.1 Industrial espionage ... 6

2.2 Phishing and pharming ... 6

2.3 Botnets ... 7

2.4 Current attack vectors and malware developments ... 7

2.5 VoIP security ... 7

2.6 Rootkits ... 8

2.7 Mac OS X: Increase of security threat? ... 8

3 Trends / General developments ... 9

3.1 Individualized Trojan horses, social engineering, spear phishing: Greatest threat of industrial espionage ... 9

3.2 Botnets: Greatest threat of cybercrime ... 9

3.3 Professionalization of the attackers: Division of labour, massive increase of malware production, new attack vectors ... 10

3.4 Phishing: Increasing threat also in 2006 ... 10

3.5 Threat to mobile devices (mobile phone, PDA) ... 11

4 Current national ICT infrastructure situation ... 12

4.1 Breakdowns, failures ... 12
ADSL interruptions ... 12

4.2 Attacks ... 12
Defacements: Reaction times to athletic or political events are becoming increasingly short ... 12
Lotterie Romande: Yet another case of fraud ... 12

4.3 Crime ... 13
Phishing websites in Switzerland ... 13
Economic crime on the internet is increasing dramatically ... 13
CYCO Report 2005: Number of reported incidents has increased significantly ... 13

4.4 Terrorism ... 14
The central computer of the University of Geneva as a centre for Islamist propaganda ... 14
Al-Zawahiri video published in forum ... 14

4.5 Miscellaneous ... 15
Spam smear campaign against Schengen/Dublin ... 15
Threat from the inside also in Switzerland ... 15
E-voting: Inaugural run in Switzerland ... 15

5 Current international ICT infrastructure situation ... 16

5.1 Breakdowns, failures ... 16
Computer breakdown at the Tokyo Stock Exchange resulted in losses ... 16

5.2 Attacks ... 16
Titan Rain: Targeted espionage attacks against the US, the UK, Canada and other countries, presumably from China ... 16
Worm war between Zotob, Bozori and IRCbot for the creation of a botnet – arrests provide insight into the hacker scene ... 17
Sober worm: Class reunions, deceptive FBI / BKA e-mails, and right-wing spam ... 18
Critical holes in Windows systems rapidly exploited: WMF 0-day exploit ... 19

IM threats: Worms with rootkit capacities and language abilities 19

5.3 Crime 20
Phishing: Widespread 20
Arrest of botnet owners in the Netherlands and the United States: Insights into the botnet scene 20

5.4 Terrorism 21
What terrorists use ICT technologies for:
"Virtual Afghanistan": Training/propaganda for jihadists now conducted online 21
What terrorists do not use ICT technologies for: Debate on the threat of cyberterrorism 22
Germany: New federal government continues red-green anti-terrorism strategy 23

6 Prevention 24

6.1 Software 24
Microsoft invests in security 24
Effective protection for the PC 24
Using instant messaging securely 24
Developments relating to Sender ID / Domainkeys 25

6.2 Hardware 25
New developments relating to wireless networks 25
Network Admission Control 26
New Bluetooth threats 26

6.3 Miscellaneous 26
New developments relating to anti-phishing tools 26
Fight against bot networks 27
Insider threats 28

7 Activities / Information 29

7.1 State 29
Switzerland: Tender of licenses for broadband wireless access 29
EU: Parliament decides on storage of telecommunications connection data 29
EU: Commission launches Green Paper on Critical Infrastructure Protection 29
Germany: National Plan for the Protection of Information Infrastructure presented
by Interior Minister and BSI / Report on the Situation of IT Security published 30
New anti-terror laws in some EU States / Anti-terror strategy of the EU 30
United States: Tighter organization of cybersecurity efforts and renewed criticism 31

7.2 Private sector 32
ICT manufacturers: Anti-Spyware Coalition defines spyware and adware 32

8 Legal foundations 33
Federal Council prevents revision of online consumer protection legislation 33
Legal foundations for Voice over IP (VoIP) 33

9 Statistics 34
Switzerland: Fewer investments in IT security 34
Switzerland: Economic effect of an internet blackout 34

10 Miscellaneous 35
Sony employs rootkits to preserve digital rights and creates security problems 35

11. Glossary 36

Focus areas of issue 2005/II

- *Targeted industrial espionage with individual Trojan horses and social engineering*
  Targeted industrial espionage attacks, especially against →critical national infrastructures, military systems, and increasingly also against the private sector rose in the second half of 2005. With targeted →Trojan horses developed exclusively for the attack in question that are therefore unknown to anti-virus software manufacturers, and employing clever →social engineering methods, information of economic or strategic value is systematically stolen. Enterprises should consider this threat serious.
  ► Current situation: Chapter 2.1
  ► Trends for the next half-year: Chapter 3.1
  ► Examples / incidents: Chapter 5.2

- *Botnets: Greatest danger with respect to cybercrime*
  With at times more than 1,000,000 zombie computers under their control, operators of →botnets earn a lot of money through cybercrime: sending spam, illegal installation of →adware, theft of login, credit card, or e-banking data (using →spyware), blackmail through encryption of files or with →DDoS attacks (increasingly also against SMEs) are only the major activities. Computers of home users are affected, but also company, university, and government systems. Botnets are growing, their owners are earning more and more money, and suppressing them is becoming increasingly difficult.
  Botnets are the greatest cybercrime threat.
  ► Current situation: Chapter 2.3
  ► Trends for the next half-year: Chapter 3.2
  ► Examples / incidents: Chapter 5.2 und 5.3

- *Improvement of malware quality: Professionalization of the hacker scene*
  The hacker scene pursuing pecuniary objectives is becoming increasingly professional and is evolving more and more into the shape of organized crime, or is working increasingly with organized crime. This is linked to a massive increase of professionalization, faster development times for →malware, qualitatively better malware (polymorphic malware, hidden with →rootkit functions), and the exploitation of new attack vectors (fewer attacks against operating systems, more attacks against applications such as web applications, virus protection programs, →instant messaging, backup applications, etc.).
  In the next half-year, even more rapid development times and even higher-quality malware are to be expected.
  ► Current situation: Chapters 2.4 and 2.6
  ► Trends for the next half-year: Chapter 3.3
  ► Examples / incidents: Chapters 5.2 and 5.3

- *Phishing and pharming*
  →Phishing and →pharming continued to be current and wide-spread threats in the second half of 2005, increasingly also in non-English-speaking countries. Although countermeasures have been improved, this threat is likely to increase again in 2006, both in its classic form with phishing websites as well as with spy software.
  ► Current situation: Chapter 2.2
  ► Trends for the next half-year: Chapter 3.4
  ► Examples / incidents: Chapters 4.3 and 5.3
  ► Prevention: Chapter 6.3

1 Introduction

The second semi-annual report (July – December 2005) of the Reporting and Analysis Centre for Information Assurance (MELANI) presents the most significant trends involving the risks arising from information and communication technologies (ICT), provides an overview of the events in Switzerland and abroad, illuminates the most important developments in the field of prevention, and summarizes the activities of public and private actors. Explanations of jargon and technical terms (marked with a →) can be found in a **Glossary** at the end of this report.

Chapter **two** describes the current situation, threats, and risks of the last half-year. Chapter **three** provides an outlook on the expected developments.

Chapters **four** and **five** discuss breakdowns and failures, attacks, crime, and terrorism connected with ICT infrastructures. Using selected examples, the most important events of the last six months of 2005 are illustrated. The reader will find illustrative examples and information supplementing the general observations in the strategic-analytic chapters two and three.

Chapter **six** discusses technological developments in the field of prevention and for increasing the security of information and communication technologies.

Chapter **seven** focuses on public and private sector activities relating to information assurance in Switzerland and abroad.

Chapter **eight** summarizes amendments to the legal foundations.

Chapter **nine** provides a summary of important studies and statistics relating to ICT.

In chapter **ten**, Sony's use of rootkits to preserve digital copyright is described, which has led to considerable security problems.

2 Current situation, threats, and risks

2.1 Industrial espionage

Targeted espionage is a focus of this issue. While →viruses and →worms used to be disseminated as widely as possible, an increase of targeted attacks with Trojan horses on a smaller circle of persons has been observed recently. The goal is targeted espionage. Accordingly, 74% of the currently discovered →malware was developed to collect confidential data.[1] Sophisticated →social engineering methods are used to place the spy programs. Malware, infected CDs or e-mails are personalized and sent directly to potential victims. Since, due to their limited dissemination, these smuggled-in Trojan horses are unknown to anti-virus software manufacturers, they are also not automatically recognized by their software. Such targeted attacks are also called →spear phishing. The attacks discovered in the second half of 2005 primarily target government authorities and operators of critical infrastructure. The British National Infrastructure Security Coordination Centre (NISCC) announced in June of this year, for instance, that critical national infrastructure and government offices have already been targeted by attackers since 2003. All large industrial countries were victims of such attacks last year (see chapter 5.2, Titan Rain). In the summer, Canada experienced targeted attacks with individualized Trojan horses, and attacks were reported against Australia and New Zealand. In August, it became known that systematic and professional computer espionage had been perpetrated against military systems of the U.S. government for two years. The attempt to abuse the WMF hole (see chapter 5.2) for espionage purposes among British parliamentarians has failed for now. Chapter 3.1 includes an assessment of the future threat.

2.2 Phishing and pharming

→Phishing and →pharming remain relevant cybercrime topics. In addition to eBay and PayPal login data and credit card numbers, phishing and pharming attacks have primarily obtained login data for e-banking gateways of financial institutions. What began in 2003 in the United States and then reached Australia and the UK has now become a hot topic throughout Europe. On the weekend of 17/18 September, for instance, phishing attacks were observed on customers of over 24 European banks, primarily in Italy and Spain. Since 2005, the frequency of phishing cases has also increased in German-speaking Europe (see chapter 5.3). Switzerland has also not been spared, although it is far less affected than Germany. This is in part due to the high security standard of Swiss financial institutions, but also the smaller size and multilingualism of Switzerland. So far, no German-language phishing e-mail against a Swiss financial institution has been reported (see chapter 4.3). In Germany, for example, phishing is no longer limited to a single financial institution, but rather is employed across a large area and in many different variations. There are still significant differences in the quality of the attacks, however. For instance, URLs are cached through →redirects via Google or MSN or by inserting special characters. Using another method, the original page is loaded in the background, and the counterfeit page is superimposed in a pop-up window. The address and origin of the pop-up window are then invisible. It is very difficult to give an estimate of the damage caused, since many losses are not even known to the authorities. Even if, according to the statistics of the Anti-Phishing Working Group[2], phishing is not receding, some investigation successes have still been achieved, such as the arrest of a phishing gang in Estonia. In addition, the average online time of phishing pages has been reduced from 5.9 days in August to 5.3 days in December 2005. Only good cooperation between the affected countries and the continuous improvement of security features in financial services can curb this phenomenon. Chapter 3.4 provides a preview of the expected development of phishing attacks, while Chapter 6.3 summarizes preventive measures against phishing attacks.

[1] According to Symantec, 74% of the 50 most important reported viruses have spying capability.

[2] The most important resource in the fight against phishing: http://www.antiphishing.org (as of: 15 Feb 2006).

2.3 Botnets

→Botnets are an important tool of cybercrime, used to blackmail (through DDoS attacks or encryption of company data), collect confidential information, plunder bank accounts, collect money for terrorist activities, send spam, and undertake many other illegal activities. Fighting botnets is very difficult, since firstly, the computers of innocent home users and/or company computers are infected, and these users cannot simply be identified and notified without huge efforts. Secondly, botnet operators always discover new means to conceal their botnets.[3] The arrest of botnet owners in the Netherlands and the United States (see chapter 5.3) showed the extent of bot networks and confirmed the assessment in the last semi-annual report. According to official sources, the botnet owners in the Netherlands operated a network of over 1.5 million computers. In California, a 20-year-old botnet owner was arrested who controlled a network with approximately 400,000 computers. To curb such bot networks, the German betting agency jaxx.de set a reward of 40,000 euros for the arrest of →Distributed Denial of Service (DDoS) attack blackmailers, after the company was attacked and requested to pay blackmail. DDoS attacks can be very costly for an attacked company. The costs for the online transaction service Protx (UK), for instance, which had to fight off several DDoS attacks, amounted to about US$ 500,000. Sometimes, DDoS attacks are also launched for purely political reasons, without financial motives: Over the course of the second half of 2005, for instance, several attacks were conducted against German consumer protection websites on the internet. Chapter 3.2 gives a preview of the expected threat development of botnets, while chapter 6.3 describes an attempt by the Australian government to suppress bot networks.

2.4 Current attack vectors and malware developments

In 2005, a further professionalization of malware developers was observed. While the Slammer worm surfacing in January 2003 was still only able to exploit a security hole that Microsoft had already fixed months before, the authors of Zotob, Bozori and IRCBot only needed a few days in August 2005 to develop their malware. In December, the WMF hole was already actively being exploited before Microsoft even became aware of it. Anti-virus manufactures reported monthly records in September, October and November 2005 in the number of newly discovered malware – in particular, new variants of already known malware families (such as MyTob, AgoBot, Sober, etc.) surfaced. Reports are unanimous that →mass e-mail viruses have receded in the past year, but at the same time, a massive increase of spy software by up to 68% has been recorded. Anti-virus companies estimate the share of spyware in the number of pests discovered to be about 70%. They assume that over 70% of computer systems worldwide are infected with spy software. Today's malware variants have become astonishingly sophisticated and employ →rootkit techniques to hide from anti-virus software or use polymorphic code to update the pest continuously via the internet and to subsequently upgrade its functionality or ability to hide from anti-virus programs. Increasingly, vulnerabilities of applications (especially web applications, anti-virus software, backup programs, →instant messaging software [IM], etc.) are exploited. The focus is shifting away from exploiting vulnerabilities of operating systems, which are becoming increasingly difficult to infect due to automated updates, integrated personal firewalls, and other advances, toward exploiting security holes in client-side applications and web applications. Chapter 3.3 analyzes the expected development of malware and investigates the causes of this trend.

2.5 VoIP security

Because of the increasing popularity and dissemination of →Voice over Internet Protocol (VoIP), more attention is being paid to its security and confidentiality. Since VoIP uses the →IP protocol, the threats and risks are similar to those known from the internet, namely →DoS attacks, →man-in-the-middle attacks, and malware. Spam can also become a problem for VoIP. If companies use VoIP instead of a conventional telephone system, then a breakdown of the IP network not only affects data, but also voice. In a study, the German Federal Office for Information Security (BSI) warns companies to think carefully before introducing

[3] An NISCC security advisory offers a good overview of botnet threats: http://www.uniras.gov.uk/niscc/docs/botnet_11a.pdf (as of: 14 Feb 2006).

VoIP, since this entails a significant threat potential.[4] Spectacular attacks have not occurred so far, but they must be feared. Confidentiality and availability are the two greatest challenges for VoIP security. It has been known for a long time that conversations over the internet can be recorded. Encryption algorithms exist, but effective key management is still lacking.[5] The new technique also requires a reinterpretation of the legal foundations, as will be discussed in chapter 8.

2.6 Rootkits

Since Sony's use of a →rootkit to protect digital copyrights on music CDs, this term has become widespread. According to its original definition, a rootkit is a collection of computer tools that are installed on a computer system once it has been broken into, in order to hide future logins of the intruder and processes (such as a spy program) from the user. While rootkits formerly were found exclusively on Unix/Linux systems, an increasing number of rootkits are now also being developed for Windows systems. This trend is likely to continue, especially since a book on this topic was published in the summer of 2005. Rootkits may not be new, but their use by large companies is. What makes the situation worse is that the rootkit installed by Sony apparently transmits data not only without the knowledge of the user, but also has enabled malware to be concealed (see chapter 10). In general, more malware with integrated rootkit concealment techniques surfaced in the second half of 2005, which has made their discovery and removal considerably more difficult (see also chapters 2.4 and 3.3).

2.7 Mac OS X: Increase of security threat?

This year for the first time, the SANS Institute[6] included vulnerabilities in Mac OS X in its annual top-20 ranking of vulnerabilities. In this ranking, SANS consolidated all discovered vulnerabilities in OS X into a single incident. Like every operating system, OS X is not immune from vulnerabilities, as the analysis of the security updates shows: According to the Open Source Vulnerability Database, Apple offered 81 patches last year, while Microsoft offered 89.[7]

One main reason for the smaller number of →malware for Mac OS X is probably the smaller distribution, although Mac OS X also uses the advantages of Unix and avoids Active X, unsecured services, and other potential security problems. The greatest security problems arise from applications such as the iTunes music program or the Safari web browser. Problems could emerge from the perception of these security problems. Apple still is very reserved in public statements on operating system security. In addition, the feeling of invulnerability is also widespread among users, so the motivation to protect one's computer is lower than for users of other operating systems. Accordingly, updates are often not downloaded, no firewalls are used, and the systems are often poorly configured. Once virus writers have taken on an operating system, however, it is only a question of time before the first attacks will follow.

[4] http://www.bsi.bund.de/literat/studien/VoIP/index.htm (as of: 21 Feb 2006).

[5] Tim Mather from Symantec at the RSA Conference (http://2005.rsaconference.com) (as of: 21 Feb 2006).

[6] http://www.sans.org (as of: 21 Feb 2006).

[7] http://www.osvdb.org/ (as of: 21 Feb 2006).

3 Trends / General developments

3.1 Individualized Trojan horses, social engineering, spear phishing: Greatest threat of industrial espionage

Already in the last semi-annual report, we discussed targeted industrial espionage, which is the focus of this issue: Chapter 2.1 analyzes the method used by attackers, while chapter 5.5 (Titan Rain) describes the largest espionage case uncovered so far.

Thanks to the professional approach and division of labour used by attackers, as described in chapters 2.4 and 3.3, and because more and more qualified hackers are selling or renting their services to organized crime, it must be assumed that much more powerful spy programs will be employed in the future, and an increasing number will be unknown to anti-virus manufacturers. The known methods (see chapter 2.1) are unlikely to change much, however.

Attackers engaging in targeted espionage often have resources at their disposal that make a systematic approach and a high degree of professionalism possible. Presumably, many attacks are sponsored by government circles, especially in the Far East (China; see chapter 5.2, Titan Rain). But such actions must also be expected on the part of private sector competitors, as the espionage case in Israel illustrated in the first half of 2005.

This shows the importance of comprehensive protection of a company network. This not only includes the technical protection of the systems down to the level of individual →hosts (host monitoring), but also the development of a security policy that governs the treatment of e-mails from unknown sources and the usage of mobile devices, via which spy software may also enter the company network (see also chapter 3.5). Regular training, especially of employees with access to confidential data, and the establishment of a company culture that is sensitive to IT security threats are indispensable for efficient protection from this kind of attack. Even an efficiently implemented anti-virus strategy alone cannot do much against unknown, targeted pests.[8]

In particular the operators of →critical national infrastructure, government and military circles, and military suppliers are in danger – it must be expected that this type of attack will continue to spread and will soon also affect smaller companies. Companies are likely to be especially exposed that maintain relationships with the Far East, that develop new technologies that are of interest to the competition, or that already have such technologies. Even if no information (yet) is available on similar incidents in Switzerland, MELANI believes there is no reason to assume that Switzerland can be excluded as a potential espionage target. The threat still must be considered serious

3.2 Botnets: Greatest threat of cybercrime

→Botnets already played a key role in the last semi-annual report and in chapter 2.3 – and this will hardly change in 2006. The two arrests of botnet owners and the worm war being fought over botnets (see chapters 5.2 and 5.3) clearly indicated in what way cybercriminals earn money and how seriously this threat must be taken. Even if the arrests represented great successes, they were only a drop in the ocean. As long as the operation of botnets is profitable and only few perpetrators can be identified, then the threat will hardly recede. The IT security service Prolexic, which specializes in defence against →DDoS attacks, estimates the loot of the most efficient of the botnet owner groups observed so far to be over US$ 8 million from DDoS blackmail.

Experts assume that botnets operating via →VoIP or →P2P networks, perhaps even with encrypted control commands, are to be expected in the future. If, for instance, the central (so far generally an →IRC) server is replaced by a flat control structure, it will be extremely difficult in the future to identify and deactivate a botnet.

[8] A security advisory of the NISCC provides more information on the types of the attacks and how to defend against them: http://www.uniras.gov.uk/niscc/docs/ttea.pdf (as of: 14 Feb 2006).

Comprehensive basic protection of the personal computer, as described on the MELANI website, offers far-reaching protection against infection from malware that could turn the personal computer into a botnet component. Additional measures can be found in chapter 6.

The threats emanating from botnets (spam, espionage, identify theft, DDoS attacks, encryption attacks, and the related blackmail, dissemination of malware, etc.; see chapter 2.3) are likely to further increase in 2006, especially since the number of botnets is steadily growing. Especially SMEs (in particular those with an internet presence) will likely be increasingly exposed to blackmail by botnet operators. Because of their diverse uses, their simple creation, and the criminal success achieved with them, botnots must be considered the greatest cybercrime threat.

3.3 Professionalization of the attackers: Division of labour, massive increase of malware production, new attack vectors

In the last semi-annual report, we already noted that →malware programmers pursue pecuniary objectives and that organized crime has also discovered cybercrime as a field of operation. The second half of 2005 clearly illustrates what the consequences are: rapidly increasing professionalism and division of labour, resulting in the accelerating development of malware (see, for example, chapter 5.2: worm war / critical holes rapidly exploited, and chapter 5.3: arrests grant insight into the →botnet scene; for an analysis, see chapter 2.4).

The cause of this development is the "successful" business of the financially-motivated cybercriminals: Malware code is published online and can easily be adapted by non-experts; there is a lucrative market for stolen data (such as e-banking customer data, credit card data, economically valuable information, etc.), just as there is for →exploit codes, spam botnets, and →DDoS blackmail. The division of labour of the organized hacker group will continue to increase in 2006, so that the steadily improved pests can be employed increasingly rapidly. The wide availability of such malicious code on the internet, in conjunction with the increasing popularity of e-banking and online shopping, also entails that more and more criminals will try their luck on the internet. In this respect, initial estimates are not astonishing which predict the gains through cybercrime will exceed those through the drug trade.

For 2006, MELANI expects a further qualitative improvement of →malware (better concealment through →rootkit-like functions, more flexible uses, more powerful functionality) and an even more rapid appearance of different versions of a malware family, shorter time periods between discovery of security holes and dissemination of the matching exploit code, increased use of new attack vectors (see chapter 2.4) and new →0-day exploits.

3.4 Phishing: Increasing threat also in 2006

→Phishing was already an important topic in the last semi-annual report and will continue to be timely (see chapter 2.2 for an analysis; 4.3 and 5.3 for incidents; and 6.3 for protection measures).

The improvement of phishing countermeasures (see chapter 2.2) feeds back on the armament of the attackers: Using ever more sophisticated →social engineering methods, such as phishing e-mails in the appropriate language and better-written messages, as well as new technological tricks, attackers try to find new phishing victims.

Additional phishing incidents should be expected in 2006 that may also affect Switzerland. To be expected in particular are even better counterfeit phishing websites than before (sometimes even with official →digital certificates), an increase in →keylogging software that can hardly be detected and that picks out confidential data on the victim's computer, an increase in DNS attacks to systematically redirect victims to phishing pages (both on local →hosts-files and also on →DNS servers), as well as an increase in websites containing malicious code for stealing passwords (via which keyloggers are distributed). In addition, an improvement of social engineering techniques (mainly better language skills; exploitation of the helpfulness of victims such as after Hurricane Katrina or the Indian Ocean Tsunami) and of the technical means of the attackers (→man-in-the-middle attacks in real-time, use of redundant phishing pages; constantly changing →redirect mechanisms) must be expected. Moreover, attacks against smaller financial service providers who

(still) have little experience in combating phishing and targeted →spear phishing espionage attacks against companies (method described in chapter 2.1; see also 3.1) are increasingly likely.

3.5 Threat to mobile devices (mobile phone, PDA)

The increase of →malware for mobile devices projected in the last semi-annual report, to be expected in particular with the dissemination of third-generation (3G) devices with constant internet connections, must again be emphasized here. In the second half of 2005, more 3G mobile devices were sold than ever before. At the same time, anti-virus manufacturers (especially F-Secure and McAfee) reported an increase of malware for mobile devices – already more than 100 such pests have been identified in the meantime (at the beginning of 2004: 10; according to F-Secure). In addition, an infection of several mobile devices with the Cabir worm for the Symbian operating system occurred at the track-and-field world championships in August 2005 in Helsinki and has meanwhile spread to over 30 countries. The threat is enhanced by the fact that only few users of mobile devices are sensitized to the danger, so that they configure their device in an unsafe way and fail to employ virus protection.

So far, the main functions of the pests have been limited to rapidly depleting the battery reserves or making the mobile device unusable; the attack vectors have been limited to Bluetooth and MMS messages, which must expressly be accepted by the receiver.

For 2006, MELANI expects an increase of threats against users of mobile end-user devices. Similar functions are to be expected as for computer malware: Encryption of mobile phone data followed by demands for money to restore it, or picking out of personal data such as date books and contacts. The first pests have already surfaced that can be transferred to a personal computer upon synchronization with the mobile device. Especially companies employing mobile devices are therefore exposed to a considerable threat of espionage.

4 Current national ICT infrastructure situation

4.1 Breakdowns, failures

ADSL interruptions

In the second half of 2005, there were two nationwide interruptions of ADSL service. On 6 December 2005, some of the business clients of Sunrise Business ADSL were affected by breakdowns of ADSL services. On 7 December 2005, the interruption was fixed. As Sunrise reported, the cause was a software error. The second ADSL interruption affected all customers of Tele2. During the entire weekend of 11 December, the services were only partially available. According to the provider, a malfunction of the hardware was the cause of the interruption. The consequences of these interruptions for the affected customers are not known.

Both of these incidents show how important it is to have a solid infrastructure for data transmission and, in particular, to be able to remedy malfunctions as quickly as possible. According to a national study conducted by the ETH Zurich, a national interruption of the entire internet for one week could cause losses to the national economy in the amount of 5.83 billion (thousand million) Swiss francs (see chapter 9).

4.2 Attacks

Defacements: Reaction times to athletic or political events are becoming increasingly short

In 2005, Switzerland was also not spared from attacks launched via the internet. The first MELANI semi-annual report discussed *script kiddies*, groups of young people who rather arbitrarily penetrate a server and commit mischief. For a wide range of reasons, the kiddies alter internet pages and abuse them for their political and social appeals. After Switzerland won the football world championship qualification against Turkey in November 2005, battles erupted outside the stadium between the supporters of the two teams. Already one day after the game and for the next few days, i.e. from 18 to 22 November, there were also fierce reactions on the internet: Several forums located on Swiss servers were attacked and their websites were defaced. The group responsible for the defacement called itself "IMHOT3b". Slogans were uploaded such as "Welcome to hell" or "Made in Turkey". On one of the websites, the Turkish national anthem and quotes by Atatürk appeared. According to Zone-H[9], IMHOT3b has been active since July 2005. So far, 165 cases of website defacement have been attributed to this group. All affected sites relied on versions of the support forum "phpBB" that were no longer active. Common to the versions used was that they were known to have several security holes. MELANI drew the attention of numerous hosting providers to the fact that some of their hosted sites had been targeted by such attacks. Normally, these attacks aim to alter the content of one or more websites, without however enabling access to further information. It is surprising how quickly the attacks were launched: From the time the result of the football game was announced, only several hours elapsed before websites became the targets of defacement.

Lotterie Romande: Yet another case of fraud

Spam is the quintessential internet plague. Swiss companies were not spared in 2005. Numerous financial institutions were targeted by spam attacks. The Lotterie Romande – a company that is also responsible for other lotteries – became the victim of a flood of spam. In e-mails supposedly signed by two promotion managers of the Lotterie Romande, the recipients were promised lottery winnings of one million euros. The e-mails were accompanied by a form that needed to be filled out. This form also requested the entry of banking information. According to J. Bessar, the communications director of Lotterie Romande, he does not know of anyone who incurred a loss because of this attempted fraud. The Lotterie Romande issued a preventative press release drawing attention to the dangers of such fraud attempts.

[9] http://www.zone-h.com (as of: 23 Feb 2006).

4.3 Crime

Phishing websites in Switzerland

At the end of June, the Cybercrime Coordination Unit (CYCO) received information from a Swiss internet provider that a client had abused webhosting services for illegal purposes. One person repeatedly used Romanian IP addresses to set up a URL address and subscribed to a web account using false data. As a rule, the hosting provider offers the requested service and subsequently bills the customer for the service. During this timeframe of approximately 48-72 hours, this person, who used the alias Willy Hertz (willyhertz@bluewin.ch, an address not used in Switzerland), attempted to set up a (PayPal) phishing site on the webserver and send numerous phishing mails. The fraud was only discovered after several days. Other Swiss hosting providers were also used for these activities without their knowledge.

Economic crime on the internet is increasing dramatically

A report by the Cybercrime Coordination Unit (CYCO) indicates that the number of economic crimes being committed with the help of the internet is increasingly dramatically. The report discusses the development from 2003 to 2005. During this time, the number of these economic crimes doubled from one year to the next. While CYCO recorded 145 cases in 2003, there were 289 cases in 2004. 275 cases had already become known in the first half of 2005.

"Economic crime and the internet" is a broad term encompassing several types of offences: e-mail phishing, money laundering, fraudulent escrow services (internet trustee services), abuse of credit card data, illegal acquisition of data, violations of copyright, and numerous other forms of fraud. According to the CYCO report, phishing was still a rather marginal phenomenon in 2003. Already in 2004, this type of offence increased dramatically, however, and represented a significant problem for Swiss financial institutions by 2005. Reports of counterfeit websites also became more frequent. Often, the prefix "swiss" – whether in an address or a title – is used to engender an impression of seriousness and trustworthiness.

Fraud still constitutes by far the largest share of internet offences, however. Internet users must be sensitized to the different types of fraud. In many cases, the fraud would have been preventable if the victims had shown a bit more care in advance. But despite the warnings and the information disseminated in the media about fraud on the internet, people repeatedly allow themselves to be taken in by the supposed opportunity to make a lot of money with little effort. CYCO is very well aware of the fraudulent means by which gullible users are lured into a trap. For instance, a private person sold several mobile phones to an Asian buyer. The payment was supposed to be made by credit card, but the credit card was stolen. In another case, an internet user bought a digital camera that he saw on a Chinese website; he transferred the money to an account in Beijing, but never received the camera. The outcome was similar for another person who bought several articles at an online auction and was asked to transfer the money in advance via Western Union.

CYCO Report 2005: Number of reported incidents has increased significantly

The Cybercrime Coordination Unit has been operational for three years now. The latest CYCO report indicates a significant increase in reported internet offences. While they were still 6,540 reported incidents in 2004, the figure increased to 7,345 in 2005. This represents an increase of about 800 reports or 12%. Several causes are conceivable: With the increasing number of internet users, the number of potential victims who fall for fraudulent intrigues on the internet has also increased. In the meantime, CYCO has gained recognition both in Switzerland and abroad and is consulted or informed more frequently in cases of doubt. That the number of reports has increased may also be due to the option of anonymous reporting of incidents, thereby protecting privacy.

In the reporting year 2005, CYCO forwarded 206 suspected cases to the cantonal police authorities. 79% of these cases were discovered thanks to CYCO monitoring; 21% of the reports came from internet users. Most cases affected cantons with the largest populations: The cantons of Zurich, Berne, and Aargau were ranked first. Of particular note is that in 89% of the forwarded reports, an investigation was initiated. In 78% of the cases, incriminating prosecution evidence was confiscated.

The work of the police is made more difficult if, for instance, a relevant website is accessed from an internet café and the identity of the user has not been recorded. It is also difficult to secure incriminating evidence if special software deletes the relevant data or if too much time elapses between the reporting of a case and the house search. A further problem is the increased ease of using software that encrypts or suppresses personal information. CYCO therefore recommended that cantonal investigators verify whether the computers of suspects contain software of this kind: It turned out that this software had actually been used in 9% of the cases.

The CYCO report is dedicated to several trends and topic areas: For instance, the number of reported economic offences has increased significantly. This fact can be considered evidence that internet crime is becoming increasingly professional and commercial. A further topic concerns chatrooms: At the latest since 2005, the question of the punishability of discussions conducted in chatrooms and the aspect of criminal prosecution have become more important. These are points that must continue to be discussed, especially since chatting is one of the most popular and widespread forms of communication among young people. Fortunately, the preventative measures adopted in this area appear to be successful.

In 2005, the abuse of weblogs garnered increased attention, after illegal material had been published and defamation had occurred. Such abuses were primarily reported from Western Switzerland. The abuse of weblogs should increasingly also be expected in German-speaking Switzerland.

4.4 Terrorism

The central computer of the University of Geneva as a centre for Islamist propaganda

In its issue of 29 October 2005, the *Weltwoche* reported that someone was uploading and disseminating Islamist propaganda on the internet via the IT network of the University of Geneva. Apparently, the propaganda came from al-Qaeda. The propaganda included films showing the Jordanian terrorist Abu Musab al-Zarqawi committing acts of violence (see chapter 5.4). The persons responsible: a 27-year-old Moroccan who had lived in Geneva for years without a residence permit, and a 41-year-old asylum-seeker from Algeria who had illegally entered the country. Apparently, the two men used four internet access accounts belonging to registered students to transfer the propaganda videos and other materials to webservers located in several locations around the world. In the first half of October, the two perpetrators worked from 10am to 4pm almost every day. According to reports, their activities included downloading two videos of suicide attacks in Iraq and then publishing them on relevant websites. The case was uncovered by Evan Kohlmann. For years, this American expert for cyberterrorism has been patrolling Islamist websites. Kohlmann directs the independent Global Terror Alert office in New York, which has its own website: *Global Terror Alert*.[10] In this case, he also informed *Weltwoche*.

The two perpetrators obtained the access data (username and password) of the accounts they used by simply "looking over the shoulder" of the lawful users while they were logging on.

Al-Zawahiri video published in forum

On 23 December 2005, a video message by the deputy leader of al-Qaeda, Aiman al-Zawahiri, was published in an internet forum. In this video, the terrorist threatened Western countries. The video could be seen in an internet forum operated by a Dutch woman of Moroccan descent living in Düdingen (FR). Her husband died while committing a suicide attack in Afghanistan. This woman was not unknown to the authorities: In September 2004, she uploaded pictures of decapitations of hostages held in Iraq onto her website. In February 2005, the Federal Criminal Police searched several apartments of persons suspected of affiliations with militant Islamist circles. Five suspects were arrested, including the woman in question. After she had been released, she expressed open threats against the law enforcement authorities. Apparently, she is currently writing a book in which she describes the law enforcement activities against her.

[10] http://www.globalterroralert.com (as of: 23 Feb 2006).

4.5 Miscellaneous

Spam smear campaign against Schengen/Dublin

Prior to the vote on acceptance of the Schengen/Dublin agreements, Swiss internet users were confronted with a wave of spam in the middle of 2005. This large-scale mass-mailing tried to mobilize against Schengen/Dublin. The spam campaign tried to convince undecided voters to vote against acceptance of the agreements. The general manager of the Zurich IT security company *Apexis Cleanmail*, Andreas Reinhard, confirmed that such a spam campaign had been unique up to that point.[11] According to Reinhard, the professionalism required by the mass-mailing of such messages, the method used, and the fact that the entire campaign was conducted completely anonymously indicated that a professional spammer or an excellently organized group was responsible. Reinhard suspects that the spammer or spammers were probably operating on behalf of a client.

Threat from the inside also in Switzerland

Preconceptions of IT or internet crime often focus on external hackers who – using the most modern technical devices – attack IT systems from a hiding place on the outside. It is too easy to forget that the far greater threat for a system often comes from one's own employees. The "Computer crime and security survey 2005", jointly published by the CSI and FBI, concludes that security incidents in American companies are primarily the company's fault. Often, the consequences of such internal failures are far more serious than the damage caused by hacker attacks. For instance, the managers of the Tokyo branch of UBS admitted that a hard disk had been lost on which highly confidential client data had been saved. The loss was the result of an unclear division of responsibilities and neglect of internal guidelines.

In the second half of 2005, the business and financial periodical "Cash" received an anonymously sent 169 megabyte data carrier. It contained client data from the private bank Julius Bär. The data covered the business years 1997 to 2003. According to "Cash", the data concerns known individuals from business, politics, and culture, including Swiss citizens. Even just the fact that such data could reach the public was a hard blow to the image of Swiss banks.

For more on this topic, see also chapter 6.3.

E-voting: Inaugural run in Switzerland

For the first time in a Swiss popular vote, citizens were able to cast their vote by internet or SMS. The system was put to the test by the municipality of Bülach in the canton of Zurich in a cantonal vote. According to official information, 37.3% of votes were cast electronically, most of which (around 25%) via the internet. Of particular note is that as many voters voted by SMS as in person at the ballot box. The only significant problem was that the PIN code included in the voting certificate had been printed lightly for reasons of security and was therefore difficult to read. Some difficulties also surfaced with respect to verification whether voters had voted twice. However, the political authorities and the voting officials were equally satisfied with the e-voting trial run, especially since the lines at polling stations were much shorter than usual. The trial was repeated a month later at a municipal vote in the municipalities of Bülach, Bertschikon, and Schlieren. 24% of the votes were cast electronically over the internet or by SMS; 11% voted in person at the ballot box, and the large majority voted by mail.

No obvious security problems surfaced and no cases of abuse were identified during these pilot votes. E-voting trials are being continued: In 2006, the cantons of Geneva and Neuchâtel will also make e-voting available. Afterwards, no further electronic votes are planned until an evaluation report is available. In the end, the Confederation and the cantons will have to decide whether voters should be offered e-voting as an alternative supplementing the traditional methods.

[11] http://www.cleanmail.ch (as of: 23 Feb 2006).

5 Current international ICT infrastructure situation

5.1 Breakdowns, failures

Computer breakdown at the Tokyo Stock Exchange resulted in losses

Two computer breakdowns in November and at the beginning of December caused considerable financial losses at the Tokyo Stock Exchange (TSE).

On 1 November, large parts of stock trading had to be interrupted for about 90 minutes due to a computer failure. According to the TSE, the manufacturer of the trading system, Fujitsu, followed wrong instructions when installing an update. Not only the Fujitsu manager, but also the CEO of TSE received a salary reduction because of the incident.

At the beginning of December, an employee of the trader Mizuho Securities wrongly placed a sales order for J-Com. Instead of offering one share for 610,000 yen (4,200 euros), the trader offered 610,000 shares for one yen. Although the employee noticed the mistake immediately, the trading system did not allow him to correct his entry for 10 minutes. This was enough time for several investors to place hundreds of thousands of shares on their purchase lists, even though only 14,000 shares were in free circulation. The subsequent deterioration of the value of the share and payment obligations caused Mizuho Securities a loss of approx. 283 million euros. Mizuho Securities is investigating whether compensation can be claimed from TSE.

TSE in turn is investigating whether the entire computer system must be reviewed. The CEO of TSE has meanwhile offered his resignation, while the Japanese minister of finance is recommending massive investments in the TSE computer system, rather than continuing to invest in a listing of TSE on the stock market.

At the Swiss Exchange (SWX) in Zurich, failures of this kind are not to be expected, according to SWX. Updates of the SWX computer systems are always verified in a test environment and only applied after a successful test using steps defined by a checklist. If wrong entries are made in the trading system, two protective mechanisms are available – both before and after the transaction has been made. If an entry is conspicuous, the system automatically intervenes, temporarily suspends the trade, and requires a confirmation by the trader. A transaction that has already been performed can be declared invalid if the price resulting from the transaction deviates substantially from the market price, or if an ordered market environment is no longer guaranteed. These protective systems have been successful in practice for years, so that the events at TSE did not give rise to action at SWX.

5.2 Attacks

Titan Rain: Targeted espionage attacks against the US, the UK, Canada and other countries, presumably from China

In June 2005, the British National Infrastructure Security Coordination Centre (NISCC) warned of targeted attacks with sophisticated →social engineering methods using tailored →Trojan horses. NISCC reported that →critical national infrastructure and government authorities had already been targets of potential attacks since 2003.[12] At the beginning of 2006, Chinese attackers unsuccessfully tried to spy on British parliamentarians with social engineering e-mails. The e-mail attachment contained prepared images that exploited the WMF vulnerability (see below).

As became known in July, Canada also experienced targeted attacks with individualized Trojan horses. These pests take aim in particular at the National Cryptologic Agency, at which the attackers apparently conducted a targeted search for confidential information. In addition, targeted attacks are also reported to have taken place against Australia and New Zealand.

It became known at the end of August that for two years already, systematic, professional computer espionage had been operated from China against military systems of the US government and against private

[12] http://www.uniras.gov.uk/niscc/docs/ttea.pdf (as of: 23 Feb 2006).

subcontractors, and that these operations continue to take place. Apparently, only non-classified networks of the Departments of Defense, State, Homeland Security and Energy, as well as of NASA and the World Bank had been successfully hacked. Within a maximum of 30 minutes, all interesting information had been downloaded without leaving any suspicious traces and with a high degree of professionalism. Among other data, the attackers stole military flight-planning software. An employee of Sandia National Laboratories, which was also targeted and is one of the must important developers of the US nuclear arsenal, traced the attackers via South Korea, Hong Kong and Taiwan back to their suspected origin: the southernmost province of China, Guangdong, from where the attacks were also launched against the British Parliament using the WMF exploit. The attacks could apparently always be traced back to the same three routers. Thanks to reporting software installed on one of the routers, the Sandia security expert discovered other actions of the attackers. His assessment: Each router is serviced by about six to ten workstations that are staffed around the clock. The FBI has apparently been investigating this case for some time under the codename "Titan Rain" and was working closely together with the Sandia expert.[13] After this information became known, the Sandia employee was fired and dropped by the FBI.

It remains unclear so far whether an action by the People's Republic of China is behind the attacks or not. Even though many attackers operating from other countries often use several hops via China to cover their tracks, several facts indicate an involvement of the Chinese government. The professionalism of the attacks, the continuous use of the source network, and the choice of the targets indicate an actor with very large financial resources – a State or mafia-like structures. An extract from the report of the U.S. Department of Defense concerning the military resources of the People's Republic of China also notes the following: "China's computer network operations (CNO) include computer network attack, computer network defense, and computer network exploitation. […] The PLA [People's Liberation Army] has likely established information warfare units to develop viruses to attack enemy computer systems and networks […]. [R]ecent exercises have incorporated offensive operations, primarily first strikes against enemy networks."[14] As the director of the British NISCC also explained at the end of November, the greatest threat to critical infrastructure emanates from States in the Far East, since these rapidly growing national economies have an insatiable need for information. He did not expressly mention China, however.[15] Although there is no clear proof, it should be assumed that the attacks are State-sponsored and are systematically operated against critical infrastructure, government systems, and the private sector of Western countries.

The most commonly described approach of the attackers (social engineering and use of Trojan horses with targeted programming), recommendations by MELANI to counter these attacks, and an assessment of the future threat can be found in chapters 2 and 3. *Even if information is not yet available on similar incidents in Switzerland, MELANI believes there is no reason to assume that Switzerland can be excluded as a potential espionage target of other countries or organizations. The threat must be considered serious.*

Worm war between Zotob, Bozori and IRCbot for the creation of a botnet – arrests provide insight into the hacker scene

Shortly after Microsoft published new updates on 9 August and thereby announced an existing security hole in its plug-and-play service for Windows 2000, these vulnerabilities were exploited. Several companies, particularly in the U.S., such as CNN, ABC, the New York Times, Disney, Kraft Foods, United Parcel, and construction-equipment manufacturer Caterpillar were hit by the subsequent →worm wave in a very short period of time. After the infection, the →bot controlled via →IRC downloaded additional →malware.

Within a few days, a veritable "war" could be observed between the different variants of the pest: Zotob, IRCBot, Bozori, etc., tried to trump each other. The worms not only attempted to turn as many computer systems as possible into →botnet zombies, but they also tried to uninstall each other. Of particular note is the speed with which the pests exploited the security hole. One day after the security hole was known, the first

[13] *Time* provided the most detailed press information: http://www.time.com/time/archive/preview/0,10987,1098961,00.html (as of: 25 Jan 2006).

[14] U.S. Department of Defense, Office of the Secretary of Defense, *ANNUAL REPORT TO CONGRESS: The Military Power of the People's Republic of China 2005*, p. 36, available at: http://www.dod.mil/news/Jul2005/d20050719china.pdf (as of: 25 Jan 2006).

[15] http://news.zdnet.co.uk/0,39020330,39237451,00.htm (as of: 25 Jan 2006). See also chapter 5.4.

→exploit code surfaced from the same Russian sources as Sasser in 2004. Four days later, the first Zotob variant was discovered.

On 25 August, local law enforcement authorities working closely together with the FBI and Microsoft identified Turkish citizen Atilla Ekici ("Coder", 21) and a Moroccan citizen living in Russia, Farid Essebar ("Diabl0", 18), as the initiators of the worm wave and arrested them. Apparently, Essebar was paid by Ekici for the development of Zotob, the widespread Mydoom, and also Mytob, a pest spreading by e-mail that had already been circulating in over 100 variants since February 2005. Essebar had also developed lesser-known pests. The two perpetrators belonged to a larger ring of credit card swindlers, the "0x90-Team". A few days later, Turkish authorities arrested 16 other suspected 0x90-Team members, who had apparently also disseminated variants of Essebar's worms. The motive for the attacks was commercial: The infected computers constituted a botnet via which various profitable activities could then be undertaken – in the case of the arrested credit card swindlers, the main interest was in collecting credit card information of private computer users to counterfeit credit cards.

Many companies still use Windows 2000. As a rule, companies only introduce security updates once extensive compatibility tests have been conducted, so that the hole exploited here still existed when the worm wave began. It is often very difficult to balance security considerations (introduction of the update as fast as possible) and continuity of business operations (prevention of a collapse of access after installation of untested updates). In addition, this incident demonstrates the importance of comprehensive IT security planning for companies. Even systems protected by firewalls, which would not be vulnerable to attack from the outside even without patches, could nevertheless be compromised. Linking up a private, infected notebook to the network was already sufficient to infect all the vulnerable computers in the firewall-protected network (see also chapter 6.2, Network Admission Control).

This incident illustrates the intentions, motives, and methods of increasingly professional cybercriminals discussed in chapter 3.3. Thanks to a division of labour and steadily increasing professionalism, the attackers are becoming more and more efficient and attaining ever greater financial gains (see also chapter 5.3: arrests of botnet owners in the Netherlands and the United States).

Sober worm: Class reunions, deceptive FBI / BKA e-mails, and right-wing spam

Even though →mass e-mail viruses and →worm infections decreased in 2005 (see chapters 2.4 and 3.3), several large virus outbreaks occurred, of which the Sober wave from October to December constituted the most widespread of all time.

On 6 October, a new variant of the mass e-mail virus Sober surfaced, which has been known already since October 2003, and was updated several times over the course of the following weeks. The first e-mail wave with Sober.S in the attachment contained the supposed message by a classmate who was looking for addresses for a class reunion. The system of anyone opening the attachment was infected with Sober. If the country domain of an e-mail address indicated an English-speaking country, Sober announced a supposed password change. In the middle of November, new versions surfaced that pretended to forward an erroneously received message actually intended for the victim. However, only the versions surfacing toward the end of November (Sober.Y / Sober.Z) became widespread, indicating in the body of the message that they had originated with the German Federal Criminal Police Office (BKA). The victims were accused of being subject to criminal prosecution because of illegal downloads of music, films, or software. In the English-speaking world, the same variant was circulated using a message supposedly originating with the FBI. Virus messages also promised winnings from RTL television or access to video clips with Paris Hilton. The large dissemination of the virus is evidenced by the fact that FBI mail servers received 200,000 messages per hour that were returned to the supposed sender after they could not be delivered.

Sober independently sends itself to all contacts in the address book of the victim. Sober is also able to download additional malicious code and can therefore add on additional functionality at any time (e.g., spy software for stealing personal data, spam mail, participation in →DDoS attacks, etc).

The security providers iDefense and F-Secure, who had analyzed the Sober code, also warned at the beginning of December that the Sober version distributed starting 22 November would download additional malicious code on 5 January 2006 and would be abused for the mailing of right-wing extremist Nazi propaganda e-mails. On 5 January 1919, the German Workers Party (DAP) was founded, which soon changed its name to National Socialist German Workers Party (NSDAP). Moreover, the Sober virus had

already previously been used several times to send right-wing extremist spam messages (see chapter 5.2 of the MELANI semi-annual report 2005/I). Because of the widespread warnings and blocking measures, the presumably German Sober author apparently refrained from downloading additional malicious software on 5 January.

The large dissemination of the mass e-mail virus is not due to particularly sophisticated code, but rather to the very cleverly employed →social engineering techniques. Using social engineering, the attacker attempts to make the victim perform some action out of curiosity or helpfulness. In the case of the Sober virus, this action was to click on the attachment. This method is also used for targeted espionage, for instance, and can be very successful if executed cleverly, as Sober demonstrates. An overview of the Sober variants identified so far can be found at:
http://www.computerworld.com/securitytopics/security/story/0,10801,107483,00.html.

Critical holes in Windows systems rapidly exploited: WMF 0-day exploit

At the end of December 2005, →exploit code was discovered that apparently had already been circulating since the beginning of December 2005. Through a security hole in the processing of WMF image files, a →0-day exploit was used to smuggle in and execute malicious code, thereby gaining control over the system. The system of anyone using Internet Explorer to visit websites containing a prepared WMF image was infected through the automatic display of the WMF image in the Windows image and fax display. The users of other browsers first had to click on a confirmation to trigger the infection. Even just the indexing of an infected image with desktop search software or its preview display in Windows Explorer also sufficed to infect the system. After the infection, the attacker was able to download additional malicious code at will. Within a few days, dozens of new exploit versions surfaced for the WMF hole in the form of greeting cards, e-mails, →instant messaging, news, or prepared websites. The WMF exploit was even used for an unsuccessful, presumably Chinese espionage attack against British parliamentarians by sending them messages containing prepared images as attachments (see above: Titan Rain attack). Due to the numerous versions, anti-virus programs were unable to offer reliable protection. By the time Microsoft released its (early) update on 5 January 2006, no satisfactory solution existed to remedy the infection risk. The installation of a patch developed in the interim by an IT security expert also constituted a potential risk, since this patch had not undergone the otherwise typical tests and therefore could lead to problems itself.

Even if the security hole could not be exploited automatically (such as in the case of worms), but rather required actions on the user side (visit of a website, clicking on an e-mail attachment, etc.), it represented a critical threat. The speed with which cybercriminals reacted to the security holes and with which variants of the exploit code surfaced is also a good example of the significant increase in professionalism of the attackers (see chapter 3). Allegedly, the WMF exploit was even being offered for sale for US$ 4000 on the internet. Also of particular note is that the WMF exploit had been completely unknown until the first active pests surfaced, which indicates that other unknown holes are already being actively exploited on the internet.

IM threats: Worms with rootkit capacities and language abilities

→Instant messaging (IM) represents an emerging threat for companies and home users (see also chapter 2.4), as vulnerabilities in IM and attacks via IM have shown. In the second half of 2005, almost all popular IM services such as those offered by Microsoft, Yahoo, and America Online (AOL) were affected. Not only the WMF exploit (see above) was distributed via IM among other channels, but also several other types of →malware.

At the end of August, a new "smart" →worm surfaced in Microsoft's MSN-IM network, which was for the first time able to adapt to the language of the user. Kelvir.HI communicated in Dutch, English, French, German, Greek, Portuguese, Swedish, Spanish, and Turkish. If the victim clicked on the link displayed in the IM message, a program was installed that gave the attacker control over the system.

By the end of October, AOL's AIM network was affected. The victim received a message with a link to a URL from an infected acquaintance already included on the victim's buddy list. The system of anyone clicking on the link was infected with malware that for the first time included →rootkit-like techniques for IM.

A further IM pest was discovered the beginning of December: A →bot was distributed through AOL's AIM network that could actively communicate with the victim. Via an (infected) acquaintance already entered in their buddy list, victims received a link by which infection with the malicious code was initiated. What was unusual about this pest was that it answered with sentences such as "lol no its not a virus" or "lol thats cool", thereby pretending to be a buddy actually communicating with the victim. This malicious code likewise allowed the attacker to control the infected computer.

Chapter 6.1 explains how computer users can protect themselves from IM threats.

5.3 Crime

Phishing: Widespread

→Phishing was also one of the greatest cybercrime threats in the second half of 2005.

In Germany, for instance, not only postal bank customers were targeted by phishers, but also customers of the Sparkassen savings banks and of Deutsche Bank. A →Trojan horse that first deactivated anti-virus software and then logged keystrokes was also sent out with counterfeit Telecom e-mails as a supposed "invoice". Over the weekend of 17 and 18 September, the security provider Websense recorded attacks on customers of over 24 European banks, especially in Italy and Spain. The largest Swedish bank, Nordea, was even forced by a phishing wave at the beginning of October to take its online banking portal offline for one day.

It is difficult to assess the damage incurred, since many losses are not even known to the authorities. As the German news magazine Focus reported in October, the criminal police of the German *Länder* were dealing with over 1000 cases in which customers suffered losses. According to Focus, the estimated losses in Germany amount to approximately 4.5 million euros, which is likely a conservative estimate. In Switzerland, however, the losses are far lower.

Even if some investigations have been successful, as indicated by reports of arrests in Estonia or the decrease in the average online time of a phishing website from over a week a year ago to 5.3 days now, phishing is a profitable business for cybercriminals.[16] In any event, they are investing increasing efforts to translate their fraudulent e-mails into other languages – one of the main reasons why phishing is spreading even in non-English-speaking regions, including Switzerland.

For an assessment of the threat posed by phishing and for expected trends, see chapters 2.2 and 3.4. Chapter 4.3 deals with phishing incidents in Switzerland, while chapter 6.3 contains preventative information on combating phishing.

Arrest of botnet owners in the Netherlands and the United States: Insights into the botnet scene

Arrests of →botnet owners in the Netherlands and California show the way in which cybercriminals employ botnets and that the increase in blackmail using botnets predicted in the last semi-annual report has come true.

At the beginning of October, Dutch authorities arrested a 19-year-old botnet owner and two of his accomplices (age 22 and 27). The three compiled an army of over 1.5 million botnet zombies with the help of W32.Toxbot (their own variant of the publicly available SDBot). The botnet was used for several purposes at the same time: Toxbot is able to record keystrokes and forward them to the attacker to spy out login data. The accused used this information to make purchases on eBay and PayPal using false names. Finally, they blackmailed the American adware manufacturer 180 solutions, threatening a →DDoS attack.

180solutions builds its business on third parties who connect the →adware of 180 solutions with their own software and then receive a fee for every installed version. Through the (illegal) installation of 180 solutions adware on compromised computers, the botnet owners regularly received money, until 180 solutions filed

[16] For information on the arrests in Estonia, see: http://www.bka.de/pressemitteilungen/2005/pm141105.html; the Anti-Phishing Working Group provides up-to-date phishing statistics: http://antiphishing.org/reports/apwg_report_Nov2005_FINAL.pdf (as of: 26 Jan 06 for both).

several lawsuits in August 2005 against illegally acting contract parties and also blocked the Dutch botnet owners from future payments. As a reaction to this development, the botnet owners demanded money from 180 solutions after a DDoS attack. On the recommendation of the FBI, the company paid, and the FBI was then able to forward the ascertained account data to Dutch law enforcement authorities. The Dutch authorities already knew of the botnet thanks to its prior discovery by the provider XS4All, so that the operators could be arrested in cooperation with the Dutch →CERTs and the National High Tech Crime Unit.

Similarly, the 20-year-old Californian Jeanson James Ancheta arrested at the beginning of November had constructed a botnet encompassing 400,000 zombies and attempted to rent it out via →IRC chat for spam mailings and DDoS attacks. Through the illegal installation of adware, Ancheta earned about US$ 60,000 and another US$ 3,000 through rentals to spammers.

Chapters 2.3 and 3.2 contain an assessment of the threat posed by botnets.

5.4 Terrorism

What terrorists use ICT technologies for:
"Virtual Afghanistan": Training/propaganda for jihadists now conducted online

Recently, there have been increasing discussions on the dubious danger of "cyberterrorism", which is why MELANI will take this occasion to assess the threat. This first part discusses the question to what extent the internet is used by terrorists. The second part below will evaluate the danger of a cyberterrorist attack and will draw a conclusion.

The number of jihad-related websites already increased dramatically after 11 September 2001 – but since the publication of the video with the decapitation of the American Nicholas Berg by the Iraqi terrorist group of Abu Musab al-Zarqawi on 11 May 2004, a professional recruiting, propaganda, and training machine of the jihadists has evolved online. While only a handful of websites were known eight years ago, there are currently over 4,700 sites, which constantly move around, exchange new content with each other, and link to each other, so they there are difficult to monitor, let alone interrupt.[17]

Since May 2004, al-Zarqawi's terrorist group has systematically distributed films and propaganda material with detailed information on their actions in Iraq. On 29 June 2005, for instance, a 46-minute, professionally produced video was linked to several jihad fora, portraying the group's fight. Several oral and written messages surface daily, and a magazine is produced once a month. The filming of terrorist attacks and killings in Iraq has become an integral component of militant action. Usually only a few hours after an attack, a film accompanying the attack becomes available on the internet. The third edition of al-Zarqawi's online magazine describes the objective: a war of information against infidels. The magazine explains that an attack without subsequent publication is hardly worth anything. Since October 2005, al-Qaeda circles have even operated a kind of terrorism TV. Instalments of the "Voice of the Caliphate", each about fifteen minutes long, have appeared twice and report on world events from the viewpoint of al-Qaeda, such as Hurricane Katrina, which was described as a soldier of God. Thanks to the use of logos, film reports, and music jungles, the program appears very professional. The fact that al-Zarqawi's webmaster, Abu Dijana, was arrested by the Americans the end of October will unlikely affect the professional web presentation of the terrorist group.

An online forum the beginning of August also called for intensified electronic jihad and offered →keylogging software, tools to conceal →IP addresses, lists of →proxy servers for anonymous internet use, and tools to attack websites or destroy data of hacked systems. In the second half of 2005, online forums of this type were also discovered in Europe (for forums discovered in Switzerland, see chapter 4.4). In the German town of Erfurt, for instance, an internet site was discovered which disseminated instructions for constructing bombs and rockets and for building up a terrorist cell.

Both suicide bombers in Iraq and jihadists in Europe, Egypt, and other countries use the internet intensively for training purposes, to obtain and process tactical information, to recruit new attackers, to procure financial resources, and for general communication purposes. It appears that the goal has already

[17] One of the most important researchers in this field is Prof. Gabriel Heimann of the University of Haifa in Israel: http://soc.haifa.ac.il/~rsso343/ (as of: 27 Jan 2006).

been achieved: The terrorists have found a replacement for the logistical terror hub of Afghanistan, which was lost in the wake of 11 September, in the virtual world of the internet. A massive, dynamic online library, for instance, offers detailed information on how to employ ricin, how chemicals found in drug stores can be used to build bombs, or in what way Iraq can be entered via Syria without being detected, in order to take part in the jihad. Detailed construction manuals for biological weapons (e.g., how to cultivate viruses in rats) and background information on nuclear explosives and carrier systems, discovered in October 2005, were distributed via Islamist forums.

In the meantime, experts therefore are calling al-Qaeda a web-oriented phenomenon. They assume, for instance, that the negotiations between al-Zarqawi and bin Laden on the "promotion" of al-Zarqawi's terrorist organization to the "Al-Qaeda Committee for Jihad in the Land of the Two Rivers" took place almost entirely online. Similar to other internet communities, such as for online role-playing, matchmaking, or collecting model trains, the online jihadists disseminate ideas, concepts, instructions, and tips for the jihad and grow together into a community that could never have been constituted in this form without the internet.[18]

What terrorists do not use ICT technologies for:
Debate on the threat of cyberterrorism

The last section analyzed terrorists' method of using the internet; this section assesses the threat of cyberterrorism. Especially in the United States, there has been a long-running debate on this question (see also semi-annual report 2005/I), which has not lost its relevance in the second half of 2005.

At an information warfare and security conference the end of November, for instance, an academic at Monash University expressed the belief that it is only a matter of time before an internet-based terrorist attack is launched against the United States or another Western country. He accordingly proposed a list of criteria for identifying cyberterror attacks: political motivation, terrorist leaders with advanced ICT knowledge, access to newest ICT, advanced knowledge of →SCADA systems, terrorist insiders within the targeted organization, and financial support.

In a speech at the end of November in London, Roger Cummings, Director of the British National Infrastructure Security Coordination Centre (NISCC), was more reserved, however. He believes that terrorists do not have well-developed capacities in this field and therefore constitute the lowest threat for →critical national infrastructure. He assessed the threat to be significantly higher that is posed by cybercriminals, who spy out critical national infrastructure for the purpose of selling information obtained. He believes the greatest threat is constituted by targeted social engineering attacks with tailored Trojan horses emanating from States in the Far East, with a clear allusion to China: "Foreign states are probing the CNI [Critical National Infrastructure] for information."[19] Cummings therefore believes the threat of cyberterrorism to be "over-hyped", similarly to the renowned cryptology and security expert Bruce Schneier, who believes the cyberterror hype is grounded in the State interest in the war on terror. Schneier is likewise convinced that the cybercriminal threat is much greater.[20] Finally, at the beginning of December, Louis Riegel, Assistant Director of the FBI and Head of the FBI's Cyber Division, made similar comments and held that neither al-Qaeda nor any other militant terrorist organization is able to attack power plants, airports, or other critical infrastructure via the internet. At the same time, he did not know of any such plans by terrorists. He also viewed foreign governments as a much greater threat to critical infrastructure.[21]

MELANI's assessment is similar to the views of the NISCC and the FBI: Cyberterrorism is still more of a media slogan than a current threat to critical national infrastructure, both in Switzerland and abroad. Most of the control systems used for the operation of critical infrastructure (→SCADA systems) are proprietary, which is why insider knowledge would be necessary for the attack, which terrorist organization probably do

[18] An overview of the jihadist forums found on the internet is available at: http://www.haganah.org.il/haganah/index.html (as of: 27 Jan 2006).

[19] Citing a ZDnet article: http://news.zdnet.co.uk/0,39020330,39237451,00.htm (as of: 30 Jan 2006). See also chapter 5.2 (Titan Rain).

[20] See: http://news.zdnet.co.uk/internet/security/0,39020375,39237490,00.htm (as of: 30 Jan 2006).

[21] See: http://www.computerworld.com/industrytopics/energy/story/0,10801,106923,00.html (as of: 30 Jan 2006).

not (yet) have. In addition, most of these systems could still be manually controlled in an emergency situation. And even if terrorists could manipulate such systems, this would be discovered quickly, and a high number of victims would be highly improbable. Since terrorist organizations deliberately choose their actions to generate as much fear and terror as possible, the cyberterrorist threat again appears minor.

The last section analyzed how terrorists use the internet for propaganda, recruitment, training, and communication – these functions of the internet are far too important for terrorist organizations that they would endanger the internet through their own actions. If terrorist acts should surface in connection with the internet or critical national infrastructure, it would be expected that this would occur in combination with a physical attack. It would be conceivable, for instance, that the communication of rescue teams after a bombing could be hampered through a cyberattack. Or, as a representative of the chemical industry of the United States fears, terrorists could gain information through internet attacks on storage sites or deliveries of chemicals that they could then use to illegally obtain these chemicals.[22]

In summary, it can be said that terrorists intensively use the internet, but are not (yet) able to use it as an instrument of terror. The far more important threat to the internet and to the infrastructure dependent on it is posed by cybercriminals and industrial spies. Nevertheless, the threat of cyberterrorism should be kept in mind: Critical infrastructure is inherently non-secure (see chapter 7.1, U.S. cybersecurity efforts), and it is certainly conceivable that terrorist organizations may some day be able to exploit this for attacks. In recent years, organized crime has likewise increased its use of professional hackers – and their know-how could be increasingly procured by terrorists in the future. In the field of arms smuggling, drug trading, and general procurement of financial resources, the link between organized crime and terrorism is already a reality.

Germany: New federal government continues red-green anti-terrorism strategy

At the beginning of November, the CDU/CSU and the SPD agreed on their domestic policy framework, within which the fight against terrorism is accorded one of the highest priorities.

The most important point in the strategy of the new government is the rapid realization of a joint anti-terrorism database for information exchange between the police and the intelligence services. In addition, the Federal Criminal Police Office (BKA) is granted preventative powers to defend against international terrorism and to operate more covertly than before. The introduction of biometric identity documents envisaged by the old government will also be maintained. To protect the →critical infrastructures in Germany, the grand coalition intends to implemented the red-green "National Plan for the Protection of Infrastructure" published in the summer (see chapter 7.1). In addition, close cooperation between the State and the private sector will be realized to make the fight against criminal activities on the internet more efficient. Implementation of the EU directives on the storage of telecommunication data (see chapter 7.1) is also being considered crucial. The grand coalition plans to store telecommunication data for six months, thereby imposing the same standards as in Switzerland.

[22] See: http://www.heise.de/newsticker/meldung/64031 (as of: 30 Jan 2006).

6 Prevention

6.1 Software

Microsoft invests in security

In the last half year, Microsoft presented new or revised security programs. Among other upgrades, the company made version 2.0 of the Microsoft Baseline Security Analyzer (MBSA) available. This tool is intended to detect incorrect configurations in Windows and other Microsoft products that are relevant to security. For instance, it verifies whether all current security updates have been installed. MBSA runs on the operating systems Windows 2000, XP, and Windows 2003. It also analyzes Webserver IIS in versions 5.0 and 6.0, SQL Server 7.0 and 2000, Internet Explorer version 5.01 and above, and Office 2000, 2002, and 2003. In particular, the scanner monitors security updates for Office XP and provides evaluations on how serious the detected security problems are.

After Microsoft bought the Romanian anti-virus software GeCad two years ago, Microsoft has now published Windows One Care Live. The beta version is free of charge. The final version will, however, probably be offered for a monthly fee. It combines anti-→spyware with anti-virus software and contains a →firewall. The software is part of the new internet appearance "Live",[23] with which the computer can be checked online via Internet Explorer for potential pests or vulnerabilities. After Microsoft's entry into the anti-virus business, the EU anti-trust commission has become interested in the company's plans.

Microsoft is also reacting to the increasing →phishing problem and offers an anti-phishing toolbar that can be downloaded for free. Unfortunately, it can currently only be started if MSN Search Toolbar is also installed. Internet Explorer 7, which should be offered sometime this year, is planned to have phishing protection implemented as a standard feature. Chapter 6.3 contains additional information on anti-phishing tools of other suppliers.

Effective protection for the PC

Attackers and malicious software often exploit security holes in the operating system or in applications that allow code to be executed at will. Attacks make use of the fact that certain functions of the operating system or the application are always located in the same addresses in memory (many →worms in the recent past exploit this fact). One type of possible countermeasure approaches this problem by assigning applications and the functions they use (libraries) to randomly chosen memory addresses upon booting up the system. In this way, it is often much more difficult for attackers or worms to execute code at will. Linux and BSD systems have already offered such protection measures for a long time; on Windows systems, however, they have not yet become a standard feature.

WehnTrust is a host-based Intrusion Prevention System for Windows based on the principle just described that is available for private users free of charge.[24]

Using instant messaging securely

The →instant messaging (IM) software manufactured by Microsoft and AOL is becoming very popular. The use of these programs consists in the simplicity and speed with which users can communicate in real time with each other and exchange data.

The distribution of malicious code via IM harbours the same dangers as the traditional distribution method via e-mail. In the case of an IM-based attack, the code directly accesses the address list and then automatically sends itself to all conversation partners online. As soon as the →worm has spread, the contact to which it has sent itself is deleted from the list. Even more powerful codes possess a distribution list of infected users, so that they know in advance to whom they do not need to be sent, since the address in question has already been infected.

[23] http://www.live.com (as of: 8 Feb 2006).

[24] http://www.wehntrust.com (as of: 22 Feb 2006).

→Social engineering plays an important role in IM-based attacks. Although in many cases the user has to perform an action (clicking a link, downloading an image, etc.) for the computer to become infected, this obstacle can easily be surmounted via IM, since most IM services allow access to the user profile. Potentially, malware could exploit this information (e.g., on gender, age, profession, or even a picture) to make the victim believe that the contact person sent the message intentionally. Examples of IM attacks are described in chapter 5.2.

Tips for using chat and instant messaging:
http://www.melani.admin.ch/gefahren-schutz/schutz/00027/index.html?lang=en.

Developments relating to Sender ID / Domainkeys

Discussions have been revived on a standard authentication procedure for e-mails. After the two competing techniques Sender Policy Framework (SPF) by Meng Wong and Sender ID by Microsoft were suspended by the Internet Engineering Task Force (IETF) in 2004 because the political and patent law controversies were too great, Microsoft has now submitted a new initiative to IETF, causing IETF to change the status of the procedure to "approved as experimental standards". In its report, however, IETF does not adopt any position on which approach is to be preferred in the fight against spam and even warns of important open questions, such as the forwarding function.

Other procedures are also being taken into account and discussed by IETF. In August 2005, the new procedure Domain Keys Identified Mail (DKIM) was presented. DKIM is based on a combination of the Domain Keys System developed by Yahoo and the Internet Identified Messages developed by Cisco. PGP and Sendmail are also in the same boat. The project is meanwhile being supported by different companies, such as EarthLink, IBM, Microsoft, and AOL, the last two of which are advocating for the Sender ID procedure.

With the DKIM method, the e-mail does not have to be signed by the e-mail client, but by the e-mail provider. Accordingly, spamming would not be prevented within a domain, and the provider would be responsible for domain-internal monitoring. But this would likely lead to considerable problems with large providers such as Hotmail and GMX. In addition, this procedure does not prevent spam in general, but only spam that is sent under a false domain. This can certainly be helpful in automatically identifying phishing e-mails, for instance, that have supposedly been sent by a bank. But it does not help if the spammer continuously acquires new domains with the associated DNS entries. It is therefore quickly becoming clear that there will be no single solution, but rather that various methods must complement each other in solving the various subproblems. It is still open which technical solutions will prevail in this regard.

6.2 Hardware

New developments relating to wireless networks

Expansion of the →WLAN protocol by exact timestamps makes it possible to determine the distance of a laptop to an access point to an accuracy of just a few centimetres. Along with the possibility of using hotspots for very precise identification of location, this "precision location" function can also be used for security. In addition to encrypting wireless communications with →WEP or →WPA, this allows attackers accessing an access point from outside the home to be identified and blocked. To calculate not only the distance to the hotspot, but also the exact position, several access points are necessary.

The processor manufacturer Intel is already experimenting with technologies that allow wireless networks to be used to determine the exact position of a receiver. With this new technology, Intel intends to develop an alternative to the Global Positioning System, GPS. GPS is only of limited use in inner cities, since high buildings block direct view of the satellites. Determining locations by WLAN is already possible today, however. According to de.internet.com, the start-up company Skyhook Wireless offers such a service. This service determines the position by measuring the signal strength of different wireless networks. This allows identification down to several meters, even in buildings. The receiver only needs a standard WLAN module and special software.

Such determination of location using WLAN wireless technology could also offer a possibility for determining the position of a caller placing an emergency call (see problem of emergency calls with VoIP in chapter 8).

Network Admission Control

Point-to-Point Protocol (PPP) is probably still familiar to many readers from the era of internet modem connections. It is primarily used for modem dial-up access to the internet. A number of authentication methods are used for PPP, including the Challenge Handshake Authentication Protocol (CHAP) and the Password Authentication Protocol (PAP). Before a connection is granted to the network, the username and password are verified. This authentication method can be expanded as needed, and certainly more than the username and password can be included in the authentication scheme. The Extensible Authentication Protocol (EAP) makes many different authentication methods available, including MD5 Challenge and one-time passwords. Other variables may fall within the scope of the authentication criteria. For instance, these include verification whether all updates have been installed on a computer and whether up-to-date virus software is being used. The verification of access criteria is then concluded by sending a success/failure packet. In general, this type of authentication is defined by the IEEE 802.1x standard.

Recently, Cisco introduced a new version of a NAC (Network Admission Control) authentication solution. NAC computers connected to the network automatically test whether up-to-date anti-virus software, the most current anti-spyware tools, and all security updates have been installed. If an attached system does not pass these tests, the connection to the network is denied, and the user is informed how to better protect his or her computer. While other authentication methods only ask for usernames and passwords, NAC also requires a system to be functioning flawlessly before it is granted access. Especially for companies using mobile devices, this technology should represent an important improvement of their security concept.

New Bluetooth threats

A secure connection between two →Bluetooth devices is based on a pairing process. The devices wanting to exchange data first introduce themselves. A connection key is exchanged; the same PIN code must be entered on both devices. The key is then used to identify the device in the future. This security mechanism has now been bypassed by Israeli researchers.

The trick is to interfere with the communication and force a termination of the connection, so that a new pairing process is triggered. The identification number of one of the two devices is used, which is openly transmitted to other Bluetooth devices within the wireless radius. Using this identification number, the attacker now pretends to have lost the encryption code, which triggers a new pairing process. It has been known for some time that a subsequent new pairing attempt can be broken into. The communication is tapped, and all possible PINs are tried out within a few seconds using special software. In the case of a four-digit PIN code, there are only 10,000 possibilities.

Tips for using Bluetooth are available on the following page:

http://www.melani.admin.ch/gefahren-schutz/schutz/00028/index.html?lang=en.

6.3 Miscellaneous

New developments relating to anti-phishing tools

Online banking has become more popular among Swiss. Criminals also want to benefit from this. With sophisticated methods, they try to obtain customer data. According to banking industry sources, however, the financial losses appear to be low compared to credit card fraud. In England and Ireland, but also in France, Italy, and Spain, some financial service providers still protect electronic banking accounts only through a username and PIN code. In Switzerland, an additional identification code is necessary for each e-banking session. This number is either distributed on a code list or generated with special calculators.

Russia and Belarus are considered possible countries of origin of these attacks. To conceal the flows of the stolen money, the criminals used middlemen, hiring people with low income. The job of these middleman is to forward assets abroad by money transfer that have previously been transferred to their account, in return for a commission; these acts are also punishable.

In addition to access controls, the countermeasures to →phishing attacks should also focus on the online behaviour of users. If a person always logs in from Switzerland and then a sudden login attempt is made from a country with high phishing activity, it is worth verifying the transactions made and, if appropriate, to contact the customer.

Software manufacturers are also reacting to the increasing phishing problem and are making anti-phishing tools available. Microsoft offers an anti-phishing toolbar, which can currently only be installed if MSN Search Toolbar is also installed. Internet Explorer 7, which will be introduced sometime this year, is also expected to have this phishing protection implemented. The e-mail program Thunderbird already offers phishing protection and, beginning with version 1.5, examines e-mail messages for attempts at fraud. Another efficient program is provided by Netcraft.[25] This toolbar, which runs both under Internet Explorer and Mozilla Firefox, automatically displays a warning if the site accessed is listed as a phishing site in the central Netcraft database. Conversely, phishing sites can be reported with a simple mouse click, which are then included in the database upon verification. Additionally, the tool displays a risk rate for each site. This is primarily based on the time the site has been online: phishing sites are generally put online only a short period before the attack, while official banking sites have generally already been online for years.

Postfinance is currently testing a new authentication procedure for its online services. The functions of the Postcard will be expanded accordingly to curb the current threats on the internet. The addition is called CAP (Chip Authentication Program), which will expand the EMV standard valid worldwide. Until the end of February 2006, this new login procedure is being tested for the web portal Yellownet by 250 postal service employees. The "normal" Postcard, which may also be used for withdrawing cash from Postomat cash points, may additionally be used as the login card for e-banking. This can prevent phishing attacks such as those that occurred in June and October of last year (see also chapter 4.3).

Other efforts are also underway to curb phishing. These include the authentication process iTAN (indexed Transaction Numbers) and mTAN (mobile TAN). In contrast to normal lists of codes, which require entry of the codes in sequence, the iTAN procedure randomly picks out a number. Phishing is made more difficult in this way, since the perpetrator does not know which code will be asked for next from the list. Using a conventional approach, the perpetrator would then have to phish for all numbers on the code list, which would probably raise the suspicion of any user. But new methods already exist to compromise this procedure. Using a →man-in-the-middle attack, an account at the German Postbank was broken into. The mTAN process sends the code list number to a mobile phone via SMS. This process is only useful, however, if every transaction is protected by TAN and, additionally, the amount to be transferred is displayed in the SMS. This process is quite complicated, however, and also costly.

Fight against bot networks

The number of zombie computers connected into →bot networks (botnets) is now in the millions, as the arrests discussed in chapter 5.3 also indicate.

In many countries, efforts are underway to combat bot networks. The Australian Communications and Media Authority (ACMA) is currently tasked by the Government to find out over three months if gentle force can be used to stop this form of cyber hijacking. Officially, the campaign is called "Australian Internet Security Initiative", while ACMA itself is calling it the "Australian Zombie-Hunting Program". The campaign is initially planned as an experiment in which the five largest internet service providers (ISP) are participating. ACMA intends to monitor data transmissions suspected of belonging to a bot network and in this way to track down zombies. The Australian NIC, which distributes addresses in the ".au" domain, reviews the IP data found in this way and verifies whether the affected computers are located in Australia, so that their owners can then be informed. This approach has already been used successfully for several years by Swiss ISPs.

[25] http://netcraft.com (as of: 8 Feb 2006).

There are also private initiatives targeting zombies. Sophos is offering a new service that warns companies of unnoticed abuse of their computers. The services track down zombies in a network of a company and warn those responsible in a timely manner. For this purpose, Sophos has set up traps (honeypots). For instance, if a spam e-mail originates from an IP address under surveillance, the company is informed. Public blackhole lists (DNSBL) are also used for the analysis.

Insider threats

In the last half year, the security firm Trend Micro published a study indicating that the majority of computer users feel more secure using IT at work than at home. As a consequence, 63% of those surveyed indicated that they prefer to open risky websites at work than at home. The threat that pests may be imported through such imprudence is obvious. Sophos is also addressing this topic and indicates that 80% of IT administrators are unhappy with the conduct of their staff members in using IT resources. According to this study, most "offences" include downloading music and films, opening e-mails, attachments, and links of unknown origin, surfing on dubious or pornographic websites, executing "programs for fun" received from friends or colleagues, installing unauthorized software and →browser plug-ins, forwarding information via e-mail and telephone to unknown recipients, use of the same password for different websites, and joint use of passwords. The threat emanates not only from carelessness and indifference, however – targeted attacks also occur in which employees (or ex-employees) deliberately break into the company network to steal or delete data. Due to insider knowledge, such attacks are even more frequent than classical hacker attacks from the outside. An example that made headlines in the summer of 2005 was the theft of customer data from the bank Julius Bär by a former employee.

According to a study by the U.S. Secret Service and Cert/CC, most insider attacks are preceded by a "negative" experience by the employee in the company.[26] This may be refusal of a pay raise or promotion or, in extreme cases, a lay-off. The motive for such attacks is therefore usually revenge. The attack is usually planned in detail, using backdoors or account clearances; the attack is committed from the outside via the network. A large problem of such insider attacks is their detection. Generally, such attacks are only registered when system irregularities become known or the system breaks down. →Critical infrastructure in particular is threatened by insiders (see chapters 5.4 and 7.1).

Particularly when companies make headlines in connection with data theft, this tarnishes the company's image, which may have a negative effect on client relationships. A study by the Ponemon Institute[27] shows that 20% of clients react negatively to such an incident. This indicates that the number of unreported cases of data theft is not negligible.

[26] http://www.secretservice.gov/ntac.shtml#programs (as of: 23 Feb 2006).

[27] http://www.ponemon.org (as of: 8 Feb 2006).

7 Activities / Information

7.1 State

Switzerland: Tender of licenses for broadband wireless access

The Swiss Federal Communications Commission (ComCom) has opened a tender for licenses for broadband wireless access (BWA). BWA is broadband wireless access to a telecommunications network, such as for access to the internet. BWA is a general term for several wireless access technologies including WLL (Wireless Local Loop), FBWA (Fixed Broadband Wireless Access), and MBWA (Mobile Broadband Wireless Access). WiMAX and HiperMAN are the corresponding trademarks. The WiMAX Forum (www.wimaxforum.org) is a non-profit association of device and component manufacturers. The goal of the association is to promote the use of devices fulfilling the IEEE 802.16 standard with the help of operators of broadband wireless systems. A further goal is to ensure the compatibility of the devices.

Once the results of the consultation procedure initiated by the Swiss Federal Office of Communications were available, ComCom decided to grant three new BWA licenses for the frequency range between 3.41 and 3.6 MHz, in light of the frequencies currently available. The primary objective of the Commission is to enliven competition in the field of broadband connections. 24 interested companies have applied for the licenses. The licenses are being auctioned. The minimum bidding price for the two large licenses is 6.1 million Swiss francs each and 5.1 million Swiss francs for the small license.

EU: Parliament decides on storage of telecommunications connection data

At the beginning of 2004, the EU initiated new efforts to govern the storage of connection data of all types of telecommunication by law throughout the EU (e.g., services such as telephone, SMS, e-mail, internet); these efforts came to fruition in 2005. On 21 September 2005, the EU Commission presented a draft directive on the storage of telephone and internet data, after months of disputes between the EU Council and Commission and the various EU authorities and council presidencies. The purpose of the buffered data storage is to increase efficiency of criminal prosecutions, especially relating to terrorism and organized crime.

On 14 December 2005, the EU Parliament gave its consent to the draft and agreed on a data storage duration of between six and 24 months. In February 2006, the EU Council is scheduled to pass a formal decision on the directive, which will require national implementation of the guidelines in the EU Member States. The Member States will be free to lay down their own data storage limitation between six and 24 months. In Germany, for instance, the government is planning a six-month storage limit, while France is planning on 12 months. The question has not been expressly regulated who is responsible for the arising costs. Especially among data protection and human rights experts, the EU Parliament decision is controversial, in particular given that the connection data of 450 million EU citizens would be stored independently of any incident, and therefore every citizen would be treated as a potential criminal. In Germany, for instance, the government is planning to allow use of the data for criminal prosecution only in cases of considerable offences or offences committed via telecommunications, while the EU directive itself provides for prosecutorial access to the data only in the case of serious crimes. A precise demarcation of "serious" and "considerable" crimes is not made, however.[28]

There is no need to amend the existing Swiss provisions, also given that they already correspond to the planned German implementation of a six months storage limit. Article 15, paragraph 3 of the Federal Law on the Surveillance of Mail and Telecommunications (BÜPF, SR 780.1) requires the providers of telecommunications and internet services to "preserve the data necessary for identifying subscribers and usage and invoicing data for six months."

EU: Commission launches Green Paper on Critical Infrastructure Protection

At the end of November, the EU Commission adopted a green paper on the topic of →critical infrastructure protection, which puts forward for discussions possible actions of the Commission, upon the request of the

[28] http://www.heise.de/ct/aktuell/meldung/66857 provides an overview of the topic (as of: 30 Jan 2006).

EU Council to create a European Program for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN). After conducting seminars and taking into account comments by Member States, this document now constitutes the basis for additional feedback by the various affected interest group representatives.

The medium-term goal is to establish a framework within the EU to protect →critical infrastructure, to guarantee appropriate and equal protection of national infrastructures, and at the same time to not distort the national competitive environments within the EU. The document is available at: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.[29]

Germany: National Plan for the Protection of Information Infrastructure presented by Interior Minister and BSI / Report on the Situation of IT Security published

In August 2005, then Interior Minister Otto Schily of Germany presented the National Plan for the Protection of Information Infrastructure, thereby explaining the IT security strategy of the federal government, which the new grand coalition likewise wants to continue.[30] One day later, the German Federal Office for Information Security (BSI) published its first Report on the Situation of IT Security.[31]

Like Switzerland, Germany considers the security of information infrastructures (→CIIP) to be a security policy responsibility of the State. Also in Germany, the focus is on addressing the problem in as holistic a manner as possible, so that computer systems or home users are examined in as much detail as company networks or government systems. The plan provides for the drafting of IT security standards for the federal government, the establishment of a MELANI-like federal IT crisis centre, and general elevation of the IT security competence of the population. The strategic goals are prevention, reaction, and sustainability.[32]

The Report on the Situation of Information Security, comparable to the MELANI semi-annual reports, discusses the security awareness and security competence of citizens, the private sector, and public authorities. Current threats are also evaluated and the potential development assessed.

New anti-terror laws in some EU States / Anti-terror strategy of the EU

Several EU States have adopted new anti-terror laws, and also in the EU as a whole, the coordination of relevant measures is being pushed forward.

Italy already passed a new anti-terror law the end of August. Criticism has arisen in the meantime in particular concerning regulation of internet cafés: The operators of internet cafés must now apply for operating licenses, register customers, archive surfing behaviour, and save e-mails. The consequences: Internet cafés in Italy are suffering losses of over 50%, and the authorities are substantially behind in processing operating licenses.

England has also passed a new, far-reaching anti-terror law. Similar to a censorship authority, police officers are now authorized to prohibit mediators of publications promoting terrorism (e.g., internet providers, booksellers, publishers) from offering the publication. This also includes the publication of information that could be useful for the dissemination or execution of acts of terrorism, or that glorify terrorism. Newly created offences include entering nuclear facilities or terrorist training areas; suspects may

---

[29] Additional background information is available at: http://europa.eu.int/rapid/pressReleasesAction.do?reference=MEMO/05/441&format=HTML&aged=0&language=en&guiLanguage=en (as of: 30 Jan 2006).

[30] Available at: http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Common/Anlagen/Nachrichten/Presse-mitteilungen/2005/08/Nationaler__Plan__Schutz__Informationsinfrastrukturen,templateId=raw,property=publicationFile.pdf/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf (as of: 31 Jan 2006).

[31] Available at: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf (as of: 31 Jan 2006).

[32] The Swiss information assurance concept is based on a 4-pillar model: prevention, early recognition, crisis management, and technical problem resolution. More information is available at: http://www.efd.admin.ch/d/dok/faktenblaetter/efd-schwerpunkte/5_infosicherheit.htm (as of: 31 Jan 2006).

now be held without judicial order for up to four weeks; and wiretaps may now be conducted for six months without a new authorization.

Shortly before Christmas, France also adopted a new anti-terror law, which is one of the most restrictive in Europe and provides for massive expansion of video surveillance and storage of connection data for 12 months (also for internet cafés). Public transport, train stations, public buildings and spaces, nuclear power plants and industrial facilities may now be placed under video surveillance; at toll plazas, automobile traffic is also registered. In the case of suspicion of terrorism, interrogations (and therefore detention) may now last six days without an arrest warrant.

At the beginning of December, the interior ministers of the EU Member States agreed on a joint strategy against recruitment and incitement for terrorism. The abuse of the internet for this purpose will be combated in particular. Recruitment in prisons and mosques will be made punishable. The intention to ensure common protection of →critical infrastructure (see above) was also emphasized. The goal of these efforts is to harmonize the national laws of the Member States.[33]

United States: Tighter organization of cybersecurity efforts and renewed criticism

After criticisms of the cybersecurity efforts of the U.S. Department of Homeland Security (DHS) (see last semi-annual report) and Senate hearings conducted on this topic in July 2005, DHS Secretary Michael Chertoff announced a reorganization of his department in the summer. A new cybersecurity chief will have the rank of Assistant Secretary and be responsible for cybersecurity and telecommunications security in the United States. The reactions to this announcement were thoroughly positive both in the Senate and in the private sector. The hope is that authority will be enhanced for enforcing regulations and that the private sector will be better integrated into security efforts. The U.S. Congress approved the necessary resources to implement this reorganization in October, but the post had not yet been filled as of the end of the year.

Nevertheless, the critics of U.S. cybersecurity measures have not been silent. An article in the August issue of IEEE-USA Today's Engineer warned that the IT infrastructures in the U.S., such as flight control systems, power plants, and financial, military, and intelligence systems are highly vulnerable to terrorist and criminal attacks; the situation is almost out of control. In a hearing before the science committee of the U.S. Congress in September, representatives of large U.S. companies expressed their fears of cyberattacks. The greatest concerns were over physical attacks combined with cyberattacks. The Government Accountability Office (GAO) of Congress announced the end of September that the networks of the flight control system were vulnerable to attackers with insider knowledge. In October, a former member of the President's Information Technology Advisory Committee criticized the lack of leadership in the field of electronic security, the delays in appointing a cybersecurity chief in DHS, and the lack of investments in research. Shortly after this, the inspector general of the Department of Transportation (DOT) announced that he had obtained control over vulnerable servers and received access to sensitive information during tests, and that he had identified over 3,000 weaknesses in the DOT network, some of which had already been known for a long time, but had never been remedied. In general, there was also a lack of an →intrusion detection system in DOT, to which the railway and flight administration authorities also belong. The lack of patch management had led to Zotob infections (see chapter 5.2). At the end of October, the inspector general of DHS criticized the security of the Secret Service systems, and at the beginning of December, the members of the 9/11 Public Disclosure Project (the former 9/11 commission) warned that the government was making too little progress in protecting its critical infrastructure, especially communication networks and the internet. Neither risk and vulnerability studies had been conducted, nor had priorities been fixed. The deficiencies were deemed to be scandalous and shocking. In the middle of December, finally, representatives of the Cyber Security Industry Alliance (consisting of large IT security providers and software and hardware manufacturers) also criticized the delays in naming a DHS cybersecurity chief as well as lacking research investments, although it was announced in November that companies will in the future be able to increase their tax deductions for

[33] The new British Terrorism Bill is available here:
http://www.publications.parliament.uk/pa/ld200506/ldbills/069/2006069.htm (as of: 31 Jan 2006).
The French anti-terror bill is available at:
http://www.assemblee-nationale.fr/12/ta/ta0506.asp (as of: 31 Jan 2006).
An overview of the anti-terror efforts in the EU can be found at:
http://www.eurunion.org/partner/EUUSTerror/EURespUSTerror.htm (as of: 31 Jan 2006).

research. Also, some researchers announced their concerns the beginning of October that American mobile phone networks could be vulnerable to SMS DoS attacks.

Even if terrorists do not yet have the resources for a cyberterrorist attack (see chapter 5.4), it must be noted that →critical information infrastructure is still vulnerable. Insider knowledge that terrorists are not yet likely to have may be necessary for successful attacks – but this could change in the future, similarly to how organized crime has obtained access to hacker circles in recent years. The fact that the U.S. in particular – the leading hi-tech nation in the field of information technology – exhibits great vulnerabilities in these infrastructures indicates that these vulnerabilities also exist in the infrastructures of all other Western industrial countries.

7.2 Private sector

ICT manufacturers: Anti-Spyware Coalition defines spyware and adware

The Anti-Spyware Coalition (ASC) founded in April 2005 began its work in the second half of 2005 and in just a few months achieved a joint definition for the previously vague terms →spyware and →adware.

ASC, founded by the Center for Democracy and Technology, includes some of the largest software and hardware manufacturers and interest group associations: America Online (AOL), Computer Associates, Hewlett-Packard, Microsoft, Yahoo, McAfee, Symantec, Trend Micro, the Canadian Internet Policy and Public Interest Clinic, the Cyber Security Industry Alliance, and the National Center for Victims of Crime. At the beginning of July, ASC published a draft spyware definition and sample solutions for combating the problem, and it invited comments and criticism from the public. Already at the end of October, ASC presented a final document that undertakes a spyware definition and a risk model document (still under development) that discusses in detail the technical differences between spyware and other software.

The goal of these efforts is to compile a common set of best practices, with which the discovery and removal of spyware can be accomplished more efficiently. Further objectives are to develop better anti-spyware products and better conditions for the sensitization of the end user. In any event, Symantec has already begun incorporating the ASC definition into its products.[34]

[34] The ASC documents are available at: http://www.antispywarecoalition.org/documents/index.htm (as of: 1 Feb 2006). See also chapter 10.

8 Legal foundations

Federal Council prevents revision of online consumer protection legislation

The turnover for internet orders around Christmas in Germany grew by a two-digit amount over the preceding year. In Switzerland, the increase is likely to be about the same. Since more and more orders are processed over the internet, the call for new regulation and legislation is getting louder.

The Federal Council refused to adopt a seven-day cancellation right for online purchases and stock transactions with banks and therefore is not harmonizing the legal situation with consumer protection in the EU. The draft legislative revision also provided that a buyer could demand the remedy of a deficient delivery. The complaint period was to be doubled to two years in this regard. The rejection of the legislative revision was justified with the explanation that it is not the State's role to force regulations on business that can also be negotiated voluntarily. The Federal Council found that, even without a legislative cancellation right for remote purchases, electronic business transactions had developed positively in Switzerland. In contrast, the consumer protection foundation expressed its disappointment that the Federal Council decided against a regulation. It believes that online customers continue to be exposed to risks on the web without protection.

Legal foundations for Voice over IP (VoIP)

Internet telephony (→VoIP) continues to boom, while the legal framework for emergency calls and reachability have not yet been clarified.

VoIP is a service that allows subscribers to operate a fixed line telephone not only through a telephone line specified in advance, but instead via any kind of internet access. This allows the user to make phone calls with the same phone number from any location, whether or not the location has been defined in the subscription.

While locations are transmitted in the case of mobile phones, there is no such standard for VoIP. For wireless connections, the IP address of the hotspot can be used to simply determine the access point and, using the new technologies described in chapter 6.2, the user's precise location can even be identified. With VoIP services via cable, however, it is very difficult to determine the location. For instance, several different IP address can be made available to a single modem (dynamic IP addresses). In such cases, it is very difficult or even impossible to determine the location.

In technical terms, it appears that the guarantee of article 28 of the Ordinance on Telecommunications Services (access to the closest emergency services and simultaneous determination of the location of the callers) cannot be guaranteed with the VoIP services. This situation is expected to be taken into account by the new draft article 87b of the Ordinance. In the case of VoIP, the guarantee of article 28 of the Ordinance only covers the scenario in which VoIP calls originate from the location that is given as the main location in the subscription contract. In all other scenarios, correct route handling and identification of the caller's location cannot be ensured for technical reasons.

9 Statistics

Switzerland: Fewer investments in IT security

According to a study by Swiss Infosec[35], 29% of companies invested less in security in 2005, 52% spent about the same amount to secure their data, and 19% indicated their willingness to invest more. These figures indicate that IT officers are forced to set priorities with respect to security questions.

Another problem is that the distribution of these investments depends on the size of the company. While larger companies appear to be well-prepared against IT attacks, small companies often save on IT security, claiming that the probability of an attack is smaller. Especially in years with high cost pressure, savings are made where the consequences are not directly apparent.

Switzerland: Economic effect of an internet blackout

A study by the Computer Engineering and Networks Laboratory (TIK) of the ETH[36] shows that the economic losses of an internet blackout cannot be ignored. According to the study, the financial loss of a one-week total failure of the internet in Switzerland, with a GDP of 482 billion (thousand million) Swiss francs, would amount to 5.83 billion francs. The ETH study identified particular problems with large-scale attacks using pests or →denial-of-service attacks.

This study shows how dependent a modern society such as Switzerland has become on IT infrastructure and the internet. 48% of the 3.6 million jobs in Switzerland are heavily dependent on IT. A business example calculates that a one-day breakdown of an internet service provider (ISP) with annual profits of 2.81 billion francs would lose 1.2% of these profits. The costs are composed of losses arising from non-availability of the IT infrastructure, repair costs, liability costs, and customer costs. If the IT structures in Switzerland would break down for one week, the ETH study claims that all institutions and users depending on the IT structures would be affected. According to the study, only 60% of the persons relying on IT infrastructure for their work would be affected by a one-day blackout; accordingly, the costs – recalculated to one day – that would arise in the first 24 hours after an attack would be lower than if the breakdown were to last seven days.

The ETH researchers believe it is conceivable that companies working with the internet could become the target of massive attacks in the form of malicious programs – malware – and DDoS attacks. Many of these companies are not aware to what extent they depend on IT networks, and what the financial losses would be if these networks were to fail. Many risk management studies do not even taken into account the failure of internet infrastructures.

[35] http://www.infosec.ch (as of: 8 Feb 2006).

[36] http://www.ethz.ch (as of: 8 Feb 2006).

10 Miscellaneous

Sony employs rootkits to preserve digital rights and creates security problems

At the end of October, an IT security expert warned that Sony BMG was using software called XCP developed by First 4 Internet on some of its music CDs protected by Digital Rights Management (DRM); using →rootkit-like techniques, XCP concealed itself and created security holes on the computer playing the CD. The software could neither be uninstalled, nor was it mentioned in the terms of the license displayed when inserting the affected CD. XCP not only conceals its own files and processes, but also everything whose name begins with sys - accordingly also →malware smuggled in by hackers. By the middle of December, most anti-virus and anti-spyware programs recognized the XCP rootkit and offered to remove it.

It also became known the middle of November that the recording software installed together with the XCP rootkit also "phoned home" and, without the knowledge of the user, transmitted data to Sony. First indications then began to surface that the first pests had already been circulated, concealing themselves with the help of XCP techniques on the infected computer. The middle of November, another DRM program by Sony called MediaMax (developed by SunnComm) was also exposed as spyware that allowed uncontrolled downloading of additional data, could not be uninstalled, and transmitted information to Sony. MediaMax also allowed attackers to obtain control over the computer, despite limited rights.

The middle of November, Sony recalled the CDs with XCP-DRM protection that had not yet been sold and apologized to its customers. Sony also announced that about 50 music albums had been fitted with the rootkit, a total of about 50 million CDs. Meanwhile, class actions had been filed by the Electronic Frontier Foundation, EFF (in the U.S. and Italy) and by the justice authorities of the U.S. State of Texas, while prosecutors in New York, Illinois, and Massachusetts had initiated investigations against Sony, since the affected CDs were still available for purchase. Sony's gaffe now also threatens to entail massive compensation for damages.

As became known in December, Sony BMG had already been notified by F-Secure in September about the damaging functions of XCP, but it decided to adopt a damage limitation strategy: maintain silence and secretly remedy the security risks in an update in 2006. Nevertheless, the company decided to revise its DRM strategy the middle of December and apologized to its customers at the beginning of 2006. Sony already was able to settle with the American EFF the beginning of 2006. Other class actions are still pending in California and Italy, however, and the criminal proceedings in Texas have not yet been concluded. The attorneys general of New York, Florida, and Illinois are continuing to investigate.

The dissemination of the XCP rootkit was apparently widespread, as a security consultant announced the beginning of January. He searched the →Domain Name System (DNS) for entries for the URLs via which XCP "phoned home" and determined that over 500,000 networks with an unknown number of workstations, including networks of the U.S. military and other government authorities, had been affected.

As this incident shows, the music industry – which is being criticized for its aggressive crackdown on filesharers – also uses dishonest methods. Sony's approach raises a fundamental question on the topic of spyware / adware: What exactly is spyware, and when is its use illegal? Is installation without the knowledge of the user already sufficient to qualify as spyware, or are damaging functions necessary? Must software always offer an uninstall option, or are there compelling security considerations that justify concealment of the software? The efforts of the Anti-Spyware Coalition (see 7.2) are therefore necessary to define clear rules for dealing with this new kind of software. The Anti-Spyware Coalition believes that software qualifies as spyware if installations take place without the consent of the user, if the installation of the software endangers privacy or system security, or if data is collected without the consent of the user. The question remains open whether serious providers will view this definition as binding or not. For Sony, in any event, this episode is likely to have serious consequences, as Spiegel Online commented: "Never before has a representative of the 'piracy is theft' faction had to slink off with its tail between its legs quite like this."[37]

[37] Quote: http://www.spiegel.de/netzwelt/technologie/0,1518,387480,00.html (as of: 6 Feb 2006).

11. Glossary

This glossary contains all the expressions marked with a „→". A more extensive glossary containing even more expressions can be found at:
http://www.melani.admin.ch/glossar/index.html?lang=en.

Active Scripting (ActiveX)	A technology developed by Microsoft to download small applications, so-called ActiveX controls, to the client's computer from where they run when web pages are viewed. They enable different effects and functions to be carried out. Unfortunately this technology is often abused and represents a security risk. For example, dialers are downloaded through ActiveX to the computer and run. ActiveX problems only concern Internet Explorer because the other browsers do not support this technology.
Adware	The term "Adware" is a contraction of the words "advertising" and "software". It is difficult to draw a clear distinction between →Spyware and Adware. Adware is often used for advertising purposes, by recording the user's surfing habits and offering the corresponding products (e.g. through links). Spyware and Adware usually reach the computer via downloaded programs.
Bluetooth	A technology for wireless communication between two terminals and which is mainly used in mobile phones, laptops, PDAs and input devices (e.g. computer mouse).
Bot / Malicious Bot	Comes from the Slavic word for work (Robota). Refers to a program, which, after being received, carries out certain commands autonomously. Bots are used mainly in the →IRC sector for administration purposes (e.g. user administration, automatic user lockout, etc.). Recently, however, this principle was also misused by attackers. So-called malicious bots are able to remotely control compromised systems and cause them to carry out arbitrary activities (sending spam, →DoS attacks, installation of additional programs such as →keyloggers, etc.).
Botnet	A collection of computers infected with malicious →bots. These can be fully remotely controlled by the attacker (the owner of the botnet). Depending on its size, a botnet may consist of several hundred to millions of compromised computers.
Browser-Plug-In	Software, which provides web browsers with additional functions, e.g. so as to show multimedia content.
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.
Critical Infrastructure Protection / Critical Information Infrastructure Protection (CIP / CIIP)	Important component in national security policies and defence planning. Generic term to describe concepts and strategies to protect →critical infrastructures / critical information infrastructures.
Critical (national) infrastructure	Infrastructure or part of the economy whose failure or breakdown would have enormous consequences on national security or the economic and/or social welfare of a nation. In Switzerland the following infrastructure has been defined as critical: energy and water supply, emergency and rescue services, telecommunications, transport and

	traffic, communications, banks and insurance, government and public administration. In the information age their smooth running is increasingly dependent upon information and communication systems. Systems such as these are referred to as critical information infrastructures.
Digital certificate	Verifies the affiliation of a public key to a topic (person or 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. A popular variant of DoS attacks in the IT sector is to send huge numbers of requests to a computer/service. Due to the flood of requests, the computer/service becomes so overloaded that a great deal of time is needed to respond or it even crashes.
DDoS attacks	Distributed denial of service attacks A →DoS attack where the victim is simultaneously attacked by many different systems.
DNS	Domain name system Computers connected to the internet communicate via the internet protocol standard (IP) and to this end have an →IP-address (e.g. 162.23.39.56). 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).
Exploit-Code	(or exploit) A program, a script or a line of code with which vulnerabilities in a computer system can be used to advantage.
Firewall	A firewall protects computer systems by monitoring incoming and outgoing connections and rejecting them if necessary. It is comparable with a sentry at a castle gate. The decision to accept or reject a connection is based on simple rules that are checked each time a new connection is established. Firewalls reduce the risk of unauthorised access by hackers and the threat of →Trojan horses, →spyware and →worms. Most companies protect their networks with a powerful firewall installed on a dedicated computer placed between the Internet and the local network. 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.
Host	This was used and is still used in IT to refer mainly to computers with vast computing power (banking). Today, however, this also refers to smaller computer systems (computers of private users, web servers etc.).
Hosts-File	File, in which computer names are assigned to →IP addresses. This file is to be found on every computer and is used first, as a rule, when locating the computer name/IP address (even before the →DNS).
IDS	Intrusion Detection System System with which unauthorised access to data or computers can be detected.
Instant-Messaging (IM)	Chat is a form of communication with other people on the Internet in real-time. Unlike a telephone conversation, however, the discussion does not take place with speech but by typing messages. Depending on the subject, there are different so-called chat rooms (also called channels) available. A user can either chat to all participants in the chat room simultaneously or move with another user to a private room not accessible to others. Many chat platforms on the Internet can be used

	free of charge. A similar form of communication is offered by the instant messaging services (e.g. AOL, MSN, ICQ and Yahoo) with which millions of users all over the world are registered.
Internet Protocol (IP) / IP-Adresse	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 130.92.3.15).
IRC	Internet relay chat A form of →instant messaging (IM) protocol.
Keylogging-Software (Keylogger)	Devices or programmes in operation between the computer and the keyboard to record keystrokes. These are stored in a file on the computer or are sent to a server via the internet. Keylogger software is often a component of →Trojan horses.
Malware	Comes from the terms "malicious" and "software". Generic term for software which carries out harmful functions on a computer. This comprises amongst others →viruses, →worms, →Trojan horses.
MITM	Man-in-the-middle attacks (MITM) Attacks in which the attacker infiltrates unnoticed the communication channel between two partners and is thereby able to spy on or even modify their data exchanges.
Mass e-mail virus	→Malware which is spread by sending e-mails. The term "e-mail worm" is often used for this.
P2P	Peer to peer Network architecture in which those systems involved can carry out similar functions (in contrast to client-server architecture). P2P is often used for exchanging data.
Pharming	Manipulation of name resolution via →DNS or via local configuration (e.g. →hosts-file) with the aim of redirecting users to false servers so as to gain access to confidential data (login data).
Phishing	The word Phishing is a contraction of the words "Password", "Harvesting" and "Fishing". 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.
PKI	Public Key Infrastructure Infrastructure for the management and use of →digital certificates.
PoC	Brief, not necessarily complete proof that an idea or method works. For example, →exploit codes are often published as PoC so as to underline the effects of a weak point.
Proxyserver	Often used as a synonym for HTTP proxy. A system which accepts and forwards browser requests. It is used, amongst other things, for speeding up similar requests, examining contents and for gaining anonymity.
Redirect	Used mostly in connection with websites when the surfer is automatically redirected to another website.
Rootkit	A collection of programs and technologies which allow unnoticed access to and control of a computer to occur.
SCADA Systems	Supervisory Control And Data Acquisition Systems. Are used for monitoring and controlling technical processes (e.g. in

	energy and water supply).
SIP	Session Initiation Protocol Protocol suite standardised by the IETF for →VoIP and other communication technologies.
Social Engineering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order to gain access to confidential data or to prompt them to perform certain actions, for example. Of all the forms of attack, this is still one of the most successful. An attacker can use social engineering, for example, to gain access to the user names and passwords of company staff by pretending to be a system administrator or manager on the phone. By alleging to acute computer problems and showing knowledge of the business (e.g. supervisor's name, work flows, etc) the victim is unnerved until he/she discloses the desired information. Social engineering methods are often used to spread →viruses and →Trojan horses, e.g. if the name of an e-mail attachment with a virus promises a particularly interesting content (e.g. "I love you", "Anna Kournikova", etc.). →Phishing is also a special form of social engineering attack.
Spear Phishing	Targeted →phishing attacks. The victim is made to believe that he/she is communicating via e-mail with a person they are acquainted with. In this way, the victim is mislead into sending data to the attacker or into installing programs. The personal environment of the victim is the first to find out about this.
Spyware	The term "Spyware" is a contraction of the words "spy" and "software". Spyware collects information about the user's surfing habits or system configuration without his knowledge and transmits it to a predefined address. The information selected depends on the Spyware and can include anything from surfing habits to passwords. It is difficult to draw a clear distinction between Spyware and →Adware. Spyware and Adware usually reach the computer via downloaded programs.
Trojan horse	Trojan horses (often referred to as Trojans) are programs that covertly perform harmful actions while disguised as a useful application or file. Trojan horses are often programs downloaded from the Internet. However, sound and movie files (e.g. in the common MP3 or MPEG format) can also be Trojan horses. They use security holes in the corresponding player programs (e.g. Media Player) to install themselves covertly. Trojan horses are also often distributed via e-mail attachments.
Virus	A virus consists of program instructions that tell the computer to perform certain actions. In order to spread, the virus attaches itself to a "host application". The "host application" may be an application (e.g. downloaded software) or a document (e.g. a Word file, Excel file). When the application is executed or the document is opened the virus is activated, causing the computer to perform harmful actions. Viruses often infect a computer via e-mail attachments or downloaded files from the Internet. Once activated, they may spread via e-mail to contacts in the address book. External data storage devices are further means of distribution (e.g. CD-ROMs, USB memory sticks, etc).
VoIP	Voice over IP. Telephony via internet protocol (IP). Frequently used protocols: H.323 and →SIP.
Wired Equivalent Privacy (WEP)	An encryption procedure used in →WLAN connections. Encrypt your wireless LAN connections if possible with →WPA2, failing this use

	→WPA, or use WEP if nothing else is available.
WiFi Protected Access (WPA)	Improved encryption method used in wireless LAN (→WLAN) connections after →WEP proved to be insecure. Encrypt your wireless LAN connections if possible with WPA2, failing this use WPA, or use WEP if nothing else is available. Both the WLAN access point and the network card in the PC must be WPA compatible. WPA2: New security standard for Wireless-LANs (→WLAN) in accordance with IEEE 802.11i specification. Successor to the WPA technique and to the →WEP technique considered to be insecure. If at all possible always use WPA2, failing this WPA or if nothing else is available WEP.
Wireless Local Area Network (WLAN)	WLAN stands for Wireless Local Area Network. In a WLAN the device (e.g. a laptop, PDA, etc.) communicates via a wireless connection with a WLAN Access Point which is connected (just like a normal computer) via a cable to the Internet or the local network. As the devices are not wired up the users are mobile. This is the advantage of a WLAN. The indoor range depends on structural factors and is considerably lower than outdoors, where WLAN connections are possible over more than 200 metres.
Worm	Worms, like →viruses, are programs that instruct the computer to perform certain actions. In contrast to viruses, however, worms to not require a host program in order to spread. Instead, they use security holes or configuration errors in operating systems or applications in order to spread by themselves from one computer to the next. Computers that have security holes or configuration errors and are connected to other computers (e.g. via the Internet, the local network, etc) are possible targets for worms.
0-day-exploit	→An exploit which appears on the same day as the security holes are made public.