INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2005-0685

Study on Security Countermeasures on Commercial Sites

April 2006

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

SIT

Fraunhofer Institut
Sichere Informations-
Technologie

Rheinstraße 75
64295 Darmstadt (Germany)
Phone +49 (0)6151 / 869-701
Fax +49 (0)6151 / 869-704
http://www.sit.fraunhofer.de

Management Summary

This document provides a study on security countermeasures particularly with regard to commercial sites in the European Union.

Some basic concepts are described that are important to information on the Internet. It gives an overview about the documents' purpose and its structure.

Three basic security concepts important to information on the Internet are confidentiality, integrity, and availability; or relating to Internet users authentication, authorization, and non-repudiation. Other basic concepts are privacy, anonymity, and pseudonymity.

The document starts with Internet vulnerabilities that allow attackers to violate confidentiality, integrity, and the availability of services. Internet vulnerabilities are originated in the history of the Internet. Its design was geared to the needs of researchers, but not to today's commercial and government use.

The document discusses in detail the technical aspects of threats and possible countermeasures. By means of empirically collected and statistically evaluated data trends are pointed out.

Some recommendations are given to secure commercial web sites and to make them more attractive for consumers.

The document considers theoretical aspects and the legal situation as well as organizational measures like organizations, agencies, initiatives, and enterprises dealing with Internet security and data protection.

Table of Contents

1 Introduction

This document provides a study on security countermeasures particularly with regard to commercial sites in the European Union.

1.1 Document Purpose

The increasing use of the Internet for commercial operations requires increasing information security, privacy, and data protection.

Starting from Internet vulnerabilities this study takes an inventory of possible threats and effective countermeasures. Both service providers and users will be considered thereby.

Special examples demonstrate the organizational and quality assurance supporting measures which are taken in Europe and its member states, particularly with regard to Germany, the United Kingdom, and France. The legal situation will be addressed shortly.

The study will be completed by outlining trends and developments of Internet threats and countermeasures.

1.2 Basic Security Concepts

Three basic security concepts important to information on the Internet are confidentiality, integrity, and availability; or relating to Internet users authentication, authorization, and non-repudiation. Other basic concepts are privacy, anonymity, and pseudonymity.

Confidentiality

Confidentiality means that information only should be read or copied by someone who is authorized to do so. The loss of confidentiality is a very serious incident for various applications especially in a commercial context. Examples are the transfer of credit card numbers in business transactions, or the importance to protect research data, new product specifications, and investment strategies. Just as well data has to be protected in a medical context. In a lot of coherences there are legal obligations to protect the privacy of individuals. For example for banks or loan companies that extend credit to their customers, or for individuals that offer services such as psychological consulting or drug treatment.

Integrity

Integrity means that information has to be protected from unauthorized changes when it is available on an insecure network.

Modification of information in unexpected ways is known as loss of integrity. Integrity is important both in a commercial context like Internet shopping and for critical safety like air traffic control.

Availability

Availability means that information that people are authorized to get has to be available for them. When information is erased or become inaccessible, loss of availability has happened. Availability is very important in businesses depending on timeliness of information or selling goods via Internet. A Denial of Service (DoS) is an incident where users cannot get access to a network or specific network services.

To protect information and make it available to people that are authorized to use it, organizations dispose authentication and authorization.

Authentication

Authentication means identifying a person or an object by a unique characteristic. Checking a user's identity may involve something the user knows, such as a password, the user holds, such as a smartcard or another token, or a personal characteristic, such as a fingerprint. To identify objects like web (World Wide Web / www / web) servers or like access points simple cryptographic methods are used.

Authorization

Authorization means to determine whether a particular user, group of users, or computer system is/are allowed to access definite information or to perform a certain activity, whereby the decision depends on defined access roles.

Non-repudiation

Non-repudiation means to provide strong security measures. Security is strong, when a user or computer system cannot later deny definite information access or performance of a certain activity.

Privacy and Anonymity

To prevent fraudulent use of personal data it must be possible to encrypt them, for example to protect passwords or private information, or to make them anonymous, for example to prevent user profile generation in the course of Internet shopping. These measures are required to ensure privacy and anonymity.

1.3 Document Structure

Chapter two lists potential categories of vulnerabilities of web sites.

Chapter three describes web principles and possible threats and countermeasures, and point up some trends and recommendations.

Chapter four discusses various measures taken in Europe and its member states, beginning with the legal situation and introducing organizations, agencies, initiatives, and enterprises dealing with Internet security and data protection.

Chapter five gives a short conclusion and outlines trends and developments of Internet threats and countermeasures.

Chapter six lists the references used in this document except of the HTML-references given in chapter 4.

Chapter seven (Appendix) explains abbreviations and acronyms used in the document. It lists the figures contained in this document.

2 Internet Vulnerabilities

Vulnerability is a weakness that a person can exploit to come up to something that is not authorized or intended as a legitimate use of Internet services. When vulnerability is exploited to compromise the security of a network, the result is a security incident (see “Security of the Internet” [INet-Security]).

ARPANET

The Internet began in the earlier seventies as the ARPANET (Advanced Research Projects Agency Net), a project funded by the U.S. Department of Defense. The ARPANET protocols (rules of syntax that enable computers to communicate via network) were originally designed for openness and flexibility, not for security. The design was geared to the needs of researchers, but not to today’s commercial and government use.

Protocols and Services

The ARPANET protocols IP (Internet Protocol), ICMP (Internet Control Message Protocol), TCP (Transport Control Protocol) are the base of today’s Internet protocols. Additionally, network services were developed that enabled a quiet convenient use of the Internet protocols. Examples are the Telnet service providing connection of terminals to remote hosts, the File Transfer Protocol, and various email services. The development of the platform independent graphic browser Mosaic and the representation of the Internet as World Wide Web leveraged the openness of the Internet for a widespread user circle and commercial and governmental applications. At the same time an abrupt rise in connected computers began. Over the period of 1999 to 2005 the number of Internet users rose from 286 to 964 million (see “Monitoring the Information Economy – 8th Factual Report” [TNS-INFRA]). Along with the convenience and easy access to information rose the risks. Those affected organizations include banks and financial companies, insurance companies, consultants, government agencies, hospitals and medical laboratories, network service providers, utility companies, universities and wholesale and retail trades as well as private users. Everyone has to be informed about Internet vulnerabilities because no central supervisory entity exists. A great part of threats could be fended or bounded by taking simple administrative measures or by using available software products.

2.1 Types of Technical and Conceptual Vulnerabilities

2.1.1 Flaws in Software and Protocol Designs

If a protocol has a fundamental design flaw, it is vulnerable to exploitation no matter how well it is implemented. If software is designed without integrating security as an original component but added it later on to the completed system, unexpected vulnerabilities may be present. Without taking additional measures traffic on the Internet is not authenticated, not confidential, and not of integrity.

The following examples will point up this.

Unprotected Transfer of Information

Unprotected transfer of IP addresses enables attackers to adopt foreign IP addresses (IP spoofing) and to use them for Denial of Service (DoS) attacks.

Source Routing Misuse of source routing information enables attackers to redirect packages and to spy confidential information like passwords.

Loss of Integrity Not to ensure data and information integrity enables attackers to manipulate data remaining undetected.

Absence of Authentication

Without taking additional measures authentication does not occur between interconnected computers, e.g. between clients and servers.

Absence of authentication enables attackers to masquerade themselves using foreign IP addresses (IP spoofing) or hostnames. Manipulating the mapping between IP addresses and hostnames (DNS spoofing) enables attackers to obtain by fraud unauthorized access to foreign hosts. Affected network services are for example. rlogin, NFS (Network File Service), or X-Windows.

Another type of attack is to create request packages searching for not-existent IP addresses, which are broadcasted in an interconnected network. This attack causes a network capacity overload (DoS attack).

Absence of Server Authentication

Server authentication is as important as client authentication. If a client sends a request to a Domain Name Server, Network File Server, or Network Information Server on an insecure way, e.g. without using a SSL/TLS (Secure Socket Layer / Transport Layer Security) -protected connection, an attacker may be enabled to masquerade himself. He may send back a prepared answer that enables him to access the clients system in a trusted manner, that is only simulated, or in an unnoticed manner.

Non-repudiation Particularly with regard to commercial applications it is important to add bilateral authentication mechanisms to interconnections. It is recommendable to sign and to record commercial transactions. These measures are required to ensure non-repudiation.

Misuse of Disposable Information

Disposable Information like host names, user accounts, or name and version of used operating systems, may be used by intruders to prepare an attack. Especially well-known ports may be attacked. As an example an attacker, who is masqueraded as a trusted port user, may spy password files on port 513, who is bound to the rlogin service.

2.1.2 Weaknesses in Protocol and Software Implementations

Programming faults are the most important reason for vulnerabilities (see: “Erkennung und Behandlung von Angriffen aus den Internet” [BSI-WebServ]). By exploiting program weaknesses, intruders at a remote site can gain access to a victim’s system. As a first step intruders try to fool a system (or user) to send them user and password information, or to take over an existing connection under a faked identity. In the following some examples for programming lacks are pointed up.

Pseudo-random Numbers

Predictability of counters, e.g. sequence numbers, may enable intruders to infiltrate their own packages into an existing connection. Counters should be created by a pseudo-random number generator.

Buffer Overflow Non-existent checking of data content and size may lead to buffer overflow attacks.

Intruders may exploit this vulnerability to infiltrate Trojan Horses or other kinds of malicious code like worms and viruses.
Or they cause a system crash and make web sites or services inaccessible to people that are authorized to use them.
Other examples of vulnerabilities that may cause a buffer overflow are

- race conditions in file access,
- incomplete checking of operating environment,
- inappropriate use of system calls, etc.

2.1.3 Weakness in System and Network Configurations

Configuration For making networks secure it is necessary to check the default settings of software and hardware components. System administrators or users may fail to change the defaults, or they may simply set up their system to operate in a comfortable but insecure way.

Insecure Network Services

If a secure computer is coupled with an open network, the risk will rise to become infected. Used network services may be configured in an insecure manner and may contain undetected program errors. To limit these type of risks, it is recommendable to activate only required services and to take local countermeasures, e.g. to use personal firewalls.

2.1.4 Flaws in Organizational Measures

Bad Credentials Often authentication is realized using passwords. To enhance security, it is better to use one-time passwords, particularly for critical applications like home banking and similar services.

Access Control To prevent fraudulent use it is important to protect information about net structures as well as passwords. This means physical access control measures to protect computer systems as well as controlling remote access to databases and system information.

2.2 Vulnerability Effects

The following three figures demonstrate the negative effects of Internet vulnerabilities. The information provided in Figure 1 to Figure 3 was taken from the “Online-study IT-Security 2004”, published on “InformationWeek Live” (see [IW-Live-Study]). Data were collected from April to June 2004 on the base of 842 answering IT- and Security-Managers from various countries, 693 from Germany. The following statistics have been generated on the base of 514 analyzable answers.

Figure 1 shows a ranking of type of attacks. Viruses, Worms and Trojan horses are still the most noticed attacks.

Figure 1: Type of Attacks

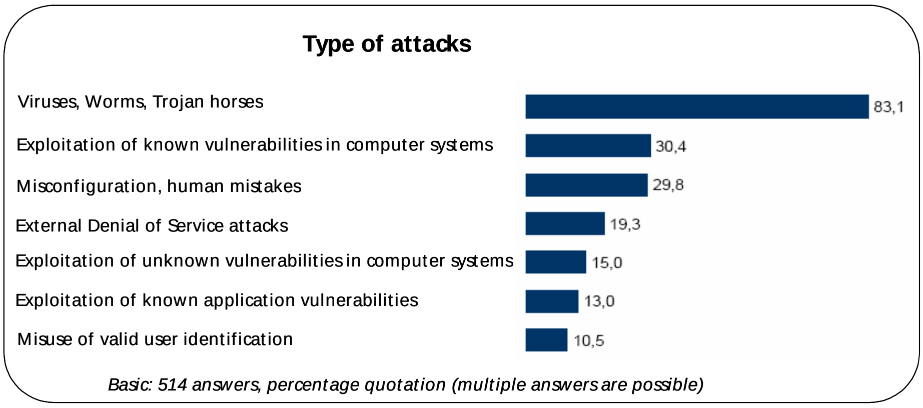
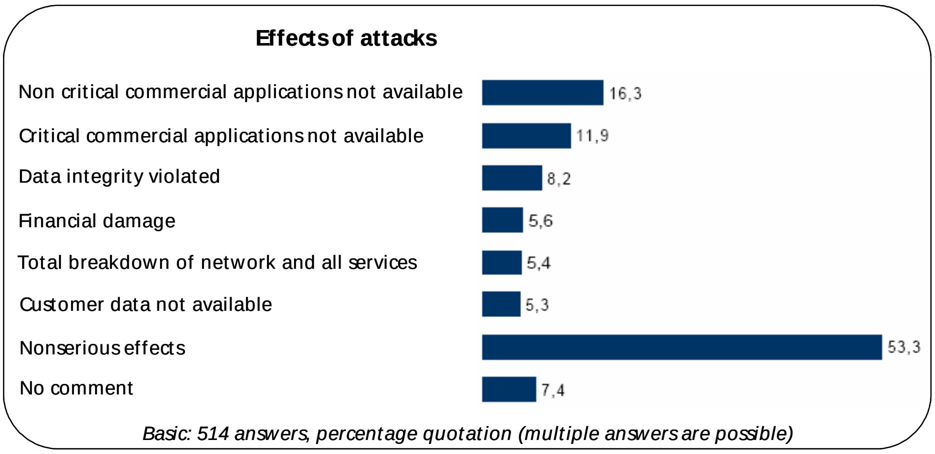


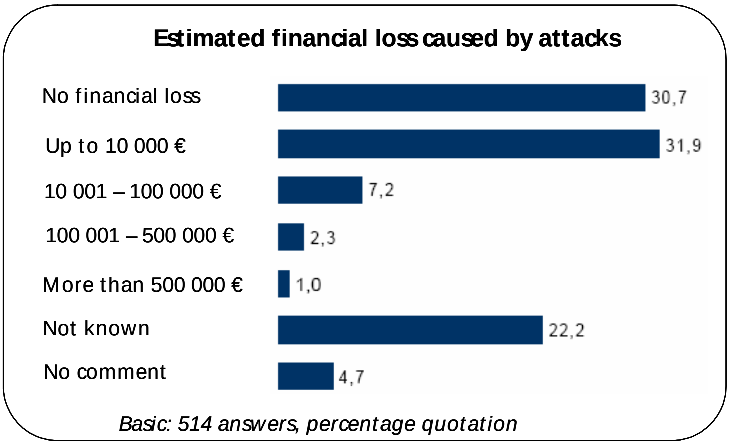
Figure 2 shows a percentage quotation of the effects being noticed. Non availability is the most quoted attack, both for non critical and for critical commercial applications.

Figure 2: Effects of Attacks



In Figure 3 the financial loss is estimated caused by attacks. This figure shows the highest rate of “unknown” answers.

Figure 3: Estimated Financial Loss Caused by Attacks



Basic: 514 answers, percentage quotation

3 Threats and Countermeasures

Security threats may result from the following attacks:

– from unauthorized reading of electronic messages, which may contain sensible personal or commercial data,
– from unauthorized modifications of data on its way to recipients,
– from erasing data or making information inaccessible for authorized people,
– or from simulating a trustworthy identity to communication partners with intent to obtain by fraud private and confidential information.

3.1 World Wide Web

3.1.1 Definitions and Security Principles

The World Wide Web integrates existing network services providing a consistent addressing and handling, and a standardized document format (see: "IT-Sicherheit – Konzepte, Verfahren und Protokolle" [IT-Sicherheit]). The World Wide Web comprises objects, servers, and browsers. Web objects may be documents or data collections, and web sites written in HTML (Hypertext Markup Language) and transferred by HTTP (Hypertext Transport Protocol). Web sites are multi media documents containing links to other documents or sites. They also may contain mobile and executable code. Web browsers represent the user interface of the World Wide Web providing services like navigation, file access and download, or interactive data exchange, e.g. login procedures on commercial sites. To transfer web objects from server to browser they have to be identified definitely. This is done by means of a URL (Uniform Resource Locator) or a URI (Uniform Resource Identification).

Web Security

Without taking additional measures the HTTP protocol doesn't provide authentication, data integrity, and privacy.

Absence of authentication enables attackers to masquerade server addresses and URLs. Absence of encryption enables attackers to intercept secret information like credit card numbers. Insufficient access control caused by configuration faults enables attackers to spy out and modify secret web server information. The ability to transfer executable code contained in Hypertext documents raises the probability of web server attacks leading to significant troubles with the availability of networks and sites.

Security Policies

A security policy is a document being concerned with a nontechnically oriented plan for organization-wide computer and information security. It provides guidelines for specific decisions, such as which defense mechanisms should be used and how to configure services. It builds the basis for developing secure programming guidelines and procedures that users and system administrators should follow (see "Security of the Internet" [INet-Security]). Security policies are especially important when a secure network (e.g. Intranet) is coupled with an open network environment (e.g. Internet).

A security policy may cover the following aspects:

- high-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy,
- risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss,
- guidelines for system administrators on how to manage systems,
- guidelines for access control rules for users and administrators,
- guidelines for reacting to a site compromise.

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users.

Technical options that support a security policy may include the following measures:

- challenge / response systems for authentication,
- auditing systems for accountability and event reconstruction,
- encryption systems for the confidential storage and transmission of data,
- network tools such as firewalls and proxy servers.

Relating RFCs

The requests for comments RFC 1244 "Site Security Handbook, July 1991" (see [RFC-1244]) / RFC 2196 "Site Security Handbook, September 1997" (see [RFC-2196]), and RFC 1281 "Guidelines for the Secure Operation of the Internet, November 1991" (see [RFC-1281]) are guidelines dealing with security policies. They are written by the Internet Engineering Task Force.

3.1.2 Threats and Countermeasures

Dynamic Code

Implementing the Common Gateway Interface (CGI) allows input form the user to be sent to an external program or script, processed there and the result given back to the user (see "The Open Web Application Security Project, A Guide to

Building Secure Web Applications and Web Services" [OWASP-Guide]). CGI is one example for processing dynamic information supplied by a user or a data store and giving the dynamic output back. This kind of processing is now common practice for web applications. CGI's lack of session management and authorization controls retarded the development of commercially useful web applications. To avoid buffer overflows or resource leaks, one of the most common security issues, web developers moved to interpreted scripting languages first, and then to Sun's J2EE web development platform or Microsoft's ASP.NET framework, depending on the used platform.

Mobile Code

Mobile code, respectively active contents, is downloaded from a server to a client machine and processed there. It is a threat on the client side whereas CGI scripts are processed on the server side and enables attackers to damage a server.

Server Side Includes

Dynamic HTML pages may be created in various ways, e.g. by server side includes. A client does not send executable code but commands identified by keywords like *exec* or *include* to a server side. The server executes the commands and creates a modified HTML page.

Countermeasures against Misuse of Dynamically Created Web Sites

To bind the risks of dynamically created web sites and to prevent common web attacks, such as replay, request forging, and man in the middle attacks, it is recommendable to add authentication and session control to client – server communication.

Cross Site Scripting

All dynamically created web sites are vulnerable to malicious code attacks caused by non proper validated user input. All clients accessing such a manipulated site are affected by cross site scripting because the malicious code is automatically executed if the according script language, e.g. JavaScript, is activated. A malicious attacker may use this to present new forms, fooling users to enter sensitive data. Unwanted advertising could be added to the site. Cookies can be read with JavaScript on most browsers and thus most session ids, leading to hijacked accounts.

As a countermeasure all characters that have special meaning to HTML has to be converted into HTML entities on server side. Only user input known as safe should be accepted, e.g. requesting a document only a valid file name should be accepted.

Caching

Logging of user access data may compromise users' privacy. Accessing a HTML site a user sends a lot of private and context information to a web server side. An example is the result of a search request. The search engine responds with a complete list of strikes. Combining this information with the user's IP address may enable providers to create a personal profile. Insufficient protection of cached user data may enable attackers to misuse foreign IP addresses.

As a countermeasure clients may use proxy servers to mask critical header data.

Auditing

Many industries are required by legal regulations to be auditable and traceable. That means to record all activities that affect user state or balances and to make it possible to determine when and where an activity took place.

Well-written applications should be able to easily track or identify potential fraud or anomalies of protected audit and error logs.

Cookies

To enhance the stateless HTML protocol, servers are enabled to store cookies on a user's side. Cookies do not contain executable code but information about users, domains, and session identifiers. They are critical to both privacy and security.

Setting cookies enables a server to collect data about users and to create a personal profile. Especially setting unnoticed cookies that are stored beyond session duration enables providers to send undesired advertisement or to sell personal data to other commercial dealers. Cookies enable attackers to infiltrate active contents that can be misused, leading to hijacked accounts, processing of malicious code, session replay attacks (see below), or unauthorized access to protected memory.

As a countermeasure non-persistent cookies should be used. When a session is closed by logging off a user or idle expiring, it should be ensured that the client side cookies are cleared as well as all server side session state information, e.g. in order to prevent session replay attacks.

Session Replay Attacks

Session replay attacks are simple if the attacker is in a position to record a session. The attacker will record the session between the client and the server and replay the client's part afterwards to successfully attack the server.

This type of attack only works if the authentication mechanism does not use random values to prevent this attack.

Exploitation of Trust

Computers interconnected with networks often have trust relationships with one another. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

Web Spoofing

Caused by the absence of authentication an attacker may masquerade a web server address and use it to present a manipulated web site to potential victims. Often masquerade of URLs is done by minimal changes of location identifiers. After spoofing the server address attackers are able to manipulate the web browsers status indication too, e.g. to simulate a SSL connection adding a faked icon to status band.

Phishing

These attacks are known as Phishing (password fishing). Delivery via web site, email or instant message, the attack asks users to click on a link to *re-validate* or *re-activate* their account. Attackers leverage the trust of well-known enterprises or public services to gain valuable information; usually details of accounts, or enough information to open accounts, obtain loans, or buy goods through e-commerce sites. Phishing attacks are one of the highest visibility problems for banking and e-commerce sites. Banks, Internet service providers (ISPs), stores and other Phishing targets are victimized as well as their (potential) customers.

To minimize the risk of Phishing providers should create a policy detailing exactly what they will do and will not do, and they should publish it on their web site. Because users are the primary attack target for Phishing attacks, providers should train their users to be wary of Phishing attempts. To ease validation of URLs a server should use hostnames and no IP addresses. Attackers will often ask users to provide their credit card number, password or PIN. Providers should tell their users that they will not ask them for secrets and to notify them if someone has done this. Providers should add authentication both to email clients and to client – server communication to make email communication safer.

Packet Sniffer

A packet sniffer is a program that captures critical data from information packets as they are transferred over the network. That data may include user names, passwords, and other secret information being transferred in clear text. Those captured data enable intruders to launch widespread attacks on networks and systems.

To be protected against sniffer programs data should be transferred encrypted.

Denial of Service

The goal of DoS attacks is not to gain unauthorized access to systems and data but to prevent legitimate users of services, e.g. customers of an Internet shop, for using them. DoS attacks may appear in various forms. Attackers may flood a network with large volumes of data or intentionally consume a lean or limited resource. They may disrupt physical components of a network or manipulate transferred data. Often so called *bot networks* are used to perform DoS attacks.

Countermeasures against DoS attacks depend on the form of the discovered attack. As an example attacks are performed by flooding a target with SYN (short for synchronization) requests using a forged IP address and without completing the initial request. In this case the potential for DoS attacks can be reduced by performing egress filtering on all outbound traffic looking for forged source addresses. In general only authenticated and authorized users should be allowed to take up significant CPU, disk space, and network resources.

Bot Networks

Bots (short for *robots*) are programs that are covertly installed on a user's computer in order to allow an unauthorized user to control the computer remotely. Bots are designed to let an attacker create a network of compromised computers known as a bot network, which can be remotely controlled to collectively conduct malicious activities.

Malicious Code

Malicious code is a general term for programs that, when executed, would cause undesired results on a system. The presence of malicious code usually is overlooked until the damage is discovered. Malicious code includes Trojan horses, viruses, and worms.

Other Damage Software

Also spyware that is intended to collect secret data such as usernames, passwords, banking information, and credit card details, and adware that is intended to collect personal data for profiling and undesired advertising, often are overlooked until the damage is discovered.

Countermeasures against Malicious Code and other Damage Software

To be protected against malicious code and other damage software it is recommendable for organizations and their staff members as well as private users to install firewalls, antivirus, and antispy software and to keep them up-to-date.

Support of Web Services

Administrators should keep patch levels up-to-date, especially on computers that host public services – such as HTTP, FTP, SMTP, and DNS servers – and are accessible through a firewall or placed in a demilitarized zone (DMZ).

3.2 Electronic Mail

Electronic Mail (email) is one of the most widespread Internet services. It provides the exchange of messages and data between one or more communication partners. The transfer is based on the Simple Mail Transfer Protocols (SMTP) or, as common today, the Internet Mail Extension Protocol (MIME) or the enhanced S/MIME (Secure MIME) Protocol.

Email Security

Without taking additional measures the email protocols do not provide authentication, data integrity, and privacy. Especially the addresser isn't verified electronically and it is easy to spoof email addresses by attackers.

To prevent profiling it is possible to use a so called *Remailer*, which makes the header information anonymous and is able to encrypt it. Common mail clients, like MS Outlook, Mozilla, or Netscape, provide security by enhancing certificate or key based authentication of addressers and encryption of email contents.

Spam

Spam is usually defined as junk or unsolicited email from a third party. While it is an annoyance to users and administrators, spam is also a serious security concern, as it can be used to deliver Trojans, viruses, and Phishing attempts. Furthermore, high volumes of spam can create denial of service conditions in which email systems are so overloaded that legitimate email and network traffic are unable to get through. Many spammers try to obscure their actual location. In an attempt to bypass blacklists, they build coordinated bot networks, allowing them to send spam from sites that are distant from their physical location.

During the first six months of 2005, spam world-wide made up approximately 61% of all email traffic. This is a slight increase over the last six months of 2004 when just over 60% of email was classified as spam. While the six-month average slightly increases, there is a month-to-month decline in the percentage of email that is spam between January 1st and June 30th. In January 2005, 67% of email was categorized as spam. By the end of June, this number had declined to 53% (see "Symantec Internet Security Threat Report, Volume VIII" [Sym-Threat-R]).

Despite of the high appearance of spam mails, anti spam measures aren't applied in all German enterprises and administrations. About 9% of them rest unprotected (see "Die Lage der IT-Sicherheit in Deutschland 2005" [BSI-Status-R])

Countermeasures

To minimize the volume of spam on their networks, it is recommendable that administrators implement IP filtering and traffic shaping. It is also recommendable that Internet service providers (ISPs) employ outbound filtering, which can significantly reduce the distribution of spam from compromised ISP accounts and bot networks. Port 25, the TCP port bound to SMTP mail, should only be unlocked for authorized network users. Administrators should also consider applying rate-limiting control in order to limit the ability of potential spam relays to send high volumes of email. Analysis of header information heads the list of anti spam measures in front of black and white lists, weighting bad or good addressers.

User Training

End users should be instructed to employ antivirus and antispy software and a personal firewall. They should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. They should never view, open, or execute any email attachment unless the attachment is expected and comes from a trusted source, and the purpose of the attachment is known.

Instructions may by given by public agencies, e.g. the Federal Office for Information Security (BSI) in Germany (see [BSI-En]), and private initiatives, e.g. "Deutschland sicher im Netz" (see [DsiN]), as well as enterprises introducing their staff members.

3.3 Trends

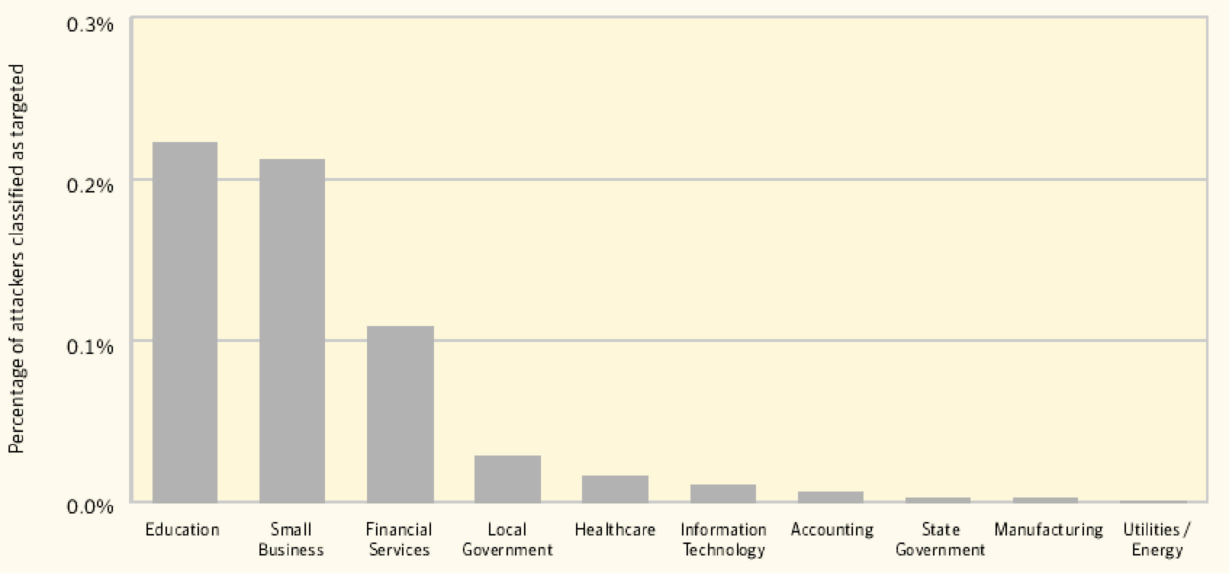
All Figures shown in this section are taken from the "Symantec Internet Security Threat Report – Volume VIII" (see [Sym-Threat-R]). Symantec has established a comprehensive test net consisting of more than 24,000 sensors monitoring network activity in over 180 countries. As well, Symantec gathers malicious code data along with spyware and adware reports from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products. Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec to scan global spam and phishing activity. Symantec is publishing its Internet Security Threat Report two times a year.

Who is targeted?

Attackers choose their targets for various reasons. Some attackers are simply opportunistic, randomly attacking vulnerable computers regardless of the owner or organizational membership of the target. Other attackers select their targets specifically in order to compromise computers within an organization or a specific industry. This metric explores attacks targeted at specific industries.

The third most frequently targeted industry between January 1st and June 30th, 2005 was financial services (see Figure 4). This industry is generally considered to be a popular target for attackers hoping to profit from their attacks. Corresponding to the growing of malicious code for profit attacks, targeted attacks against the financial services industry may increase as the focus of attackers.

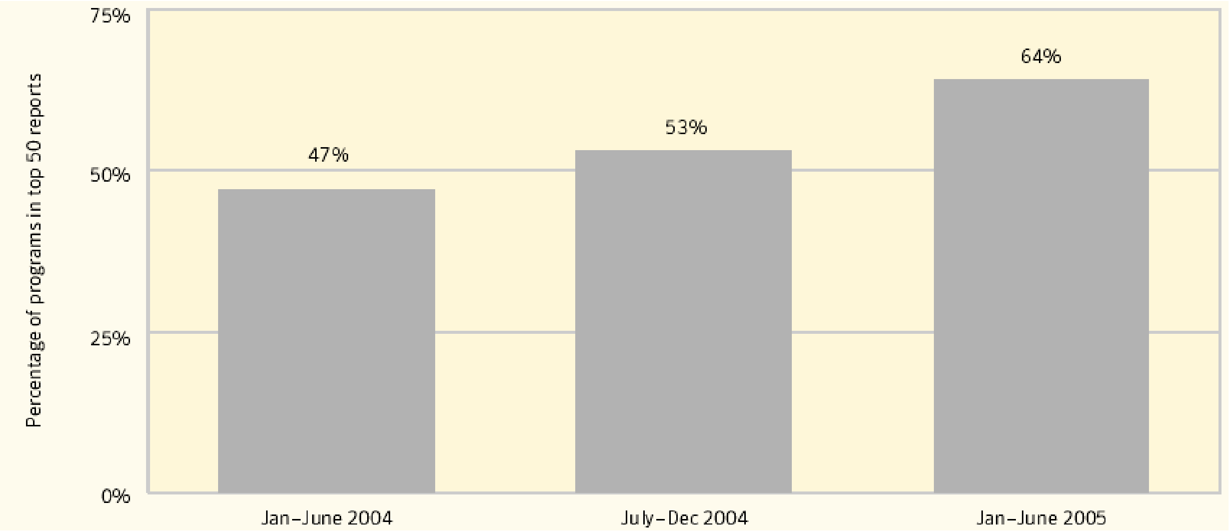
Figure 4: Targeted Attacks by Industry



Malicious Code for Profit

Malicious code that can be used to generate profit appears to be on the rise. That is mainly caused by the growing use of malicious code to wide spread unsolicited email (spam) for profit. In the first half of 2005, 64% of the top 50 malicious code samples reported to Symantec allowed email relaying, compared to 53% in the last six months of 2004 and 37% in the first half of the year (see Figure 5).

Figure 5: Malicious Code that Allows Email Relaying



An example for the growing use of malicious code for profit is the development of bot networks used to gain financial benefits. For further information see the clause *Bot Networks* below.

Other examples are the use of Trojan horses, e.g. to encrypt data files such as documents, spreadsheets, and database files. This Trojan creates a file in each folder on compromised computers containing information, how the user can obtain a decoder for the files with costs. Other Trojans download adware onto a compromised computer.

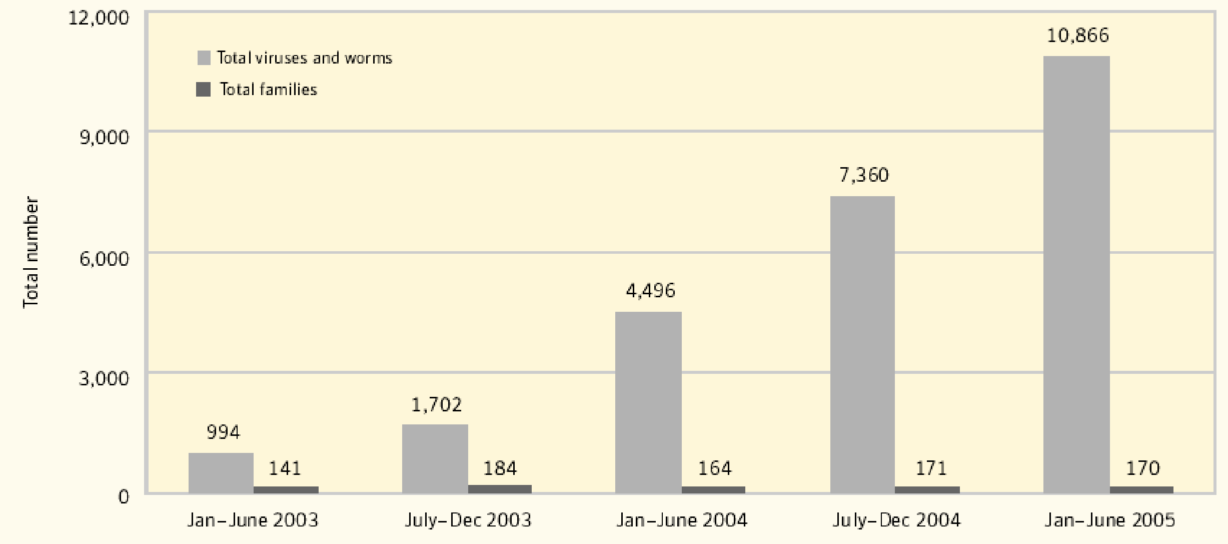
A really alarming trend is the use of malicious code for targeted Trojan attacks. Since attacks are targeted to a specific user or group of users, it is likely that social engineering will be used to argue users into running the Trojan application. To protect against these threats, users should always verify the authenticity of any application before running it on critical computers. Administrators should use firewalls and email gateway protection to prevent these threats from reaching end users.

For the future it can be expected that new forms of malicious code will be deployed by attackers, e.g. deployment of modular malicious code. Modular malicious code, once installed efforts to disable antivirus solutions and then download further functionality from different sources.

Malicious Code Variants

Malicious code can be classified in two categories: families and variants. A family is a new, distinct sample of malicious code. In some cases, a particular family of malicious code may have multiple variants. A variant is a new iteration of the same family, one that has minor differences but that is still based on the original. A new variant is often created when the source code of a successful virus or worm is modified slightly to bypass antivirus detection definitions developed for the original. The rapid rise in variants is important because each variant represents a new, distinct threat against which administrators must protect their systems.

Figure 6: New Win32 Virus and Worm Variants, 2003-2005



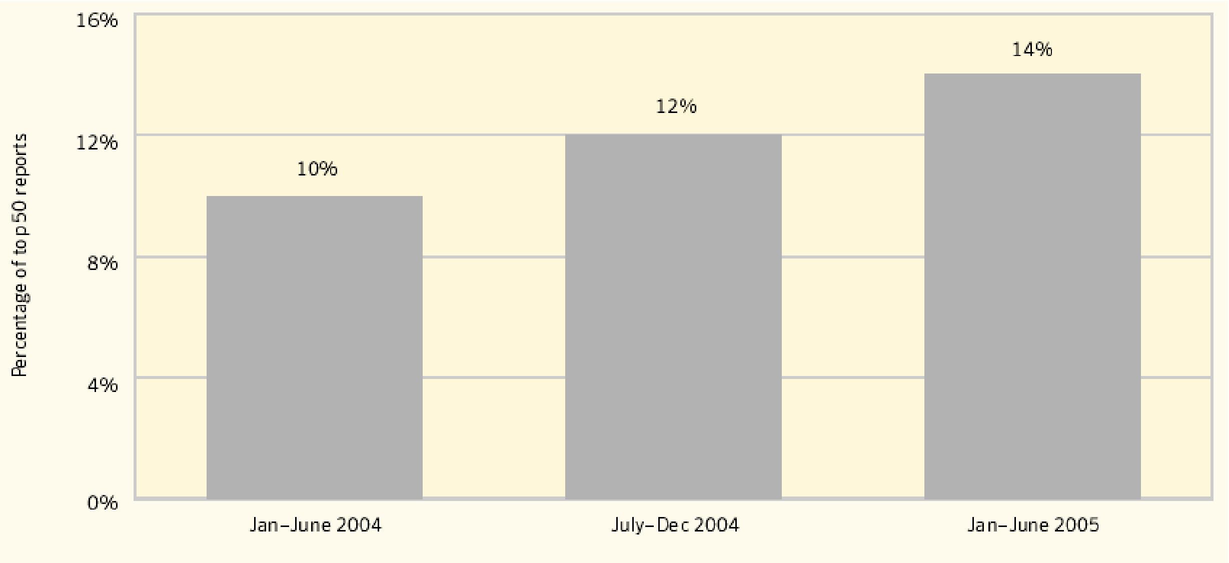
As an example see Figure 6, documenting the increase of Win32 viruses and worms. Win32 threats are executable programs that operate by using the WIN32 API. During the first six months of 2005, Win32 threats continued the increase in volume that was first noted in 2003. With the significant growth in Win32 viruses and worms, the number of new Win32 families could be expected to also show a notable increase, but this has not been the case. The number of new families reported has remained relatively level for the past five reporting periods, indicating that the huge majority of the new viruses and worms reported are variants of existing families.

Disclosure of Confidential Information

Threats that disclose confidential information from a compromised computer are a concern to all users, both in the home and enterprise environment. These threats may disclose system information, sensitive files and documents, or cached logon credentials. Some threats, such as back doors, may give a remote attacker complete control over a compromised computer. With the increasing use of online shopping and Internet banking, compromises of this type can result in significant financial loss, particularly if credit card information or banking details are disclosed.

During the first six months of 2005, threats with the potential to disclose confidential information continued to increase, as they have in the Year 2004 three reporting periods (see Figure 7).

Figure 7: Threats to Confidential Information



The rise in confidential information threats is primarily due to the dissemination of bots; however, other new threats also contributed to this trend, e.g. some kinds of mass-mailing worms that include remote access capabilities, which could allow remote attackers access to a compromised system and the data stored on it.

Bot Networks

One of the changes in the threat landscape is that it will likely be dominated by emerging threats like bot networks and that bot networks are available for hire. These can be used for malicious purposes, such as extorting money from e-commerce sites by threatening DoS attacks.

Bots can have various effects on an enterprise. A single infected host within a network, such as a laptop that was compromised outside the local network and then connected to the local network again, can allow a bot to disseminate to other computers that are normally protected against external attacks by corporate firewalls.

Symantec identifies bot networks by analyzing coordinated scanning and attack patterns. In the past six months bot network activity has increased to a median average of 10,352 unique bots identified per day (see Figure 8). This is an increase of over 138% from the average of 4,348 bots identified per day in December 2004. It may be supposed that this increase in bot network activity is a reaction to security implementations put in place in the last half of 2004.

Figure 8: Bot Network Computers

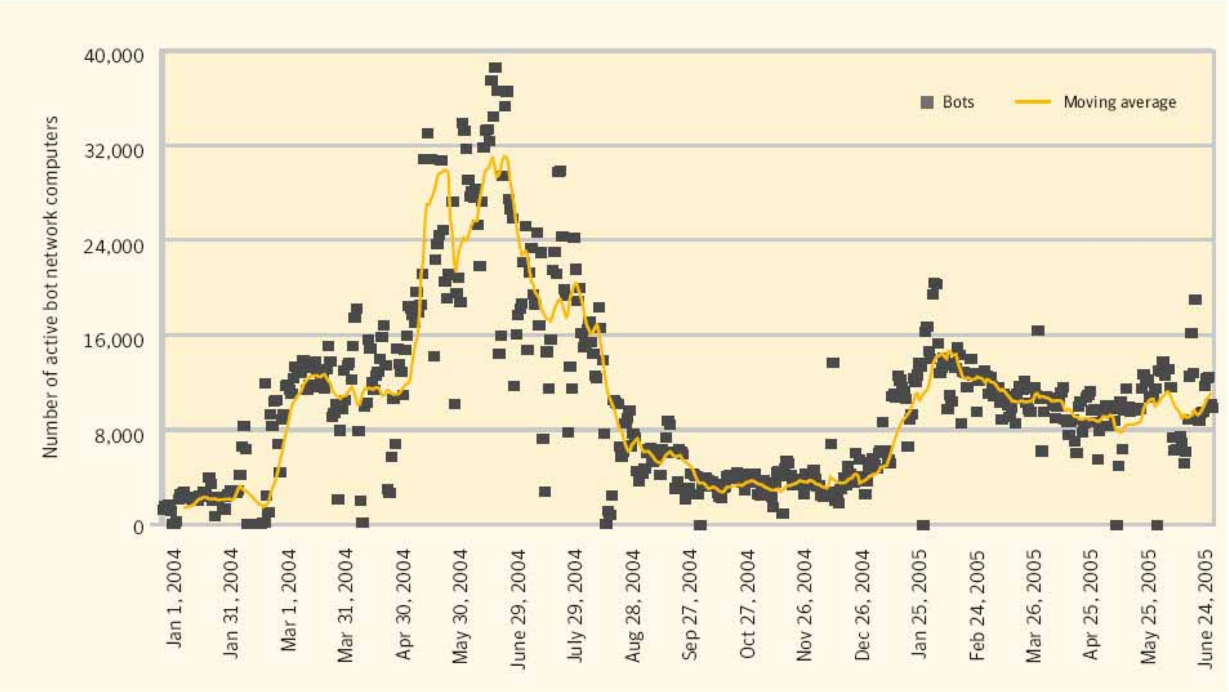
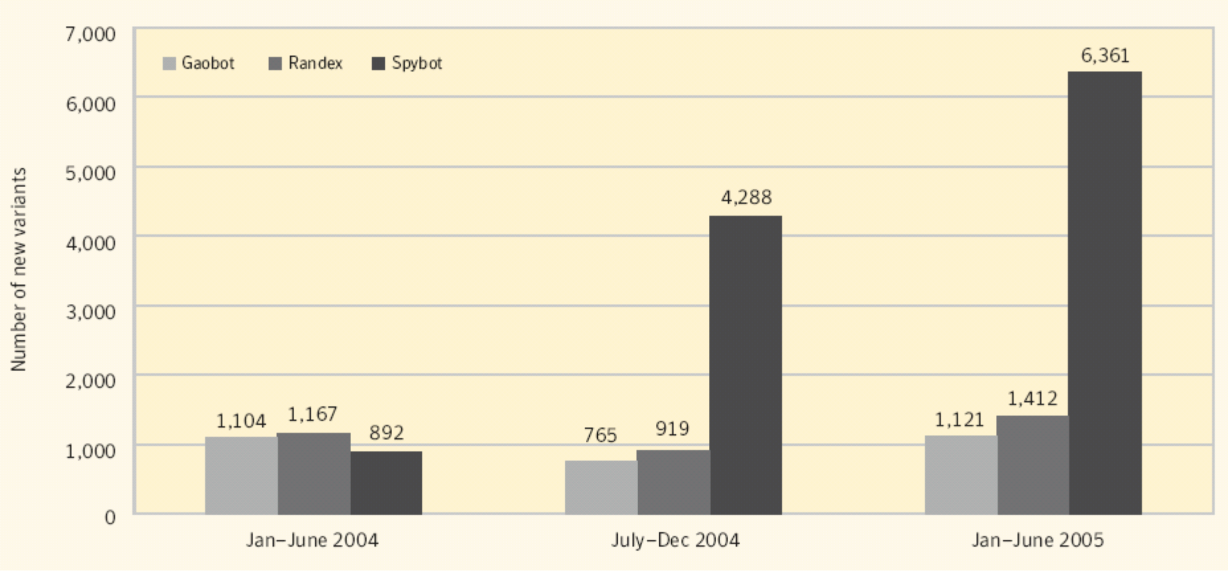


Figure 9: Number of New Bot Variants

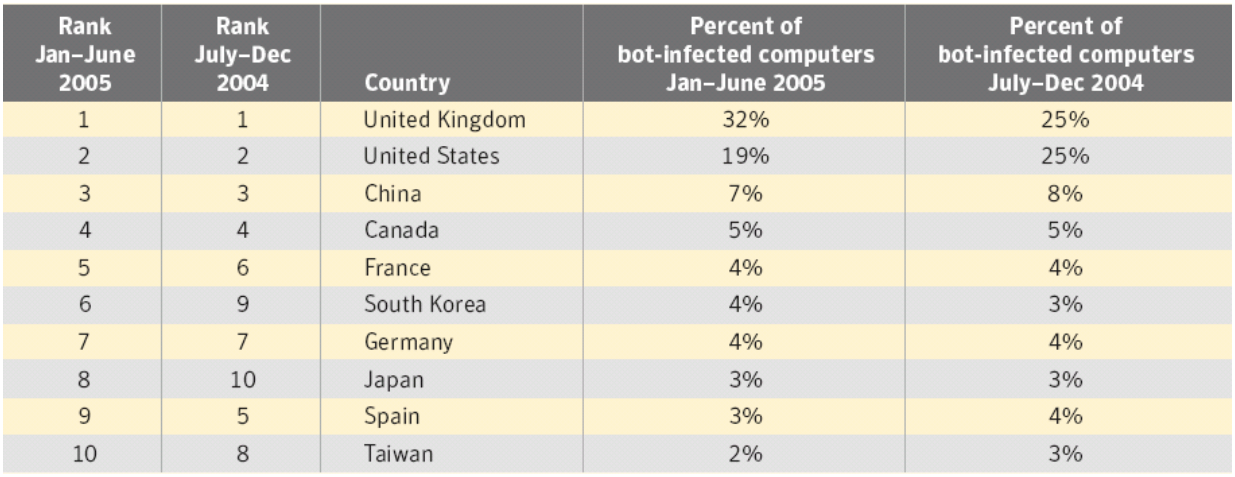


The number of new bot variants continues to go up (see Figure 9). The increase in variants is problematic for organizations because each one represents a new threat against which administrators must secure their systems and for which antivirus providers must develop and provide updates.

To prevent bot infections, it is recommendable to filter both incoming and outgoing traffic to block known bot network activities. Antivirus definitions should be updated regularly. All systems within an organization's network should be monitored for signs of bot infection, ensuring that any infections are detected and isolated as soon as possible. It is also recommendable to filter out potentially malicious email attachments to reduce disclosure to companies and end users.

Being aware of the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers worldwide, calculates the numbers of computers that are known to be infected with bots, and charges what percentage are situated in each country. During the first six months of 2005, the country with the highest proportion of bot-infected computers worldwide was the United Kingdom, with 32% (see Figure 10).

Figure 10: Top Countries by Percentage of Bot-infected Computers

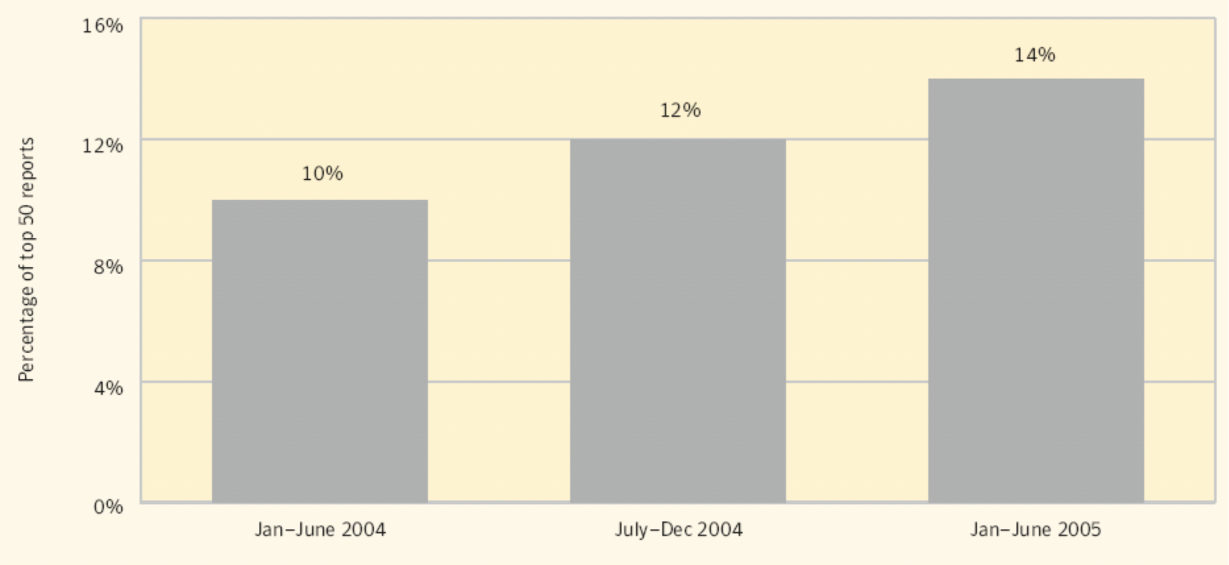


Rank Jan–June 2005	Rank July–Dec 2004	Country	Percent of bot-infected computers Jan–June 2005	Percent of bot-infected computers July–Dec 2004
1	1	United Kingdom	32%	25%
2	2	United States	19%	25%
3	3	China	7%	8%
4	4	Canada	5%	5%
5	6	France	4%	4%
6	9	South Korea	4%	3%
7	7	Germany	4%	4%
8	10	Japan	3%	3%
9	5	Spain	3%	4%
10	8	Taiwan	2%	3%

It could be observed that bots predominantly infect computers connected to high-speed, broadband Internet. It has also been observed that rapid expansion of broadband connectivity eases the spread of malicious software, including bots. This is likely due to the failure of security infrastructures in keeping up with rapid broadband growth.

In the first half of 2005, the percentage of bot-related malicious code reported to Symantec increased, accounting for 14% of the top 50 (see Figure 11).

Figure 11: Bots in Top 50 Malicious Code Reports



Bot networks that can be used for malicious purposes are available for hire. It is not uncommon for those who maintain control of these networks to provide full or partial access to the compromised systems for a nominal fee. Such a service is typically requested for purposes of profit or general malicious activity. In addition to offering access to an existing bot network, unique customized versions of a bot binary could supposedly be purchased. Vendors promise that such binaries are unique and would not be detected by current antivirus definitions. But while it is possible to create a unique bot binary to avoid detection by previous antivirus definitions, most antivirus products will be able to identify the threat using a generic definition or a heuristic signature.

It is expected that over the next year there will be a more coordinated community of bot network computers performing more sophisticated, targeted attacks. This may include the use of bot networks as a method of contaminating compromised networks with other types of malicious code, which could be used for spam, phishing, and theft of confidential information. As bot networks continue to emerge they may begin to employ more sophisticated methods to avoid detection, such as encryption, packing, and rootkits.

DoS Attacks

DoS attacks are a major threat to companies that rely on Internet connectivity to carry out their business and to earn their money by this means. They are typically performed by flooding a targeted computer with requests for data in order to slow or block legitimate access to services it provides. Fortunately, while the number of DoS attacks appears to have increased essentially, corresponding to the increasing use of bot networks, major companies have not experienced any notable impact from these efforts.

Although there are numerous methods for carrying out DoS attacks, Symantec derives the data for the metric shown in Figure 12 by measuring attacks performed by flooding a target with SYN (short for synchronization) requests. Often SYN requests with forged IP addresses are sent to a target, causing a single attacking computer to initiate multiple connections. The result is undesired traffic, so called *backscatter*, being sent to other computers on the Internet. This *backscatter* is used to derive the number of DoS attacks.

Figure 12: Median DoS Attacks per Day from 01/2004 to 06/2005

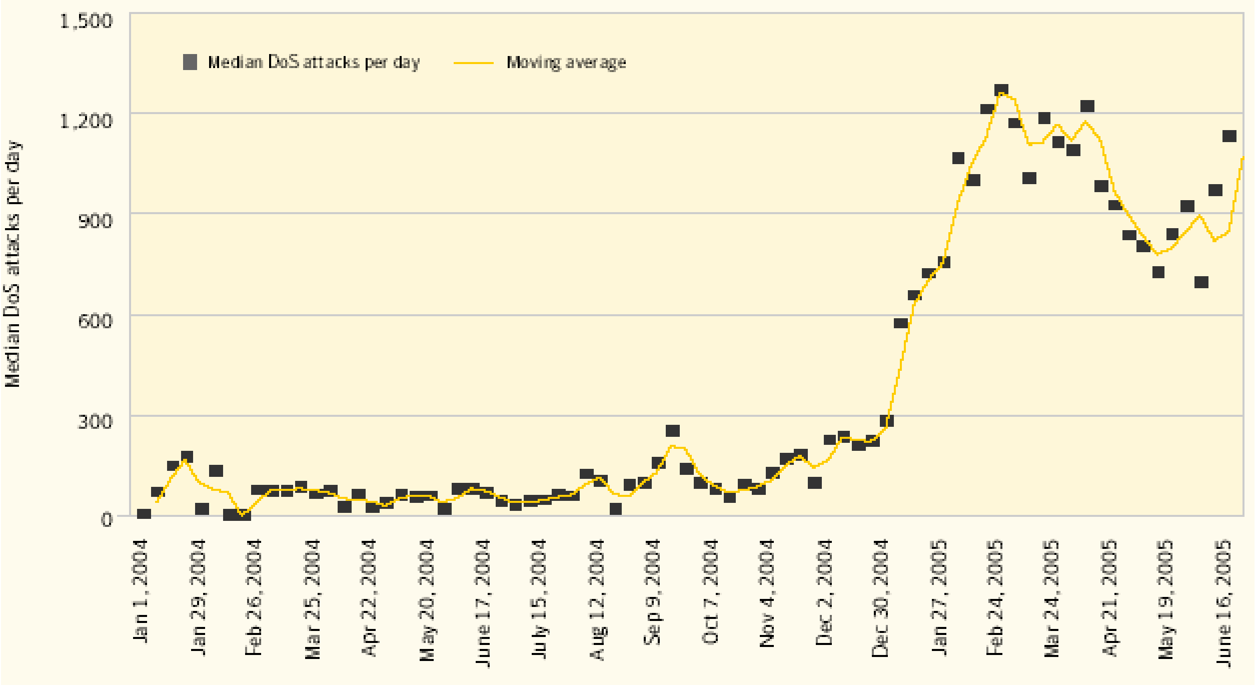


Figure 12 shows a huge increase of DoS attacks in the first half of 2005. This may be caused by the growing bot network activities, observed in the same period that is documented in the clause below.

With the growing of Voice over Internet Protocol (VoIP) as a widely adopted alternative to traditional phone systems, it may be supposed that DoS attacks against voice servers will increase.

Phishing

Phishing is an effort of attackers to ask for confidential information from an individual, group, or organization, often for financial benefits. This type of attacker is called Phishers. Phishers are groups or individuals who try to trick people into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information. This attack is intended to use the obtained data for criminal acts.

Symantec has collected the data shown in Figure 13 to Figure 15 having regard to

- Six-month growth in phishing messages
- Number of blocked phishing attempts
- Phishing as a percent of email scanned

Figure 13: Unique Phishing Messages Detected

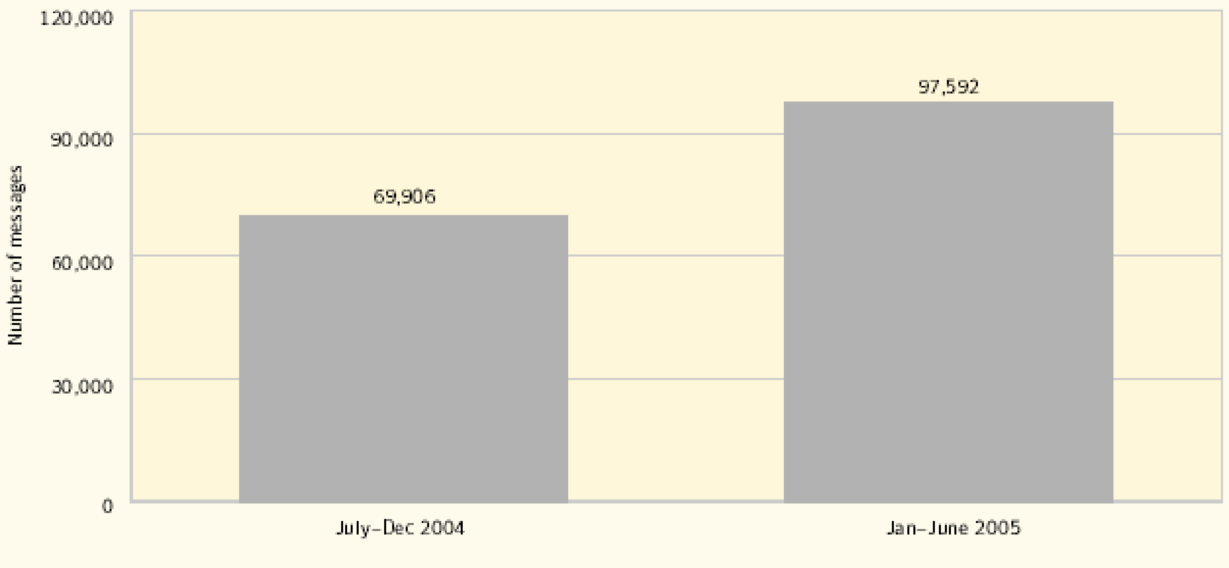


Figure 13 shows the number of unique messages that could be observed in each sequence of messages identified by the Symantec Probe Network as a phishing effort. In the first half of 2005 97,592 unique phishing messages could be observed. This is an increase of 40% over the 69,906 unique phishing messages that were detected in the second half of 2004. In addition the number of companies identified by Symantec as phishing targets increased, including companies that were previously being phished but were undetected, and those that had not previously been phished.

Figure 14 shows the number of blocked phishing emails that were blocked in the Symantec Probe Network by antispam filters. The number of blocked phishing efforts reports a significant increase for the first half of 2005. In this period 1.04 billion phishing efforts were blocked. Compared to 546 million in the last six months of 2004; this is a 90% increase.

Figure 14: Number of Blocked Fishing Efforts

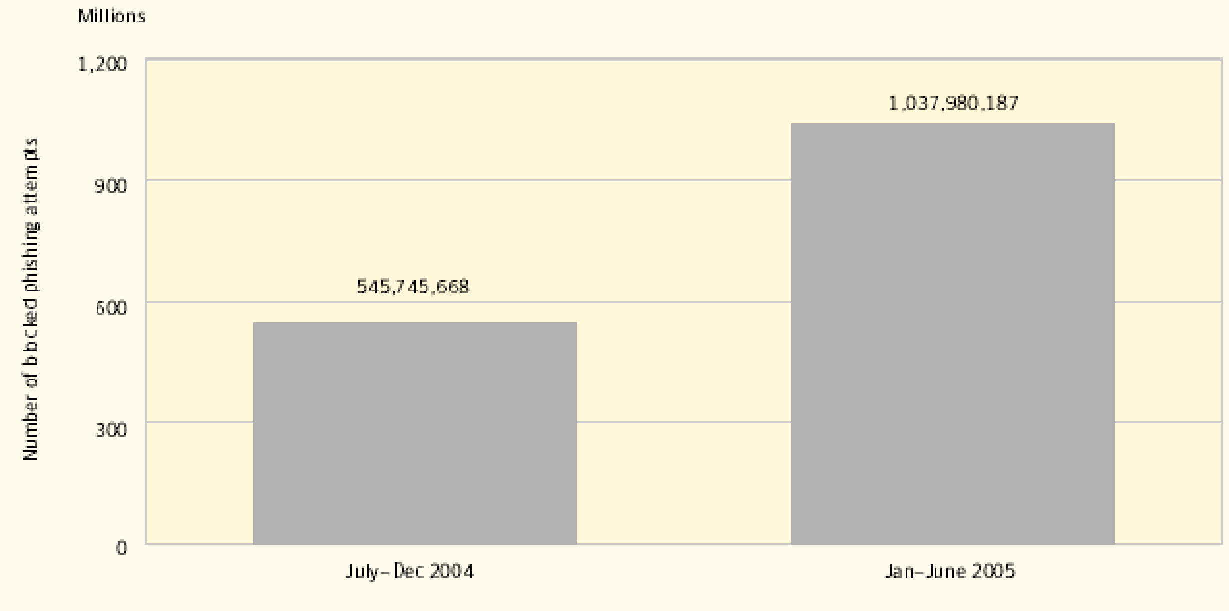


Figure 15: Phishing as a Percentage of Email Scanned

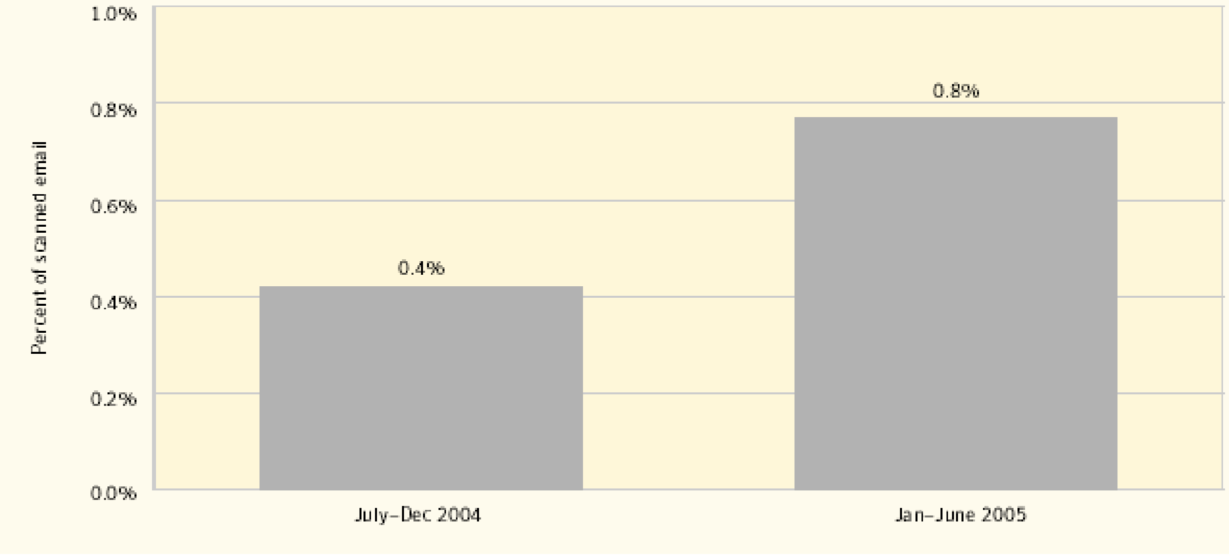


Figure 15 shows the volume of phishing attempts as a percentage of the total email scanned by Symantec.

In the first half of 2005, the percentage of email messages identified as phishing efforts increased from 0.4% of the messages observed, or an average of 2.99 million efforts per day, to 0.8% of the messages observed, an average of approximately 5.70 million phishing efforts per day. On peak days during this period the number of phishing efforts accumulated to 13 million efforts per day.

Caused by the increasing number of phishing efforts, it is very important to take effective countermeasures to protect companies' staff members against such efforts. In chapter 3.1.2, clause *Phishing* meaningful countermeasures are described. In addition it is recommendable to filter email traffic and to check the addressers of emails.

It is to suppose that phishing efforts will increase by the following reasons:

- Attackers benefit from affecting new targets. Due to the fact that there are a lot of smaller targets (such as regional banks) compared with a few large ones (like credit card companies) and that it is easier to affect smaller targets the number of phishing targets will as likely as not continue to grow.
- Phishing messages are continually being altered in order to avoid antispam and antiphishing filters. New methods will be developed, particularly in the use of randomized changes in phishing messages.
- Any method that is successful in fooling end users into disclosing valid personal information is supposed to be continuously used for criminal efforts.
- With the growing of Voice over Internet Protocol (VoIP) as a widely adopted alternative to traditional phone systems, voice phishing, in which users are pushed by voicemails to return calls and disclose critical personal information, will increase.

Voice over IP

While there are currently few reported attacks targeted at VoIP systems, it is supposed that the number of threats will grow in accordance with the widespread acceptance and deployment of this new technology.

VoIP may be vulnerable to a wide range of possible attacks, including but not necessarily limited to the following threats:

- Efforts to discover legitimate IP phone addresses through directory scanning
- Blocking voicemail systems with voice spam sent as audio files
- Phishing with means of voicemails urging users to return calls and disclose critical personal information
- DoS attacks against voice servers
- Utilize vulnerabilities in VoIP products for malicious purposes
- Efforts to redirect calls to another phone
- Hijacking of ongoing calls
- Turn on other phones so they act as receivers of conversations

The adoption of VoIP on company networks in absence of appropriate security measures is supposed to open another entry point that may be utilized by attackers for malicious purposes. It is recommendable that companies that are aiming the adoption of VoIP perform a risk analysis to be able to adopt appropriate security measures.

Wireless Local Area Networks

In recent years an increasing use of Wireless Local Area Networks (WLAN) in companies and other locations has been noticeable. WLAN connections can be found in such places as coffee shops, airports, and hotels. Many home users benefit from the convenience of wireless connectivity. Even municipalities aim at adopting low-cost or free wireless access in public places. But the growing number of people using wireless connectivity led to corresponding growing attacks targeting at insecure wireless access points. It is possible to monitor and capture connections made over wireless networks. To be protected against attacks, it is recommendable to add secure configuration, encryption, and authentication to devices that are interconnected by means of WLANs. In particular, companies should ensure that wireless networks are used over a Virtual Private Network (VPN) and that connections be placed in a DMZ, in which inbound and outbound connections are required to pass through a firewall. It should be ensured that mobile staff members only connect to secure wireless access points or, when devices are insecure or not in use, they are turned off or disabled.

Mobile End Devices

One of the changes in the threat landscape is the growing development of malicious code for mobile devices. Despite the fact that the number of reported threats is still relatively small, the discovered ones show the robust capabilities of malicious code for mobile devices, e.g. the first Multimedia Messaging Service (MMS) worm that was discovered in March 2005.

The most commonly attacked mobile devices are smart phones. Those are mobile phones that contain an exhaustive operating system with a diversity of user–installable software.

The first detected mobile device worm was Cabir, which spreads via Bluetooth. In the second half of 2004, multiple variants of this worm were detected. In the second half of 2004, two newly documented malicious code samples for the Windows CE (Windows CE Pocket PC) operating system were documented. But not any additional threats for this platform appeared in the first half of 2005. It is supposed that in the future, attackers will prefer smart phone threads, because they are widely used and offer high connectivity.

While previous malicious code used Bluetooth that requires physical proximity between an infected device and a target, attackers now are developing Multimedia Messaging Service (MMS) worms that only require a connection between a phone and the network in order to send messages and files to other phones.

Until now no automatically spreading malicious code has been developed. Worms still has to be run by the recipient to be effective. Users can protect themselves against these threats by performing safe computing practices. For instance, they can prevent infection of devices by not installing unknown programs or accepting connections from unknown sources.

Additional Security Risks

At least some highlights about the growing of additional security risks:

- Adware made up 8% of the top 50 reported programs. That is an increase of 3% since the second half of 2004.
- Eight of the top ten adware programs were installed through web browsers.
- Six of the top ten spyware programs were bundled with other programs and six were installed through web browsers.
- Of the top ten adware programs reported in the first six months or 2005, five hijacked browsers.
- Messages that constitute Phishing attempts increased from an average of 2.99 million per day to approximately 5.70 million messages.
- Spam made up 61% of all email traffic.

3.4 Recommendations for Commercial Sites

3.4.1 Threat Risk Modeling

When designing secure web applications for commercial use it is essential to perform a threat risk modeling process. It allows organizations and enterprises to determine the correct controls and produce effective countermeasures within a reasonable price-performance ratio. There are various steps in a threat modeling process. First the prospective security objectives should be identified by management and developers by answering the following questions:

- Is it necessary to protect the user’s identity from misuse, e.g. required for many banking applications?
- Is reputation a high level security objective, e.g. leads the loss of reputation caused by Phishing attacks to a high financial loss?
- Have financial risks an important part in the planed application, e.g. comparing the risks of a banking application versus those of an Internet forum?
- To what extend protection of user’s data is necessary, e.g. depends the planed application on regulations and privacy legislation (such as tax regulations or consumer protection legislation)?

- Is availability a high level security objective warranting the high costs that are bound with availability guarantees?
- Is the enterprise or organization bound by a security policy, common standards, legal agreements, or other laws and regulations?

After designing the application architecture the features and modules having a security impact need to be identified. The known threats should be documented and associated to the identified modules. Potential attackers should be identified and classified by answering the following questions:

- Is the attacker an authorized user exploiting an unknown mistake in your application?
- Is it automated malware searching for known vulnerabilities?
- Are the attackers' security researchers noticing something wrong and testing further?
- Are the attackers' computer criminals compromising your application for personal prestige or political motivations?
- Is it a disgruntled staff or a paid attacker?
- Is organized crime behind a threat, attacking a higher risk, e.g. e-commerce or banking application?

Threat risk modeling is intended to make a reasonable cost/performance estimation to minimize the costs and to maximize the security performance.

3.4.2 Handling E-Commerce Payments

Carrying on a business via the Internet it is recommendable to pay attention to the following rules:

- Handle payments in a safe and equitable way for users of e-commerce systems
- Minimize fraud from cardholder not present (CNP) transactions
- Maximize privacy and trust for users of e-commerce systems
- Comply with all local laws and Payment Card Industry (PCI) (merchant agreement) standards, e.g. the Payment Card Industry Data Security Standard (see [PCI-DSS])

(See "The Open Web Application Security Project, a Guide to Building Secure Web Applications and Web Services" [OWASP-Guide].)

3.4.2.1 Legal Requirements

In Germany the following Information and Communication Services Acts are to observe for the areas:

- E-Commerce

- Information and Communication (ICT) Data Protection
- Protection against illegal web contents

E-Commerce

Germany

- Act on the Utilization of Teleservices (Teleservices Act – Teledienstegesetz (TDG))
- Act on the protection of services based on, or consisting of, conditional access

Europe

- Directive 2000/31/EC of the European Parliament and of the Council of June 8th, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

Information and Communication (ICT) Data Protection

Germany

- Act on the Protection of Personal Data used in Teleservices (Teleservices Data Protection Act – Teledienstedatenschutzgesetz (TDDSG))

Europe

- Directive 95/46/EC of the European Parliament and of the Council of October 24th, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 97/66/EC of the European Parliament and of the Council of December 15th, 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

International

- Misuse of International Data Networks, Report submitted by the Expert Group to G8 Ministers and Chief Advisors of Science and Technology (Carnegie Group), Rome, October 17th, 1997

Protection against illegal web contents

Europe

- Internet Action Plan
- European Commission - Legal Advisory Board: Legal Aspects of Computer-Related Crime in the Information Society
- Council of Europe: Convention on Cybercrime

Reference

The documents are listed on [IuKDG-En]: "Guideline to the Information and Communication Services Acts".

3.4.2.2 PCI Compliance

To comply with the most current regulations concerning credit cards, providers of commercial sites are required to review the PCI Guidelines and the relevant merchant agreement, e.g. the Payment Card Industry Data Security Standard [PCI-DSS].

3.4.2.3 Recommendations

E-commerce merchants are required to comply with all relevant local laws, such as all tax acts, trade practices, and so on. They should consult a source of legal advice competent for their jurisdiction to find out what is necessary.

Credit card merchants are required to agree to the credit card merchant agreements. Typically, these are extremely strict about the amounts of fraud allowed, and the guidelines for "cardholder not present" transactions. Credit card merchants have to read and to follow their relevant agreements.

Shop providers are required to publish their terms and conditions, their privacy and security notice, and possibly a duty or information notice.

As an example for form design of commercial web sites, especially to demonstrate the aspects described in chapter "3.4.2.3 Recommendations", have a look to

- http://www.amazon.com/, or
- http://www.tchibo.co.uk/

3.4.3 Best Practice Lists

Some of the organizations described in chapter 4 are publishing guidelines and best practice lists on their web sites.

Designing a secure web application it is recommendable to have a look on these sites to get the freshest information about "The Twenty Most Critical Internet Security Vulnerabilities", "Enterprise Best Practices", "Consumer Best Practices", and so on.

More detailed information about organizations dealing with Internet security and data protection are given in chapter 4.

4 Specific Measures in the European Union

All information provided in this chapter only gives examples. Especially listings of initiatives, agencies, incident response teams, and enterprises may be fragmentary.

4.1 Legal Requirements and Regulations

In addition to chapter 3.4.2.1 of this study and chapter 4 of the “Study on Promotion Strategy of Conformity Assessment System of Information Security” this chapter gives a short survey of the legal situation in Europe and its member states France, Germany and United Kingdom in the areas

- E-Commerce
- Electronic Signatures
- Information and Communication (ICT) Data Protection
- Protection against illegal web contents

In addition some international working groups and activities are listed.

Hint The references are given in the listed form because there is no one-to-one relation between document and reference in either case.

4.1.1 E-Commerce

Europe

- Directive 2000/31/EC of the European Parliament and of the Council of June 8th, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).
  The directive aims at promoting the development of electronic commerce within the information society regarding that it offers significant employment opportunities in the Community, particularly in small and medium-sized enterprises. Increase of electronic commerce applications will stimulate economic growth and investment in innovation by European companies, and can also enhance the competitiveness of European industry, provided that everyone has access to the Internet.
- Commission Decision of October 24th, 2005 establishing an expert group on electronic commerce (2005/752/EC).
  Having regard to the treaty establishing the European Community, the European Commission has established an expert group on electronic

commerce that can be consulted on any questions relating to the directive on electronic commerce.

- Directive 98/84/EC of the European Parliament and of the Council of November 20th, 1998 on the legal protection of services based on, or consisting of, conditional access.
  The directive provides for the free movement of services applied to broadcasting and information society services.

References

The documents are available via

- http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett
- http://www.europa.eu.int/eur-lex/en/search/search_lif.html
- http://europa.eu.int/eur-lex/lex/en/repert/1320.htm#132060
- http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_320/l_32019981128en00540057.pdf
- http://www.iukdg.de/english.html

France

- Convention collective étendue: “Commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager”, (19e édition), (Convention of November 26th, 1992)
  Publication of a comprehensive convention on topics “Commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager” (commerce and sevices on subjects audivisual, electronic, and household goods).
- Pour la confiance en l'économie numérique Collection : "Aux sources de la loi" – (June 21st, 2004, Law no 2004-575, "Sur la confiance en l’économie numérique")
  This law supports the development of commerce via Internet, clearing the rules both for consumers and providers.

References

The documents are available via

- http://www.journal-officiel.gouv.fr/jahia/Jahia/catalogue
  - search with keyword “electronique commerce”
- http://www.internet.gouv.fr/accueil_thematique/securite-76m.html
- http://www.ssi.gouv.fr/en/regulation/regl.html

Germany

- Act on the Utilization of Teleservices (Teleservices Act – Teledienstegesetz TDG) of July 22nd, 1997, amended last by Article 1 of the bill on legal framework conditions for electronic commerce).
  The purpose of this act is to establish uniform economic conditions for the various applications of electronic information and communication services.
- Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz EGG – Act on the legal framework on topic electronic business connections), December 14th, 2001, published in BGBl (Bundesgesetzblatt) I 2001 Nr. 70, December 20th, 2001.
  Implementation of Directive 2000/31/EC of the European Parliament and of the Council of June 8th, 2000.
- Conditional Access Services Protection Act: "Act on the protection of services based on, or consisting of, conditional access", (Zugangskontrolldiensteschutzgesetz – ZKDSG), March 23rd, 2002
  This act serves to implement Directive 1998/84/EC of the European Parliament and of the Council of November 20th, 1998 on the legal protection of services based on, and consisting of, conditional access.

References

The documents are available via

- http://www.iukdg.de/english.html
- http://www.iukdg.de/index_ecom.html
- http://www.rechtliches.de/info_Elektronischer_Geschaeftsverkehr-Gesetz.html

United Kingdom

- The Electronic Commerce Directive (00/31/EC) & The Electronic Commerce (EC Directive) Regulations 2002 (SI 2002 No. 2013)
  Implementation of Directive 2000/31/EC of the European Parliament and of the Council of June 8th, 2000.
- The Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) (Electronic Commerce Directive) Order 2002 – Statutory Instrument 2002 No. 2157
- The Electronic Commerce Directive (Financial Services and Markets) Regulations 2002 - Statutory Instrument 2002 No. 1775
- The Electronic Commerce Directive (Adoption and Children Act 2002) Regulations 2005 - Statutory Instrument 2005 No. 3222
- The Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 – Statutory Instrument 2005 No. 1529

References

The documents are available via

- http://www.dti.gov.uk/industries/ecommunications/electronic_commerce_directive_0031ec.html
- http://www.opsi.gov.uk/
  - search with keyword “electronique commerce”

International

- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment
  By providing standards by which the legal value of electronic messages can be assessed, the Model Law aims at playing a significant role in enhancing the use of paperless communication. In particular the law contains rules for electronic commerce in specific areas, such as carriage of goods.
- UNCITRAL Working Group on Topic E-Commerce
- Site of the World Trade Organization (WTO) on Topic E-Commerce
- Site of the Organization for Economic Co-operation and Development (OECD) on topic E-Commerce

References

These sites are available via

- http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
- http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html
- http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm
- http://www.oecd.org/topic/0,2686,en_2649_37441_1_1_1_1_37441,00.html

4.1.2 Electronic Signature

Europe

- Directive 1999/93/EC of the European Parliament and of the Council of December13th, 1999 on a Community framework for electronic signatures
  The directive aims at promoting a single European market.

References

The documents are available via

- http://www.iukdg.de/english.html
- http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

France

- The Law "LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique "
  The electronic signature is a legal value in France since the adoption of the law no.2000-230 from March 13th, 2000. This law has been completed by the following decrees and decisions rendering more precisely the conditions of electronic applications, namely:
  - "le décret du 30 mars 2001" (see below)
  - "le décret du 18 avril 2002" (see below)
  - "l'arrêté du 26 juillet 2004 (en remplacement de l'arrêté du 31 mai 2002 abrogé)" (see below)
  - "la loi du 21 juin 2004 pour la confiance dans l'économie numérique" (see above)
- The decree "Le décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique"
  This decree is a technical oriented document. It makes a different between a "signature électronique" (electronic signature) and a "signature électronique sécurisée" (electronic signature reassuring). The electronic signature reassuring, defined by the decree, is the reliable signature that can resist in a legal procedure.
- The decree "Le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information
  This decree establishes a voluntary procedure for the evaluation and certification of products and systems that provide the creation of electronic signatures.
- The decision "Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation"
  This decision completes the decree from April 2002 and renders more precisely the agency that is in charge with the accreditation of the evaluation bodies, namely the COFRAC (Comité Français d'Accréditation). Accredited bodies are allowed to provide a certification service. The duration of an accreditation is limited to 5 years.

References

The documents are available via

- http://www.chambersign.tm.fr/certificat/droit.jsp
- http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSX9900020L
- http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSC0120141D

- http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=PRMX0100183D
- http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INDI0403348A
- http://www.ssi.gouv.fr/en/regulation/index.html#produits_crypto
- http://www.ssi.gouv.fr/en/regulation/regl.html

Germany

- Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations of May 16th, 2001 (Federal Law Gazette I, p. 876), last amended by Art. 1 of the First Act Amending the Signature Law (First Signature Amendment Act – 1. SigGÄndG) of January 4th, 2005 (Federal Law Gazette I, p. 2) – unofficial consolidated version for industry consultation
  This version aims at simplifying the procedure for the issue of qualified certificates and to reduce the associated costs.
- Digital Signature Ordinance – SigV
  Ordinance on Electronic Signatures of November 16th, 2001 (last amended by Article 2 of the First Act Amending the Signatures Act (unofficial consolidated version). On the basis of Section 24 of the Signatures Act of May 16th, 2001 (Federal Law Gazette I. p. 876), and in conjunction with the Second Section of the Administrative Costs Act of June 23rd, 1970 (Federal Law Gazette I p. 821).
  - Draft of a Law on the Framework Conditions for Electronic Signatures as decided by the Cabinet on August 16th, 2000
  - Justification of the Draft of a Law on the Framework Conditions for Electronic Signatures as decided by the Cabinet on August 16th, 2000

References

The documents are available via

- http://www.iukdg.de/english.html
- http://www.iid.de/iukdg/gesetz/Signaturg_engl.pdf
- http://www.iid.de/iukdg/gesetz/SigV161101-engl.pdf
- http://www.iid.de/iukdg/eval/VIB2Referentenentwurfenglisch.pdf
- http://www.iid.de/iukdg/eval/VIB2RefEntwBegEngl.pdf

United Kingdom

- Electronic Communications Act 2000, 2000 Chapter c.7
  An act to make provision to facilitate the use of electronic communications and electronic data storage and to make provision about the modification of licenses granted under section 7 of the Telecommunications Act 1984; and for connected purposes.
- Electronic Communications Act (Northern Ireland) 2001, 2001 Chapter 9
  This act aims at making provision to facilitate the use of electronic communications and electronic data storage.
- The Electronic Signatures Regulations 2002, 2002 No. 318, ELECTRONIC COMMUNICATIONS, Coming into force March 8th, 2002
  These regulations implement Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.
  - Annex I to the Directive “Requirements for Qualified Certificates”
  - Annex II to the Directive “Requirements for Certification-Service-Providers Issuing Qualified Certificates”

References

The documents are available via

- http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html
- http://www.opsi.gov.uk/legislation/about_legislation.htm
- http://www.opsi.gov.uk/
  - search with keyword “Electronic Signature”
- http://www.dti.gov.uk/industries/information_security/electronic_signatures_associated_legislation.html
- http://www.opsi.gov.uk/si/si2002/20020318.htm

International

- UNICITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
  The law aims at bringing additional legal certainty to the use of electronic signatures.
- OECD – Cryptography guidelines and issues

References

The sites are available via

- http://www.iukdg.de/index_esig.html
- http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

- http://www.oecd.org/
- http://www.oecd.org/searchResult/0,2665,en_2649_201185_1_1_1_1_1,00.html
  - search with keyword “Cryptography guidelines and issues”

4.1.3 Information and Communication (ICT) Data Protection

Europe

- Directive 95/46/EC of the European Parliament and of the Council of October 24th, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 97/66/EC of the European Parliament and of the Council of December 15th, 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
- Directive 2002/58/EC of the European Parliament and of the Council of July 12th, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
  The directive aims at allowing the free movement of lawfully gathered personal data within the EU Member States. Therefore it defines confidentiality as the basic principle for all forms of electronic communication. The directive had to be transposed into national law by EU Member States until October 31st, 2003.

References

The documents are available via

- http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm
- http://www.iukdg.de/english.html
- http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
- http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf
- http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf
- http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/cs%20compo%20data%20protec%20en.pdf
- http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

France

- Implementation of the European Directive 95/46/EC:
  The law n° 2004-801 of August 6th, 2004 relating to the protection of individuals with regard to the processing of personal data and modifying the law n° 78-17 of January 6th, 1978 relating to data processing, data files and individual liberties was published with OJ (Official Journal of the European Communities) of August 7th, 2004.
  Under the new law, the following types of processing must be authorized in advance by the French data protection authority, the National Computing and Liberties Commission ('CNIL'):
  - Processing of sensitive personal data
  - Use of automated processing techniques
  - Automated interconnection of separate databases
  - Use of biometric identifiers
  - Transfers of personal data outside the EU

References

The documents are available via

- http://www.cnil.fr/index.php?id=1351
- http://www.journal-officiel.gouv.fr/jahia/Jahia/catalogue/
  - search keyword “loi n° 2004-801”
- http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSX0100026L
- http://www.bild.net/dataprFr.htm
  (English version)

Germany

- Act on the Protection of Personal Data Used in Teleservices (Teleservices Data Protection Act - Teledienstedatenschutzgesetz TDDSG) of July 22nd, 1997, amended last by Article 3 of the bill on legal framework conditions for electronic commerce
- Bundesdatenschutzgesetz (BDSG) – Federal Data Protection Act (DLP) Implementation of the “Directive 95/46/EC of the European Parliament and of the Council of October 24th, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data” and its’ successors in 1997 and 2002:
  - publication date December 20th, 1990 (Bundesgesetzblatt I S. 2954)
  - adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May (unofficial English translation available, see last link below)
  - new version on January 14th, 2003 I 66, modified by § 13 sec. 1 on September 5th, 2005 I 2722 (German version only)

All countries ("Länder", except Sachsen and Bremen) adopted new DPLs to implement the Directive. These acts apply to the public sector of the respective countries.

References

The documents are available via

- http://www.iukdg.de/english.html
- http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf
- http://www.bfdi.bund.de/cln_029/nn_532042/SharedDocs/Publikationen/GesetzeVerordnungen/BDSG,templateId=raw,property=publicationFile.pdf/BDSG.pdf
- http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm#germany

United Kingdom

- Data Protection Act 1998, 1998 Chapter 29
  The act regulates the right of data subjects and others, gives some notifications regarding data controllers, and regulates the exemptions.
- Freedom of Information Act 2000
  Under the Freedom of Information Act 2000, anybody may request information from a public authority which has functions in England, Wales and/or Northern Ireland. The Act confers two statutory rights on contenders:
  - To be told whether or not the public authority holds that information; and if so,
  - To have that information communicated to them.

  The Freedom of Information Act 2000 came into force on 1 January 2005.
- Statutory Instrument 1999 No. 2093 "The Telecommunications (Data Protection and Privacy) Regulations 1999"
- Statutory Instrument 2003 No. 2426 "The Privacy and Electronic Communications (EC Directive) Regulations 2003"

References

The documents are available via

- http://www.dca.gov.uk/foi/index.htm
- http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm#ukingdom
- http://www.opsi.gov.uk/
  - search with keyword "data protection act"
- http://www.opsi.gov.uk/acts/acts1998/19980029.htm
- http://www.opsi.gov.uk/cgi-bin/htm_hl.pl?DB=opsi&STEMMER=en&WORDS=data+protect+act+&COLOUR

=Red&STYLE=s&URL=http://www.opsi.gov.uk/si/si1999/19992093.htm#muscat_highlighter_first_match
- http://www.opsi.gov.uk/cgi-bin/search.pl
  - search with keyword "data protection"
- http://www.opsi.gov.uk/cgi-bin/htm_hl.pl?DB=opsi&STEMMER=en&WORDS=data+protect+&COLOUR=Red&STYLE=s&URL=http://www.opsi.gov.uk/si/si2003/20032426.htm#muscat_highlighter_first_match

International

- Misuse of International Data Networks
  Report submitted by the Expert Group to G8 Ministers and Chief Advisors of Science and Technology (Carnegie Group), Rome, October 17th, 1997.

References

The documents are available via

- http://www.iid.de/iukdg/archiv/carnegie_e.html

4.1.4 Protection against illegal or harmful web contents

In addition to the regulations described in this chapter, have a look to the web sites according with "Safer Internet" in chapter 4.6 below.

Europe

Legal Requirements

- Decision No 1151/2003/EC of the European Parliament and of the Council of June 16th, 2003 amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.
  Part of the "Community action plan on promoting safer use of the internet" ("Safer Internet" – January 1999 to December 2002) that aims at promoting the safer use of the Internet and to encourage, at European level, an environment conducive to the development of the Internet-related industry.
- Decision No 854/2005/EC of the European Parliament and of the Council of May 11th, 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies.
  Part of the "Safer Internet plus programme (2005-2008)" building on the aim of its predecessor (see above) to promote an environment conducive to the development of the Internet-related industry while supporting safer use of the Internet and fighting against illegal and harmful content. In addition the new program also covers other media, such as videos, and explicitly addresses the

fight against racism and unsolicited content (e.g. "spam", unwanted by the end user). It will focus more closely on end-users: parents, educators and children and consider new filtering technologies.

References

The documents are available via

- http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32003D1151:EN:HTMLFrance
- http://europa.eu.int/scadplus/leg/en/lvb/l24190.htm
- http://europa.eu.int/scadplus/leg/en/lvb/l24190b.htm

European Program “Safer Internet”

- New Program Safer Internet Plus 2005 – 2008
  The Safer Internet plus program aims at promoting safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and unsolicited content (e.g. "spam", unwanted by the end user), as part of a coherent approach by the European Union.
  Participation in the program is open to legal entities established in the Member States (Austria, Belgium, Cyprus, Czech Republic, Denmark , Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, The Netherlands, United Kingdom) It is further open to participation of legal entities established in EFTA States which are contracting parties to the EEA (EUROPEAN ECONOMIC AREA) Agreement (Norway, Iceland and Liechtenstein).
  The program is based on the experience and the success of the Safer Internet Action Plan 1999 – 2004.

References

The sites are available via

- http://www.europa.eu.int/information_society/activities/sip/programme/index_en.htm
- http://www.europa.eu.int/information_society/activities/sip/index_en.htm

France

Spam: the state of the right in France

- The law “La loi pour la confiance dans l’économie numérique” of June 21st, 2004
  The law assigns that the use of addresses of electronic mails for purposes of commercial advertising requires obtaining the preliminary assent of the people concerned. Otherwise it is forbidden to use it. Each electronic message sent must envisage methods to identify the account of the person who has sent the message.
- The law “loi Informatique et Libertés” of January 6th, 1978
  The law assigns that any automated treatment of personal information comprising of the electronic addresses must be declared at the CNIL (Commission Nationale de L’Informatique et des Libertés).

References

The documents are available via

- http://www.cnil.fr/index.php?id=1272

Germany

Jugendschutzgesetz (Law for the Protection of the Youth)

In Germany a uniform right framework was established in the area of the protection of children and young people in the electronic media.

- Convention “Staatsvertrag der Länder über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk (Fernsehen) und Telemedien (Internet)”
  Convention of the countries over the protection of the human dignity and the protection of children and young people in broadcast (television) and electronic media (Internet), which arranges the authority between federation and countries together with the law for the protection of the youth, harmonizes the supervision structure, and strengthens the self regulations. The directive is valid since 1 April 2003.
- Law for the Protection of the Youth – wording of the law.

References

The documents are available via

- http://www.kjm-online.de/public/kjm/index.php?show_1=94,57
- http://www.bmfsfj.de/RedaktionBMFSFJ/Abteilung5/Pdf-Anlagen/juSchGenglisch,property=pdf,bereich=,rwb=true.pdf

United Kingdom

Legislation relating to child abuse images

- Protection of Children Act 1978 (England and Wales)
- Civic Government Act, 1982 (Scotland)
- Sexual Offences Act 2003: Key Changes (England and Wales)
- MOU: Section 46 Sexual Offences Act 2003

Legislation relating to criminally obscene content

- Obscene Publications Act 1959 and 1964

Legislation relating to criminally racist content

Incitement to Racial Hatred was adopted into the Public Order Act in 1986.

- Public Order Act 1986

Directive applicable to the liability of Internet Service Providers

- Liability of intermediary service providers directive 2002

References

The documents are available via

- http://www.iwf.org.uk/police/page.22.htm

International

- Convention on Cybercrime, the Council of Europe, opened for signature in Budapest, on November 23rd, 2001, coming into force on July 1st, 2004
  On international level it is important to create standards for punishable contents and procedures. Here the Cyber Crime agreement of the Council of Europe is to be emphasized coming into force on July 1st, 2004. It concerns the first international contract over punishable actions, which are committed over the Internet or other computer networks. The agreement is concerned in detail with offences against copyright, fight against fraud and child pornography as well as offences against network security.

References

The according documents are available via

- http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
- http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

4.2 Data Protection Institutions

4.2.1 General Information

Within Europe, the individual's right to privacy is definitely codified in the European Convention on Human Rights and Fundamental Freedoms [ConFreeEU] of 1950. In 1995 the EU established the directive 95/46/EC codifying the basic principles for the protection of individuals with regard to the automatic processing of personal data, in particular with regard to the collection, storage, and use of personal data. In 1997 the EU established the directive 97/66/EC codifying the protection of personal data in the specific environment of telecommunication networks and services.

The directive 97/66/EC was substituted by directive 2002/58/EC in order to take account of technological developments. It includes conditions on security of networks and services, confidentiality of communications, access to information stored on terminal equipment, processing of traffic and location data, calling line identification, public subscriber directories and unsolicited commercial communications.

The directive had to be transposed into national law by the Member states by October 31st, 2003 at the latest.

On September 21st, 2005 the European Commission has adopted a proposal for a "Directive on the retention of communications traffic data". It aims at harmonizing the obligations for providers to retain data related to mobile and fixed telephony and internet communication data.

Article 28 of the directive 95/46/EC codified that each Member State should provide "that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive". Article 29 created a working party consisting of the independent national data protection authorities in the Member States.

Reference

The documents described in this section are available in html- and PDF-format on the web site of the European Commission:
http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm

4.2.2 Sites of Data Protection Commissioners

Europe

Council of Europe:
http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/

European Data Protection Supervisor:
http://europa.eu.int/comm/justice_home/fsj/privacy/eusupervisor/index_en.htm

National Data Protection Commissioners:
http://europa.eu.int/comm/justice_home/fsj/privacy/nationalcomm/index_en.htm

On the page above the contact information (addresses and links to web sites, if present) of the Data Protection Commissioners of the following countries are listed:

European Union Belgium, Czech Republic, Denmark, Germany, Estonia, Greece, Spain, France, Ireland, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Slovenia, Slovakia, Finland, Sweden, United Kingdom

EFTA Countries Iceland, Liechtenstein, Norway, Switzerland

Candidate countries
Romania, Croatia

Jersey/Guernsey/Isle of Man
Jersey, Guernsey, Isle of Man

Third Countries Australia, Canada, Hawaii, Hong Kong, Israel, Japan, Korea, New Zealand, Taiwan, Thailand, USA

France Commission Nationale de L'Informatique et des Libertés:
http://www.cnil.fr/index.php?id=21

Germany The Federal Commissioner for Data Protection and Freedom of Information:
http://www.bfd.bund.de/EN/Home/homepage__node.html

United Kingdom Information Commissioner's Office:
http://www.informationcommissioner.gov.uk/eventual.aspx?id=34
http://www.ico.gov.uk/eventual.aspx

USA U.S. Department of Labor, Office of the Chief Information Officer:
http://www.dol.gov/cio/programs/security/security.htm

4.3 Network Information Security Agencies

Europe European Network and Information Security Agency

The foundation of the European Network and Information Security Agency (ENISA) is based on the Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 (OJ L 77, 13 March 2004) [REG-ENISA].

The Agency assists the Commission, the Member States and the business community in meeting the requirements of network and information security, including present and future Community legislation.

To fulfill its objectives, the Agency's tasks will be focused on:

- Collecting and analyzing data on security incidents and emerging risks
- Co-operating with different players notably through the establishment of public / private partnerships with industry operating at EU and / or global levels
- Raising awareness and promoting risk assessment methods and best practices for interoperable risk management solutions
- Tracking the development of standards for products and services on Network and Information Society

ENISA publishes the "ENISA Quarterly" Newsletter.

Hint ENISA Country Pages, see the reference below

On its web site ENISA publishes so called "Country Pages" giving an overview of contact points and other relevant information related to network and information security in EU and EEA member states. National authorities are listed as well as other bodies and organizations active in network and information security. In addition current activities and events are announced.

References

The according information is available via

- http://www.enisa.eu.int/
- http://www.enisa.eu.int/publications/index_en.htm
- http://www.enisa.eu.int/country_pages/index_en.htm

France Central Information Systems Security Division

The Central Information Systems Security Division (SGDN/DCSSI) manages the French government website assigned to information systems security (ISS). It is the central Division under the "Secrétariat de Général de la Défense Nationale" (SGDN) (Department of Defense).

To fulfill its objectives, the Division's tasks will be focused on:

- Contribute to governmental decision-making processes and it's publishing in the area of information systems security (ISS)

- Act as the national regulation authority for ISS, by issuing accreditations, bails and certificates for
  - governmental information systems and
  - cryptographic processes and products used by public bodies and services
- Act as the national regulation authority for ISS, by controlling the information technology security evaluation centers (CESTI)
- Evaluate threats to information systems, give the alert, and develop capacities to counter and to prevent these threats (CERTA)
- Assist public services with respect to ISS
- Develop scientific and technical expertise in ISS, for the benefit of the administration and public services
- Provide training and increase awareness about ISS (Information Systems Security Training Centre – CFSSI)

References

The according information is available via

- http://www.ssi.gouv.fr/en/index.html

Germany

Federal Office for Information Security

The Federal Office for Information Security (BSI) is the central IT security service provider for the German government. Its goal is the safe adoption of information and communication technology in the German society. The BSI aims at considering safety aspects already with the development of IT systems and applications.

To fulfill its objectives, the Agency's tasks will be focused on:

- To provide information to all important topics of IT security
- To provide advise in questions of IT security and support during the implementation of suitable measures
- To conceive and develop IT security applications and products in a exemplary manner
- To examine, evaluate and certify IT systems regarding their safety characteristics
- The accreditation of IT systems for the processing of secret information

References

The according information is available via

- http://www.bsi.bund.de/english/index.htm

United Kingdom Communications-Electronics Security Group

The Communications-Electronics Security Group (CESG) is the national technical authority for information assurance in the United Kingdom. It provides the Information Assurance & Certification Service (IACS).

CESG is responsible for enabling secure and trusted knowledge sharing to help customers achieve their business aims. It delivers information assurance policy, services, and advice that government and other customers need to protect vital information services.

To fulfill its objectives, CESG is focused on three areas:

- Technical Advice
  - Initial technical advice on design options for secure IT architectures
  - In-depth technical consultancy on specific Information Assurance(IA) issues
  - Help with interpreting national security standards such as BS7799
  - Guidance on the use and deployment of cryptographic and other certified IA products
  - Advice on algorithm use and suitability
- Documentation
  - Production of system security documentation (SSP, SyOPs etc)
  - Advice on sources and status of technical documentation
  - Verbal and written feedback on technical documentation
- Other Services
  - Assignment of an adviser to attend meetings and provide continuity of advice throughout a project's life
  - Information on suppliers of approved / certified products
  - Help-desk style telephone advice
  - Access to alternative sources of technical advice
  - Training on specific Information Assurance issues

IACS has been designed to respond to the increasing complexity of IT products and systems and to the diverse customer requirements for assurance in the security functionality of those products and systems. It provides for independent and objective assurance in the security functionality of a product or system both within the UK and internationally.

To fulfill its objectives, IACS is currently focused on the following areas:

- ITSEC or Common Criteria formal evaluation and certification
- SYS level evaluations (SYS2, SYS3 and SYS4 are defined by the SYSn Assurance Packages Framework)
- Fast Track Assessments
- IT Health Check
- Cryptographic Evaluations
- Evaluation and certification according to the AMSG TEMPEST standards
  - TEMPEST is defined as the study of the emission of unintentional protectively marked data from an equipment or system
  - TEMPEST certification in the UK is carried out by CESG accredited test facilities. The test results from these facilities are endorsed by CESG against the AMSG TEMPEST standards.

References

The according information is available via

- http://www.cesg.gov.uk/indexNS.cfm

4.4 Computer Security Incident Response Teams

In its document "ENISA Inventory of CERT activities in Europe" [CERT-ENISA] the European Network and Information Security Agency ENISA gives a summary of the situation concerning CERTs (Computer Emergency Response Teams) and their activities in Europe as well as their international co-operations and initiatives outside of Europe.

This document provides a list of all CSIRTs (former name: CERT – Computer Emergency Response Team) established in the European Union until December 2005. Furthermore the document provides an overview about co-operation activities and projects, and supporting and standardization activities in Europe. The European activities are completed by international co-operations and initiatives outside of Europe.

In addition to the listing of European CERTs the document provides

- The date of the establishment of the CERT
- Its TI status
  - TI means *Trusted Introducer Service*. This service is meant to facilitate trust by formally accrediting CSIRTs that are ready to take that step. For a CSIRT to proceed from the status of "listed" to the status of "accredited" they need to go through a formalized accreditation scheme.
- A link to its web site
- Its FIRST (Forum of Incident Response and Security Teams) membership

- "The Forum of Incident Response and Security Teams (FIRST) consists of a network of individual computer security incident response teams that work together voluntarily to deal with computer security problems and their prevention. These teams represent government, law enforcement, academia, the private sector, and other organisations with justifiable interest as determined by the Steering Committee." [CERT-ENISA].

There is an ongoing successful cooperation between CSIRTs that deal with IT security incidents in general. This cooperation exists both on a global level (FIRST) and on a European level (TF-CSIRT and Trusted Introducer).

References

The according information is available via

- http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert.pdf
- http://www.trusted-introducer.nl/index.html
- http://www.first.org/

4.4.1 Listing of European CSIRTs

In respect of the document above this study only lists a short overview of the number of CERTs and its constituency in the following European countries:

Austria

Number: 1; Constituency: Customers of the Austrian Academic Computer Network.

Belgium

Number: 2; Constituency: Customers of the Belgium network connected universities, public administrations, high schools and research canters; the NATO Computer Incident Response Capability – Coordination Centre.

Croatia

Number: 1; Constituency: Users of systems inside the .hr namespace.

Cyprus

Number: 1; Constituency: Users of systems connected to the Cyprus Academic and Research Network.

Czech Republic

Number: 1; Constituency: Users of systems inside the .cz and the ces.net namespace.

Denmark

Number: 3; Constituency: Enterprises, users of the Danish research and educational networks, the entire Danish IT-community, the local authorities.

Finland

Number: 4; Constituency: Customers and employees in enterprises according to the telecommunications and IT sectors, the entire Finish IT-community.

France Number: 4; Constituency: Customers and employees in enterprises according to the telecommunications and IT sectors, customers from industry, services and other private companies, the French administration community.

Germany Number: 20; Constituency: Federal government departments in Germany, customers and employees in enterprises according to the telecommunications, the IT, the industrial, and the banking sectors, customers and members of the German national research network, international acting enterprises and research organizations, small and medium sized enterprises.

Greece Number: 2; Constituency: Users connected to Greek research, technology and education networks.

Hungary Number: 3; Constituency: Users of systems of the Hungarian government, users and members of Hungarian community of internet service provider, users and members of the Hungarian network for universities, education institutes, research organizations, and other non-profit institutions.

Iceland Number: 1; Constituency: Users of the Iceland research network.

Ireland Number: 1; Constituency: Users of the Ireland education and research network.

Italy Number: 9; Constituency: Internet connected sites in Italy, users of the Italian academic and research network, central public administration in Italy, national government departments, local agencies, users of the Catholic Church network, enterprises in the sectors of telecommunications and energy providers.

Lithuania Number: 1; Constituency: Users and members of the Lithuanian network for universities, education institutes, research organizations, and other non-profit institutions.

Luxembourg Number: 2; Constituency: The whole Internet community in Luxembourg, subscribers of the Luxembourgian CERTs.

Malta Number: 1; Constituency: All government employees.

Norway Number: 2; Constituency: Norwegian government departments and specified commercial organizations, users and members of the Norwegian network for universities, education institutes, research organizations, and other non-profit institutions.

Poland Number: 3; Constituency: Users of systems inside the .pl namespace, users, sites, and organizations connected to the networks provided by two Polish CERTs.

Portugal Number: 1; Constituency: Users of systems connected to the Portugal national research and education network.

Russia Number: 2; Constituency: The entire Internet community in Russia, subscribers of the Russian CERTs.

Slovenia Number: 1; Constituency: Users of systems inside the .si namespace, customers of the academic and research network of Slovenia.

Spain Number: 1; Constituency: Users of systems inside the .es namespace, users of systems connected to networks of private organizations operating in Spain.

Sweden Number: 4; Constituency: Members of Swedish government organizations and specified organizations outside government, users and members of the Swedish networks for universities, education institutes, and research organizations, of systems connected to a commercial provider of external and internal networks in the Scandinavian area.

Switzerland Number: 5; Constituency: Members and customers of a research organizations and commercial enterprises in the sectors of telecommunications and internet and security providers.

The Netherlands Number: 10; Constituency: Members and users of systems in the area of banking, universities, and governmental institutions, and customers of internet providers.

Turkey Number: 1; Constituency: Members of governmental organizations.

United Kingdom Number: 17; Constituency: Customers and members in the sector of telecommunications and other commercial organizations, subscribers of British CERTs, customers of the European research network, customers and users of British networks for universities, education institutes, and research organizations, members of central government and government departments, members of critical national infrastructure organizations and government contractors.

4.4.2 Standardization Activities

CAIF – Common Announcement Interchange Format

The Common Announcement Interchange Format (CAIF) is an XML-based format to store and exchange security announcements in a normalized way. It provides a basic but comprehensive set of elements that are designed to describe the main aspects of an issue related to security. The set of elements can easily be extended to reflect either temporary, nor exotic or new requirements in a per-document manner. Besides addressing more than one problem within a single document the format allows to group information for more than one target group of readers as well as multi-lingual textual descriptions within one document. This can be used to selectively produce different renderings of an announcement for the intended target groups addressing one, a sub-set, or all problems multi- or mono-lingual in the languages provided.

References The according information is available via

- http://www.caif.info/

Common Advisory Format

The Common Advisory Format is intended to enable an easy exchange of advisory data between the CERTs participating in EISPP (European Information Security Promotion Programme). The advisory format merges the best-practice information regarding security advisories of these CERTs. The format is defined using XML, so the various standards and standard tools of the XML-family can be used for advisory processing.

References The according information is available via

- http://www.eispp.org/

German Advisory Format – DAF

The German Advisory Format (DAF) is based on the EISPP Advisory Format. The authors assume that the document may also be of interest for the European and international CERT community, especially because DAF actively maintains dynamic parts of the advisory standard.

References The according information is available via

- http://www.cert-verbund.de/daf/daf_description.html

4.4.3 CSIRT Co-operation Activities in Europe

Caused by the great number of various CSIRTs in specific countries (e.g. Germany and the United Kingdom) some cooperation and coordination initiatives has been founded in European countries. Some examples are:

- CERT-Verbund (Germany)
  The German national CERT-Verbund is an alliance of German security and emergency response teams. The CERT-Verbund provides the German teams with a framework for co-operation and information sharing. Besides this, all the single teams stay autonomous in their responsibility for their respective constituency.

Reference: http://www.cert-verbund.de/

- circa – Computer Incident Response Coordination Austria
  The Austrian security network circa is a confidential and protected electronic communication network ("Web of Trust") between network- and safety officers of Internet Service Providers (ISPs) and other carriers of IP-networks, from the private as well as from the public sector (Private Public Partnership).

Reference: http://www.circa.at/ (German language only)

- E-COAT – European Cooperation of Abuse Fighting Teams
  E-coat aims to further the cooperation of Internet abuse fighting teams of network/information service providers in Europe, and jointly produce tangible results that will benefit its constituency and beyond and help them more effectively combat Internet based network/computer abuse. To further these goals, e-coat will co-operate with existing anti-abuse and CERT fora in and outside Europe.

Reference: http://www.e-coat.org/

- EGC – European Government CSIRTs Group
  The European Government CSIRTs group (EGC) is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.
  Current members of the European Government CSIRTs group:
  - CERTA – France
  - CERT-Bund – Germany
  - CERT-FI – Finland
  - GOVCERT.NL – The Netherlands
  - SITIC – Sweden
  - UNIRAS – United Kingdom

- NorCERT – Norway

Reference: http://www.bsi.de/certbund/EGC/index_en.htm

- NordUNET
  NORDUnet is an international collaboration between the Nordic national networks for research and education. It interconnects these networks and connects them to the worldwide network for research and education and to the general purpose Internet. The current physical connections are shown on the connectivity map referenced below.

Reference: http://www.nordu.net/
http://www.nordu.net/connectivity/

- TF-CSIRT – Task Force of Computer Security and Incident Response Teams
  This Task Force is established to promote the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. The main goals of the Task Force will be to provide a forum for exchanging experiences and knowledge, to establish pilot services for the European CSIRTs community and assist the establishment of new CSIRTs, to promote common standards and procedures for responding to security incidents.

Reference: http://www.terena.nl/tech/task-forces/tf-csirt/

- UKCERTs
  UKCERTs is an informal forum of UK CSIRT teams with participants from the government, academic, corporate and commercial CERTs. The forum has quarterly meetings of up to 25 members, with presentations provided by team members and invited information security experts. The forum is designed to encourage co-operation and information sharing between the participants. UK WARP (Warning Advise and Reporting Point) teams also recently attended the meetings, enhancing the relationship between the UK CSIRT and WARP communities.

4.4.4 International CSIRT Co-operation and Initiatives outside of Europe

- APCERT – Asia Pacific Computer Emergency Response Team
  The Asia Pacific Computer Emergency Response Team (APCERT) is a coalition of CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) of 17 teams from 13 economies across the Asia Pacific region, aiming to foster international collaboration, as the nature of security incidents on the Internet makes international collaboration increasingly vital.

  APCERT organizes an annual meeting called APSIRC conference

- APCERT & CNCERT 2006 Conference, MARCH 28-31 2006, Beijing, Chinese
- APSIRC 2005 - 22-24 February 2005, Kyoto, Japan
- APSIRC 2004 - 23-25 February 2004, Kuala Lumpur, Malaysia
- APSIRC 2003 - 24-25 February 2003, Taipei, Chinese Taipei
- APSIRC 2002 - 24-26 March 2002, Tokyo, Japan

and an annual Report consisting of APCERT members annual activities, incident response statistics, analysis and trends, as well as our future plans.

APCERTs members come from

- Australia (AusCERT – Australian Computer Emergency Response Team)
- Chinese Taipei (TWCERT/CC – Taiwan Computer Emergency Response Team / Coordination Center; TWNCERT – Taiwan National Computer Emergency Response Team)
- Hong Kong, China (HKCERT – Hong Kong Computer Emergency Response Team Coordination Centre)
- Indonesia (IDCERT – Indonesia Computer Emergency Response Team)
- Korea (KrCERT – Korea Internet Security Center)
- Japan JPCERT/CC (Japan Computer Emergency Response Team / Coordination Center)
- Malaysia (MyCERT – Malaysian Computer Emergency Response Team)
- Negara Brunei Darussalam (BruCERT – Brunei Computer Emergency Response Team)
- People's Republic of China (CCERT – CERNET Computer Emergency Response Team; CNCERT/CC – National Computer network Emergency Response technical Team / Coordination Center of China)
- Philippine (PH-CERT – Philippine Computer Emergency Response Team)
- Thailand (ThaiCERT – Thai Computer Emergency Response Team)
- Singapore (SingCERT – Singapore Computer Emergency Response Team)
- Vietnam (BKIS – Bach Khoa Internetwork Security Center)

Reference: http://www.apcert.org/index.html

- FIRST – Forum of Incident Response and Security Teams
  The Forum of Incident Response and Security Teams (FIRST) consists of a network of individual computer security incident response teams that work together voluntarily to deal with computer security problems and their prevention. These teams represent government, law enforcement, academia, the private sector, and other organizations with justifiable interest as determined by the Steering Committee.
  Currently FIRST has more than 170 members, spread over the Americas, Asia, Europe and Oceania.

FIRST and its members are dealing with the following tasks

- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations from around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

Reference: http://www.first.org/

4.5 Trusted Shops

4.5.1 Euro-Label

Euro-Label is the European electronic shopping Trust mark for consumers and retailers based on the European Code of Conduct. Euro-Label embodies four key principles:

- Fair trading
- Complaint handling
- Data protection
- Secure payments

Euro-Label guarantees that

- The company selling the product is reliable
- The selling conditions are clear and available on the website
- The trader respects laws on data protection
- The products will be delivered as specified when the consumer placed the order
- A dispute resolution procedure is in place if anything goes wrong during the transaction

The European Code of Conduct was drafted by Euro-Label in accordance with current and anticipated future European legislation. In particular it draws on the EU Directives on Electronic Commerce, Distance Selling, and Data Protection and on guarantees.

On its web site Euro-Label provides a list of certified shops in various countries (click at "search for certified shops"). This list provides links to trusted shops as well as links to the according certification bodies.

Reference The according sites are available via

- http://www.euro-label.com/euro-label/ControllerServlet

4.5.2 Trusted Shops

Trusted Shops was created in early 2000 in close cooperation with consumer protection agencies. The primary objective was to meet the demands made by leading politicians for better security in the internet and to confirm to the consumer that this security is here to stay.

Supported by the European Union, the Trusted Shops system is currently spreading across Europe, with particular focus on the United Kingdom, Germany, France, Belgium, the Netherlands, and Scandinavia. Today there are already well over 1.300 internet retailers operating under the Trusted Shops security standard to guarantee safe and secure shopping for their customers.

Reference The according sites are available via

- http://www.trustedshops.com/en/home/index.html

4.6 Sites to Combat Illegal Web Content

Europe

Insafe

Insafe is a network of national nodes that coordinate Internet safety awareness in Europe. The site provides a list of links to national nodes that participate in the initiative Insafe.

Reference http://www.saferinternet.org/ww/en/pub/insafe/

Safer Internet

Safer Internet is an awareness campaign promoted under the SafeBorders project, which is partly funded by the European Commission, under the Safer Internet Action Plan.

Reference http://www.safer-internet.net/

Germany

The German Awareness Node "klicksafe.de"

klicksafe.de organizes and leads a national marketing campaign directed toward improving public awareness on internet safety, employing various strategies such as:

- TV clips
- Direct approach to target groups
- Training courses for multipliers
- Topical events (regional and national)

klicksafe.de is one facet of the concerted measures taking place across Europe (see chapter 4.1.4, European Program “Safer Internet”) and aims to provide for Germany a platform and portal for diverse initiatives addressing the opportunities and risks presented by the internet.

Reference http://www.klicksafe.de/common/english.php

United Kingdom

Internet Watch Foundation

The UK hotline for reporting illegal content specifically:

- Child abuse images worldwide
- Criminally obscene content
- Criminally racist content

The site provides a list of links to national and international Hotlines that participate in the initiative.

Reference http://www.iwf.org.uk/

Internet Content Register

Internet Content Register is making the Internet safer by providing a register of official information sources, validated company profiles, and on-line consumer information.

Reference http://www.internet.org.uk/index.html

4.7 Commercial Sites like Symantec

Because there are a lot of commercial enterprises dealing with Internet security products, this chapter only lists some examples from various countries and with different main focus. The following commercial sites are listed in alphabetic order.

4.7.1 Acunetix

Acunetix Ltd was founded in 2004 with a view to secure companies' web applications and to combat web site hacking by developing an automated tool that could help companies scan their web applications for vulnerabilities. Since 2005 it distributes *Acunetix Web Vulnerability Scanner*, a tool that inspects websites for vulnerabilities to SQL injection, cross site scripting and other web attacks before hackers do. Acunetix is a privately held company with its offices in the US, Malta and the UK.

In this chapter Acunetix is listed as an example for a company that offers a free check of a visitor's web site.

Reference The according sites are available via

– http://www.acunetix.com/

4.7.2 Guidance Software Company

Guidance Software is a US company with a European office in UK. IT was founded in 1997 with the purpose to develop solutions that search, identify, recover, and deliver digital information in a forensically sound and cost-effective manner. According to the progress of the Internet it has moved into network-enabled investigations, enterprise-wide integration with other security technologies, and now, has developed search and collection capabilities for electronic discovery and other investigations. Guidance Software distributes the EnCase® Enterprise software toolkit to provide internal investigation, security incident response, and electronic discovery in enterprises.

Reference The according sites are available via

– http://www.guidancesoftware.com/commercial/index.asp

4.7.3 Internet Security Systems

Internet Security Systems, Inc. (ISS) is an internationally operating company. It was founded in 1994 and provides security products and services that preemptively protect enterprises and organizations against Internet threats. The company distributes the Proventia Enterprise Security Platform (Proventia ESP) and provides security services that help enterprises to design, implement, and maintain a reasonable security strategy.

Internet Security Systems is headquartered in Atlanta, USA and has facilities in North America, South America, Africa, Europe, Middle East, Australasia, and Asia.

Reference

Internet Security Systems provides web sites in various languages, one of it is Japanese. The according sites are available via

- http://www.iss.net/about/
- http://www.isskk.co.jp/

4.7.4 InformationWeek and InformationWeek LIVE

InformationWeek is a German electronically published magazine that is intended to help IT decision makers to understand technologies, to compile strategies and to select products. The magazine makers aim to translate the message of IT providers into use arguments for the IT investment managers in enterprises. One of the main focuses of the magazine is IT security.

Beside the magazine the editorship of the InformationWeek created a communication platform for the personal dialogue between manufacturers, dealers, IT managers and users in enterprises by organizing the InformationWeek LIVE Event series. Just as the magazine the meetings treat current topics e.g. IT Security or IT outsourcing and offer LIVE solutions, helpful hints and current trends from a technical and economical point of view.

InformationWeek accompanies the meetings editorial, publishes special editions to the main topics and takes part in the investigations for studies to the topic.

In this chapter InformationWeek is listed as an example for an Internet publisher and event manager in the area of IT security.

Reference

As an example for providing studies, have a look to chapter 2.2 “Vulnerability Effects” that adduces the online-study IT-Security 2004, published by InformationWeek Live (German language only).

- http://www.iw-live.de/security/start/index.php?page=4&lang=de
- http://www.iw-live.de/security/start/index.php?page=1

4.7.5 Qualys

Qualys, Inc. was founded in 1999. It is an internationally operating company, headquartered in California, USA, with European offices in France, Germany and the U.K., and Asian offices in Japan, Singapore, Australia, Korea and the Republic of China. Qualys' on demand vulnerability management solutions are intended to enable organizations to preemptively identify and revise network vulnerabilities, to measure and manage risks, and to ensure compliance with regulatory requirements. The company distributes the QualysGuard® service for large distributed organizations (QualysGuard® Enterprise), small to medium sized organizations (QualysGuard® Express), professional services organizations (QualysGuard® Consultant), for managed service providers (QualysGuard® MSP), and for organizations requiring an onsite security operations center (Qualys® @Customer).

Reference

Qualys provides web sites in various languages. The according sites are available via

- http://www.qualys.com/
- http://www.qualys.com/company/contacts/france/
- http://www.qualys.com/company/contacts/germany/
- http://www.qualys.com/company/contacts/uk/

4.7.6 RSA Security

RSA Security's is an internationally operating enterprise with a portfolio of identity and access management solutions that are intended to help organizations protect private information and manage the identities of people, devices and applications accessing and exchanging that information. It is specialized in the following topics.

- *Identity and access management* will help organizations to optimize their business processes and build online relationships with customers, partners and employees
- *Secure mobile and remote access* offers a range of authentication options enabling secure network access from outside a firewall
- With *secure enterprise access* it is possible to control secure access to business-critical information resources within the enterprise through easy login procedures such as SingleSignOn
- *Secure transactions* is a cross-platform technology that verifies the sender and path of all business communications and ensures that those messages are protected
- *Consumer Identity Protection* allow e-businesses to provide their customers a security device to prove their identity, and once a consumer's identity is authenticated, he or she can conduct transactions seamlessly across applications and web sites

Reference

RSA Security provides web sites in various languages, one of it is Japanese. The according sites are available via

- http://www.rsasecurity.com/

- http://www.rsasecurity.com/node.asp?id=1048
- http://www.rsasecurity.com/japan/

4.7.7 Symantec

Symantec is an internationally operating enterprise providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Symantec is headquartered in California, USA and has facilities in more than 40 countries, with research and development facilities located in:

- Australia
- Belgium
- Canada
- China
- Germany
- India
- Ireland
- Israel
- Japan
- New Zealand
- United Kingdom
- United States

Technology currently provided by Symantec, is separated into four categories:

- Consumer Products
- Enterprise Security
- Enterprise Availability
- Services

Symantec also operates a number of Security Operations Centers and Security Response Labs, providing 24x7 information security expertise.

Two times a year Symantec publishes the "Symantec Internet Security Threat Report" that analyzes and discusses the Internet security activities over a period of six months.

Reference

Symantec provides web sites in various languages, one of it is Japanese. The according sites are available via

- http://symantec.com/
- http://www.symantec.com/globalsites.html
- http://www.symantec.com/region/jp/

4.7.8 Utimaco Safeware AG

Utimaco Safeware AG is a European manufacturer of professional IT security solutions. The security technology and solutions developed by Utimaco are intended to protect the electronic data of companies and government bodies against unauthorized access and to guarantee that business processes and administrative procedures in the electronic world are binding and confidential. To complete its portfolio Utimaco entered into partnerships with technology oriented companies, certified sales partners, and worldwide resellers.

Utimaco is an internationally operating enterprise and has offices in 7 European countries, in the USA and Japan, as well as sales partners in Europe, Asia, Australia and Africa.

Reference Utimaco Safeware AG provides web sites in various languages, one of it is Japanese. The according sites are available via

- http://www.utimaco.com/indexmain.html
- http://www.utimaco.com/uij/indexmain.html

4.8 Non-profit Organizations like TeleTrusT

The initiatives and non-profit organizations are listed in alphabetic order.

4.8.1 Association Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is an international pan-industrial and law enforcement association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks.

Membership is open to qualified financial institutions, online retailers, Internet service providers, the law enforcement community, security solutions providers and research institutions. Actually more than 2000 members and 1300 companies and agencies worldwide take part in the APWG association.

Reference The according site is available via

- http://www.antiphishing.org/index.html

4.8.2 CERIAS

The Center for Education and Research in Information Assurance and Security (CERIAS) is a national center for research and education in areas of information security that are significant to the protection of critical computing and communication infrastructure.

It is listed as an example for an organization that is focused on education and research in the areas listed below:

- Risk Management, Policies, and Laws
- Trusted Social and Human Interactions
- Security Awareness, Education, and Training
- Assurable Software and Architectures
- Enclave and Network Security
- Incident Detection, Response, and Investigation
- Identification, Authentication, and Privacy
- Cryptology and Rights Management

CERIAS is located in Indiana, USA, on the Campus of the University of Purdue.

Reference

It is publishing a hot list of tools and resources in the area of commercial sites security at

- http://www.cerias.purdue.edu/tools_and_resources/hotlist/details.php?id=47

4.8.3 Initiative D21

Initiative D21 is a German public private partnership, where more than 400 representatives of enterprises, associations, parties, political institutions and other organizations are currently involved.

The shared goal of the Initiative D21 is to improve the general conditions necessary to move successfully into the information and knowledge society.

One of its working groups is “Team 5 – Security and Trust on the Internet” that provides projects and studies in the area of IT security criteria and IT baseline protection, security and trust on the Internet, and more security and mobility by using chip cards.

Reference The according site is available via

- http://www.initiatived21.de/english/index.php

4.8.4 Initiative "Deutschland sicher im Netz"

In January 2005 thirteen partners from society, politics and economics started the initiative "Deutschland sicher im Netz" that aims to protect users against safety problems in the Internet. "Deutschland sicher im Netz" addresses itself particularly to private users, children and young people, authorities and institutions as well as small and middle enterprises. The initiative intends to sensitize these users for the potential dangers in the Internet, and to inform comprehensively how the own on-line protection can be improved fast and effectively.

For this reasons the initiative runs a web site that provides various information and tools, in particular target group oriented online safety check lists as well as check lists on CD. In addition it provides an online training that addresses IT specialized dealer and aims at a certification as an official security consultant.

Reference The according site (German language only) is available via

- https://www.sicher-im-netz.de/

4.8.5 Signaturbündnis

The Signature Alliance (German: Signaturbündnis) has been established in April 2003 as a joint initiative of the business community and administrations. The aim of the Signature Alliance is that all citizens will be able to use a chip card based on a standardized technical infrastructure and issued by various providers.

In a joint declaration, the Alliance partners agreed in particular on:

- technical standards for the applications and products used
- the use of multi-functional chip cards
- common security standards, and
- the use of advanced and qualified electronic signatures.

Reference The according site is available via

- http://www.signaturbuendnis.de/englisch/index.htm

4.8.6 StopBadware.org

StopBadware.org is an international "Neighborhood Watch" campaign aimed at fighting badware. The initiative intends to provide reliable, objective information about downloadable applications in order to help consumers to make better choices about what they download on to their computers. Organizers of the initiative are the Berkman Center for Internet & Society at Harvard Law School, the Oxford Internet Institute, and the Consumer Reports WebWatch, a grant-funded project of Consumers Union (an American consumer protection organization). It is sponsored by the IT enterprises Google, Lenovo, and Sun microsystems.

Reference The according site is available via

- http://www.stopbadware.org/

4.8.7 TeleTrusT Deutschland e.V.

TeleTrusT Deutschland e.V. was established in 1989 as a non-profit, politically and economically independent organization for the promotion of trustworthiness of information and communication technology in open system environments.

One of its main goals was to support research into methods of safeguarding electronic data interchange, application of its results, and development of standards using digital signatures as an instrument conferring legal validity on electronic transactions.

Reference The according site is available via

- http://www.teletrust.de/index.php?id=328

4.8.8 Web Application Security Consortium

The Web Application Security Consortium (WASC) is an international group of experts, industry practitioners, and organizational representatives. Its mission is to

- build an open forum for the creation, discussion, and dissemination of knowledge pertaining to web application security,
- educate the market regarding web application security related matters, and
- build a vendor neutral representation of the web application security industry.

WASC continuously publishes technical information, contributed articles, security guidelines, and other useful documentation.

Reference The according site is available via

- http://www.webappsec.org/

SIT

Fraunhofer Institut
Sichere Informations-
Technologie

4.9 Fraunhofer Institut SIT – Security Test Lab

The Security Test Lab at the Fraunhofer Institute for Secure Information Technology SIT supports manufacturers and users in detecting and eliminating vulnerabilities at an early stage.

In the Security Test Lab all types of networked systems are examined for flaws and errors – system designs and prototypes as well as finished products. Complete systems, subsystems or individual components are tested, as required.

In the Security Test Lab is considered both formal requirements, like the Common Criteria, and the actual processes of real-life attacks. Systems can be tested as a black box, in for-delivery status, or as a white box, comprising design documents and source code.

In the Security Test Lab are tested

- Client and server software
- Embedded systems
- Mobile devices
- Telecommunication equipment

Reference

The according information is available via

- http://www.sit.fhg.de/cms/media/en/pdfs/testlabor.pdf

5 Conclusion

The increasing use of the Internet for commercial operations requires increasing information security, privacy, and data protection.

This is considered as well as for e-commerce vendors that must provide high availability of their sites to attract and bind their customers. Furthermore they have to guarantee confidentiality and privacy of personal customer data. In addition they may provide money-back guarantee free of charge for the consumers.
It is as well considered for enterprises, because the Internet opens up a new quality for industrial and competitive espionage. Targets of spying out and manipulating data and services are technology and know-how theft as well as getting the competitive advantage, e.g. through obtaining by fraud tenders, contracts, or price lists. Competitors may also gain access to sensitive research and development data.
The loss of data confidentiality can result in economic damage, and if the general public learns about the misuse of data a company's image may suffer.

One of the growing attacks is password fishing (Phishing). Delivery via web site, email or instant message, the attack asks users to click on a link to *re-validate* or *re-activate* their account. Attackers leverage the trust of well-known enterprises or public services to gain valuable information; usually details of accounts, or enough information to open accounts, obtain loans, or buy goods through e-commerce sites. Phishing attacks are one of the highest visibility problems for banking and e-commerce sites. Banks, Internet service providers (ISPs), stores and other Phishing targets are victimized as well as their (potential) customers.

Another increasing and more sophisticated performed attack, e.g. by using regional known sender addresses, is the delivery of Spam mails. As a result of a large number of Spam mails, a loss of working hours, an overloading of technical components and higher costs due to unsolicited data transfers occur. But Spam mails are also used by attackers to deliver malware, e.g. mass mail worms, Trojan horses, or viruses.

Another trend is the use of Bot networks. Attackers try to bring infected computers under their control and misuse them for criminal use. These Bot networks often consist of several thousands hacked computers and even are rented out for spreading malware or performing DoS attacks.

Furthermore there is an enhancement of traditional in-house company networks through the growing use of mobile computers and wireless transmission technologies. This new technologies have to be secured in a specific manner, e.g.

by using virtual private networks for interconnection between external and internal networks.

More and more Internet criminality is conducted in a professional and commercial fashion, where financial interests are the driving motivation to perform threads. Attackers aim at getting money by misusing IT systems through the distribution of Spam and malware to obtain by fraud sensitive data such as credit card numbers or online banking data.

For all these reasons it is important that consumers, vendors, Internet providers and companies participate in the countermeasures described in chapter 4.
Recommendations of Security Agencies, Data Protection Agencies, and other comparable institutions should be taken in attention and implemented.

In Europe the participation in security programs and projects founded by the European Union is a good way to establish a single and competitive market.

People will only be able to utilize the advantages of the information technologies and their world-wide network systems without limitations if they succeed in protecting them.

6 References

[BSI-En] The Federal Office for Information Security (BSI), http://www.bsi.bund.de/english/index.htm

[BSI-Status-R] Die Lage der IT-Sicherheit in Deutschland 2005 (*means*: The State of IT Security in Germany 2005), Stand July 2005, http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf

[BSI-WebServ] Erkennung und Behandlung von Angriffen aus den Internet (*means*: Identification and Treatment of Internet Threats), http://www.bsi.de/fachthem/sinet/webserv/angriff.htm

[CERT-ENISA] ENISA Inventory of CERT activities in Europe, Version 1.0, 12/2005, http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert.pdf

[ConFreeEU] Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.: 005, entry into force: September 3rd, 1953, http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG

[DsiN] Deutschland sicher im Netz (*means*: Secure use of the Internet in Germany), legal notice Microsoft Deutschland GmbH, https://www.sicher-im-netz.de/default.aspx?initiative/partner/default

[IuKDG-En] Guideline to the Information and Communication Services Acts, http://www.iukdg.de/english.html

[INet-Security] Security of the Internet – February 1998, http://www.cert.org/encyc_article/tocencyc.html

[IT-Sicherheit] C. Eckert, IT-Sicherheit – Konzepte, Verfahren und Protokolle (means: IT Security – Concepts, Methods, and Protocols), 3-te überarbeitete und erweiterte Auflage, Oldenbourg-Verlag, 2004

[IW-Live-Study] Online-study IT-Security 2004, InformationWeek Live, CMP-WEKA Verlag GmbH & Co. KG, April-June 2004, http://www.iw-live.de/security/start/index.php?page=4&lang=de

[OWASP-Guide] The Open Web Application Security Project, A Guide to Building Secure Web Applications and Web Services, 2.0 Black Hat Edition, July 27th, 2005

[OWASP-TopTen] http://www.owasp.org/documentation/topten.html

[PCI-DSS] AMEX, Visa, Mastercard, Discover, JCB, Diner's Club – Payment Card Industry (PCI) Data Security Standard, January 2005, https://sdp.mastercardintl.com/pdf/pcd_manual.pdf

[REG-ENISA] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 (OJ L 77, 13 March 2004), http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_077/l_07720040313en00010011.pdf

[RFC-1244] RFC 1244, Site Security Handbook, J.P. Holbrook, J.K. Reynolds, July 1st, 1991, (Obsoleted by RFC 2196, Status: INFORMATIONAL)

[RFC-2196] RFC 2196, Site Security Handbook, B. Fraser, September 1997 (Obsoletes RFC 1244, Status: INFORMATIONAL)

[RFC-1281] RFC 1281, Guidelines for the Secure Operation of the Internet, R. Pethia, S. Crocker, B. Fraser, November 1991 (Status: INFORMATIONAL)

[Sym-Threat-R] Symantec Internet Security Threat Report, Trends for January 05 – June 05, Volume VIII, Published September 2005, http://enterprisesecurity.symantec.com/content.cfm?articleid=1539

[TNS-INFRA] TNS Infratest, Monitoring Informationswirtschaft, 8. Faktenbericht – Juni 2005, Abbildungen/Folie186.JPG (Monitoring the Information Economy – 8th Factual Report – June 2005), http://www.tns-infratest.com/06_BI/bmwa_english/Faktenbericht_8/06480_index_bmwa.asp

7 Appendix

7.1 Abbreviations and Acronyms

ARPANET	Advanced Research Projects Agency Net
Bot	short for robots
CGI	Common Gateway Interface
CNP	Cardholder Not Present
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
DMZ	DeMilitarized Zone – A DMZ is subnetwork that is situated between a trusted internal network and an external public network such as the Internet.
DNS	Domain Name Service
email	Electronic Mail
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MIME	Mail Extension Protocol
NFS	Network File Service
RFC	Requests for Comments
RPC	Remote Procedure Call
S/MIME	Secure Mail Extension Protocol
SMTP	Simple Mail Transfer Protocols
SSL	Secure Socket Layer
SYN	short for synchronization
TCP	Transport Control Protocol
TeleTrusT	Non-profit organization for the Promotion of Trustworthiness of Information and Communication Technology
TLS	Transport Layer Security
URI	Uniform Resource Identification
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Networks
web	World Wide Web
WWW	World Wide Web

7.2 List of Figures

Note: to be completed