REPUBLIK ÖSTERREICH

Cyber Security Report 2014

BUNDESKANZLERAMT ÖSTERREICH

Bundesministerium für europäische
und internationale Angelegenheiten

BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

Bundesministerium
für Landesverteidigung
und Sport
bmlvs.gv.at

Publishing information

Media owner, publisher and editor:
Federal Chancellery of the Republic
of Austria, Department IV –
Coordination,
Division IV/6 – Security Policy Affairs
Ballhausplatz 2, 1010 Vienna

Graphic design: Federal Chancellery |
ARGE Grafik Vienna, May 2014

Table of Contents

1 Introduction

In accordance with Austria's Cyber Space Security Strategy (Österreichische Strategie für Cyber Sicherheit / ÖSCS), the Cyber Security Steering Group has to prepare an annual Cyber Security Report. The first report on cyber security in Austria has to be submitted to the Steering Group by June 2014. The Steering Group will inform the members of the federal government represented in the National Security Council and other members of the government who are responsible for these issues.

The aim of the report is to provide a **summary review of the cyber threats** and other important **national and international developments** in the **preceding year**. The Cyber Security Report is based on the thematically relevant reports issued by the individual ministries.

2 Cyber situation in 2013 / threat analysis

Our present-day society is becoming more and more dependent on technological progress and, consequently, on the confidentiality, availability and integrity of information. States, various social groups but also criminal actors are expanding their ICT »tools«; criminal activities committed via the Internet are thriving. In the age of »digital natives«, the skills of an individual may in fact become a cyber weapon.

2.1 Actors and their intentions

Significant threats in cyber space are caused by individual **state actors,** trying to use cyber space to implement national political and economic interests. In parallel, governments take measures to obtain information supremacy (e.g. propaganda in social media). In 2013 the spotlight was turned particularly on government-controlled **cyber espionage**. Besides Chinese cyber espionage operations, the activities of the US National Security Agency (NSA) should be mentioned in this context. Data collection programmes (such as Prism), which had originally been introduced to combat terrorism, were also used for cyber espionage. Other states have programmes similar to those of the USA.

Another field of criminal activity that should be mentioned in connection with the improper use of the Internet is **economic and industrial espionage**.

Cyber criminals play an important role at a non-governmental level. The perpetrators use the Internet as a crime scene for their world-wide criminal machinations. Their criminal motives range from money-making through spamming[1], phishing[2] and / or pharming[3] to credit card fraud and the sale of confidential data. Criminal organisations offer the technology (both hardware and software) for carrying out cyber attacks against payment to »everyone«. The Internet is not only a crime scene where fraud and financial crimes flourish. It is also an »enabling factor« for all sorts of dangerous cyber attacks against authorities, institutions and enterprises.

[1] Today bulk e-mail messages for advertising purposes account for a major part of the Internet traffic.

[2] Attempts to deceive users through e-mails (»Click on this link, otherwise your account will be suspended!«) and to prompt them to take harmful actions (e.g. by clicking on a link to a malicious website in an e-mail). Very often the aim is to extract access data (user names, passwords) to assume the digital identity of a user (user profile) and misuse it for criminal activities.

[3] Redirecting from a correct website (e.g. www.google.com) to a fake and malicious website controlled by an attacker. In most cases, this website is deceptively similar to the original. The user input (user name, password, TAN codes, etc.) is forwarded to an attacker controlling the fraudulent website.

Terrorists use cyber space predominantly for radicalisation, recruiting as well as financing terrorist operations.

»Hacktivists« (Internet activists) are a special type of online actors. As they are usually expressing their dissatisfaction through Distributed Denial of Service (DDoS) attacks[4] or website defacement[5], they could also be described as online protestors in cyber space. H ackers engaged in politically or socially motivated activities in Austria in 2013. The incidents were, however, considerably more harmless than those observed in 2012. The Anonymous movement is the best-known community of hacktivists. In its beginnings, persons joined under the guise of Anonymous to protest against global problems (e.g. infringement of the freedom of speech) or to promote the freedom of the Internet. An increasing number of Anonymous groups focusing on national or regional issues has been emerging in the course of time. Besides ordinary hacktivists, there are also »patriotic hackers«, who are often associated with their government, e.g. the Syrian Electronic Army.

Finally, individual **hackers or groups of hackers** should be mentioned. Driven by various motives, they can cause significant damage through their attacks. However, as recent trends show, »traditional« hackers intruding systems out of curiosity and for playing around have become a relatively small threat.

2.2 Methods

The **aim** of cyber attacks is to compromise the confidentiality, integrity and / or availability of networks, of the equipment used in these networks or the data and services provided on them. There are **three categories** of cyber attacks:

1. **Targeted attacks against a specific target** or a selected circle of specific targets. This method is chosen to attack well-protected targets; the malware is tailored to each individual victim. Time-consuming and resource-intensive preparations are required. As far as the actual effects of these attacks are concerned (particularly in terms of data leakage and possible external control), this type of attack (which is also called »advanced persistent threat« or APT) poses the **most significant threat**.
2. **Attacks** against a **specific group of persons**. The attack is directed against a group of persons whose common denominator motivates the perpetrator to launch the cyber attack.
3. **Large-scale simultaneous attacks** against **a maximum of targets**. This type of attack is carried out to steal information from as many unidentified computers as possible. Usually, systems with a low level of protection are attacked.

There are **numerous means and methods** to launch successful attacks in and via cyber space. The main attacks identified in 2013 were **spying on access data, embedding malware** in websites, **compromising of databases** as well as **disrupting the availability** of an individual

[4] Distributed Denial of Service: a type of attack where a server is »bombarded« with so many requests from numerous systems until it breaks down due to being overwhelmed; as a result, the services provided on it become unavailable.

[5] Infiltration of a server and changes to the websites stored on it.

services of a network. These attacks were carried out partly in combination with, and very often with the aid of, known malware; in some cases they were launched with programs developed for a specific purpose.

The **infection of Windows PCs** is still the most common way of invading corporate networks. However, Windows itself does no longer pose the most serious problems. The programs used to present Web content (e.g. PDF Viewer, text processing software, Web browsers[6] and their plug-ins[7]) are much more prone to infections. Data manipulated with malware are sent by e-mail by the attackers, referenced through links or embedded into popular websites through webhacks. Due to »social engineering«[8] (e.g.»Open this reminder/ Telecom invoice / …«), technical flaws are no longer a prerequisite for infections, and even technical security measures that are implemented properly can be evaded easily. Hence, attackers may gradually penetrate the critical systems of corporate and public networks in order to compromise them.

Another method of attack is to **invade the services** of potential victims that are **accessible on the Internet**. The websites of associations, groups and SMEs, schools as well as public authorities are particularly vulnerable. In these cases, the attacker is more interested in the resources and visitors of the server attacked than in the victim per se.

Since 2013 »Distributed Reflected Denial of Service Attacks« have been used increasingly to **attack the availability of online services**. The attacker sends numerous small falsified requests on behalf of the victim to legitimate servers; due to their size and large number, the subsequent replies block the victim’s network connection; as a result, the respective online service is no longer accessible.

In general, a marked increase in malware attacks directed at **mobile phones** could be observed in 2013. Moreover, cyber criminals are focusing more strongly on **social networks,** which they use for committing and preparing various criminal offences. Due to their widespread use, **smartphones and tablets** also became attractive targets; a huge number of malware programs targets Android (the world’s most popular mobile operating system for smartphones and tablets). Even though technical security solutions have become available to protect these devices, user security awareness is relatively low compared to the sensitisation level of PC and notebook users.

The methods of attack described above were used also, and above all, in the context of **identified targeted attacks in 2013**. As most cases showed, these cyber attacks were realised through spear phishing[9] carried out via e-mails containing malware in attachments. During 2013 it became clear that some of the cyber actors expanded and / or changed their practices. Another fact worth mentioning is that an increasing number of malware programs uses valid and verifiable digital certificates[10]; this also points to the increasing professionalisation of the actors of today’s malware scene.

[6] A software program used to display Web pages (e.g. Internet Explorer).

[7] An add-on program for Web browsers, offering additional features (e.g. to display flash videos on YouTube).

[8] An umbrella term for attacks which do not target technical systems (e.g. PCs) but their users.

[9] A phishing attack specifically developed for a targeted group of victims (e.g. members of a specific mailing list)

[10] In the context of information security, digital certificates are used as an identifying feature to authenticate the source of data.

2.3 Weaknesses

It is a pointless exercise to highlight individual technical weaknesses as they are usually subject to great volatility. The following overview provides only a deliberately general description:

- Potential attackers concentrate more strongly on the **application layer** as the network layer is reasonably controllable thanks to the implementation of security measures at the technical level. The human user is, however, a permanent weak point in any information system. Attackers often do not have to take advantage of technical flaws as they can trick users into acting contrary to their own interests, e.g. through social engineering.
- While 10 years ago, **mobile phones / SMS** were considered to be trustworthy communication channels, this is no longer the case in 2013: due to the complexity of **smartphones** and the proliferation of apps, **malware** can spread considerably more easily **to mobile phones**.
- User names and passwords alone are not sufficient for **protecting access to sensitive Web applications**. Internet fraudsters increasingly take advantage of the fact that passwords are reused by the users.
- Ongoing **software updates** pose massive management problems, ranging from the browser plug-ins of private PCs to the Web server software of enterprises.
- **The end of XP support**: As support for Windows XP was ended by Microsoft, a large number of PCs has been becoming more vulnerable since April 2014. This is due to the fact that it is impossible to eliminate security gaps which have not yet been identified. Existing anti-virus software does not provide a suitable cushion against these risks.

3 International developments

Cyber security issues have been addressed and discussed by numerous international organisations and multilateral forums in the last few years. The relevant foreign policy measures are coordinated by the Austrian Foreign Ministry (BMEIA).

The fast-paced cyber developments raise a number of serious issues regarding fundamental and human rights. In general, Austria promotes the freedom of the Internet at international level, by emphasising the need to ensure the implementation of all human rights also in virtual space. It is, however, important to strike a balance between the interests related to the prosecution of cyber crimes and the respect of fundamental human rights, such as the right to freedom of expression and information as well as the right to a private life and to privacy.

3.1 European Union

The EU addresses cyber security issues particularly within the framework of its »**Digital Agenda for Europe**« adopted in 2010. Together with the Commission, the High Representative for Foreign Affairs and Security Policy presented an EU Cyber Security Strategy in early 2013. The Communication titled »An Open, Safe and Secure Cyberspace« contains a number of proposals, e.g. to further develop capabilities, improve cooperation and communication as well as to strengthen a coherent international cyber space policy for the EU. Another goal is to enhance the common cyber defence policy – this request was reiterated in the conclusions of the European Council (EC) regarding a Common Security and Defence Policy (CSDP) adopted in December 2013. Cyber capabilities are to be enhanced and further developed on the one hand. On the other hand, the document provides for the definition of an EU Cyber Defence Policy Framework.

The activities in this area are supported by the **European Network and Information Security Agency (ENISA)**. Its task is to improve network and information security together with the Member States and the other EU institutions. Within the framework of the **European Cyber Security Month** organised by ENISA in October on the initiative of the EC, the Austrian Foreign Ministry provided detailed information to all Austrians living abroad, Austrian expat associations and Austrian honorary consulates whose e-mail addresses were available.

On 12 February 2013 the EC submitted a Proposal for a Directive of the EP and the Council concerning measures to ensure a high common level of network and information security (NIS) across the Union to the Member States. The so-called NIS Directive is an integral part of the measures to implement the EU Cyber Security Strategy. It is currently being discussed in the Council and the EP. The following key issues were identified:

- adoption of a national NIS Strategy as well as the establishment of a NIS authority and a GovCERT / CERT (Computer Emergency Response Team) as an IT emergency team;
- mandatory risk management for critical infrastructures and reporting requirements for security incidents;
- development of an EU-wide NIS cooperation network to exchange information on incidents and the data relevant for clarifying them.

3.2 United Nations

The **World Summit on the Information Society (WSIS)** had been called into life by the General Assembly of the United Nations (UN GA) already at the turn of the century. The International Telecommunication Union (ITU) played the leading role in organising the WSIS, in which state actors participate alongside with NGOs, civil society groups and the private sector. Within the framework of WSIS, progress made towards the information society in the last decade is being evaluated.

The third **Conference on Cyberspace** was held in Seoul in October, in which about 90 delegations (half of which at ministerial level) participated. Austria was represented by the Foreign Ministry and the Federal Ministry of the Interior. The conference focused on issues such as the Internet and economic growth and development, the social and cultural benefits of the Internet, cyber security, the standardisation of cyber space and capacity building. The well-known differences between the Western, Chinese and Russian positions and the difficulties in agreeing on an international set of cyber-related standards manifested themselves once more.

Cyber issues were also addressed by some committees of the UN GA. Besides the **First Committee**, which monitors developments in the area of information and telecommunication in the context of the international security regime, Austria also attaches great importance to the work of the **Third Committee**. Germany and Brazil submitted the draft resolution "The right to privacy in the digital age". Austria had participated intensively in developing the text. Following the request of Germany and Brazil, Austria – together with a small group of other countries (including Liechtenstein, Switzerland, France) – submitted the Draft Resolution at the earliest possible date. Resolution A/RES/68/167 was finally adopted unanimously by the Social, Humanitarian & Cultural Committee at the 68th Session of the UN GA in late November 2013. Its main objectives are to strengthen the fundamental right to the protection of privacy and to implement Art. 17 of the International Covenant on Civil and Political Rights (ICCPR).

In addition, the UN had requested an open-ended intergovernmental expert group – set up within the UN Office on Drugs and Crime (UNODC) – to prepare a comprehensive study on cyber crime. The expert group presented the report in February 2013. Some UN Member States urged to start deliberations on a UN Convention to combat cyber crime. This was, however, rejected by a majority.

3.3 NATO

As a defence alliance, NATO has been addressing the defence aspects of cyber issues no later than upon adopting its new strategic concept in 2010. Austria cooperates closely in this area with NATO as a partner country. In 2013 informal political consultations on cyber issues were held between the six Western European partners (WEP-6: Switzerland, Ireland, Finland, Malta, Sweden, Austria) and NATO, on the one hand; on the other hand, Austria participated in numerous meetings of the NATO-C3 Board on cyber cooperation at a technical level.

Within the framework of its bilateral cooperation with NATO, Austria was represented by a cyber expert at the NATO-Ukraine Expert Staff Talks on Cyber Defence (November 2013, Yalta). The Austrian expert described the development and main elements of the Austrian Cyber Security Strategy (ÖSCS).

Within the framework of the NATO Partnership for Peace (NATO/PfP), Austria adopted the **Partnership goals on »cyber defence«** and succeeded in meeting all requirements for the year 2013.

Furthermore, Austria intensified its cooperation with NATO in the area of cyber defence by posting an officer of the Ministry of Defence to the »**Cooperative Cyber Defence Center of Excellence« in Tallinn/Estonia,** who has been active there since October 2013.

In December 2013 the European Council decided to enhance cooperation between the EU and NATO. The European Defence Agency is therefore expected to strengthen cooperation with the NATO Centre of Excellence in Tallinn in the context of cyber issues. It is also likely to collaborate with the »Friends of the Presidency Group on Cyber Issues«, which had been called into life to support the implementation of the EU Cyber Security Strategy in 2013.

3.4 OSCE

The Ministerial Council of the Organization for Security and Co-operation in Europe (OSCE) endorsed a decision of the Permanent Council **on confidence building measures in the area of cyber security** in Kyiv in December 2013. The participating states were requested to establish points of contact for a dialogue on security of and in the use of information and communication technologies. They exchange information on their national organisations responsible for cyber security plans, both in the public and private sector. Moreover, they meet at least three times a year within the framework of the Security Committee of the OSCE to discuss new developments in the area of cyber security. By increasing transparency and building confidence between the OSCE countries as well as establishing networks between national experts, emphasis is placed on the freedom of the Internet, freedom of expression and the protection of privacy.

Other cyber-related activities that are relevant for Austria take place within the framework of **UNESCO**, the **Council of Europe**, the **Development Assistance Committee** of the Organisation for Economic Co-operation and Development (**OECD-DAC**) as well as **INTERPOL**.

3.5 Nation-states

3.5.1 United States of America

The **Office of Cyber Security and Communications** reports directly to the President. It is the supreme body providing a strategic direction on cyber security for the whole nation. The US Department of Homeland Security is responsible for the protection of nationwide ICT networks, cooperation with the operators of critical infrastructures and the prosecution of cyber criminals. The US Army Cyber Command was established in October 2010 to perform coordinating tasks.

The importance attached to cyber issues is reflected in the proposed budgets of the US government. In April 2013 President Obama submitted a budget draft to the government, in which more than EUR 9.5 billion were earmarked for cyber programs. The armed forces of the US also increased their investments in the development and expansion of offensive and defensive measures.

3.5.2 Russian Federation

President Putin signed the **Information Security Doctrine of the Russian Federation** already in 2001; it is still valid today. The Russian Federation holds the view that a **strong control of national ICT infrastructures** as well as an **international agreement to regulate the Internet** are necessary. To tighten control over the national information space, the Russian government also adopted a law in March 2013. It stipulates that websites with »dangerous content« must be blocked for children. The domestic intelligence service FSB is responsible for cyber security at national level. To detect cyber attacks as early as possible, President Putin instructed the FSB to expand its surveillance capabilities for ICT networks in October 2013. Russia's armed forces are also expanding their cyber capabilities.

3.5.3 People's Republic of China

The Chinese leadership became aware of the need to create **information superiority in cyber space** already in the early 1990s. The Ministry of State Security is responsible for the protection and surveillance of national ICT infrastructures. The Chinese government considers the targeted control of information flows on the Internet in general and in social media in particular necessary to guarantee national security. In 2013 it adopted inter alia a new law which provides for sentences **of up to three years of imprisonment for disseminating rumours via the Internet**.

In January 2013 the Chinese government acknowledged for the first time the existence of hacker units in the armed forces, the so-called »Cyber Blue Teams«.

3.5.4 United Kingdom

In 2009 the **Office for Cyber Security and Information Assurance** was set up within the Cabinet Office. This Office published the national Cyber Security Strategy in 2011. Its key elements are the protection of the economy and critical infrastructures as well as the combat against cyber crimes. About EUR 800 million had been allocated to implementing the strategy in the period up to 2015. In June 2013 the British Chancellor of the Exchequer informed that EUR 256 million had been earmarked for the **National Cyber Security Programme** (NCSP) of the Cabinet Office to safeguard the interests of the United Kingdom. The armed forces and intelligence services (especially the Government Communications Headquarters / GCHQ) are expanding their cyber capabilities. The British Defence Secretary announced the creation of a »**Cyber Reserve**« in September 2013. At international level, the United Kingdom seeks to hold bilateral talks, especially with important trading partners.

3.5.5 Germany

In 2011 the Federal Ministry of the Interior issued the »**Cyber Security Strategy for Germany**«. Basically two ministries are responsible for implementing the national cyber strategy. The Ministry of the Interior – in particular the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik / BSI) – is in charge of publishing guidelines and directives regarding protective measures for the private sector. Crucial information on cyber security is shared by the responsible bodies within the National Cyber Defence Centre (Nationales Cyber Abwehr Zentrum / NCAZ). The BSI plays a leading role in this exchange. In February 2013 the competent minister presented for example a bill to enhance the protection of critical infrastructures (abbreviated as »**IT Security Act**«). The key objectives include: reporting IT security incidents to the government, improving the protection of IT used in critical infrastructures and strengthening the tasks and responsibilities of the BSI.

The second most relevant ministry is the Federal Ministry of Defence, where above all the Strategic Reconnaissance Command (Kommando Strategische Aufklärung) is responsible for cyber capabilities. Apart from these two ministries, the Federal Intelligence Service (Bundesnachrichtendienst / BND) also plays a decisive role for cyber security. It is primarily responsible for preparing a comprehensive cyber situation report. A **Commissioner for the Cyber Policy of the Federal Republic of Germany** was appointed in July 2013. His task is to represent Germany's cyber interests at diplomatic level.

3.5.6 Netherlands

In 2013 the Netherlands published a revised version of its Cyber Security Strategy. After a series of DDoS attacks in the Netherlands, numerous awareness-raising campaigns were launched based on a cooperation project between banks and the **National Cyber Security Centre** (NCSC). The NCSC does not only provide cyber security assistance (which is available 24/7) but also operates an extensive sensor network, which has to contribute to analysing and clarifying cyber security issues and incidents.

3.5.7 Finland

In January 2013 Finland published its Cyber Security Strategy, which led to the foundation of a **National Cyber Security Centre** (NCSC). FICORA (Finnish Communications Regulatory Authority), which had previously been responsible for national cyber security, was integrated into the NCSC, and so were the government's operational responsibilities for network and information security. The budget was increased substantially.

Besides engaging in GovCERT and national CERT activities, FICORA provides services such as a system for identifying and warning against cyber security threats as well as for the graphic representation of the potential impact, which has been specifically designed for the public sphere.

3.5.8 Switzerland

The »**National Strategy for the Protection of Switzerland against Cyber Risks**« came into force in Switzerland in May 2013.

The Swiss Reporting and Analysis Centre for Information Assurance (Melde- und Analysestelle Informationssicherung / MELANI) is responsible for coordinating the implementation of Switzerland's Cyber Security Strategy. After a series of severe DDoS attacks, it published various measures to protect the IT infrastructure affected by these attacks.

4 National developments

4.1 Actors and structures

4.1.1 GovCERT and CERT.at

GovCERT is the national CERT of the public administration and critical infrastructures. It performs both coordinating and operational tasks. As Austria's Cyber Security Point of Contact (PoC), GovCERT liaises with international organisations and points of contacts such as the European GovCERT Group or the Central European Cyber Security Platform.

It provides bundled expertise in security technologies to the public administration, covering preventive measures, the collection and evaluation of security-related incidents and, if required, in-situ support services. Other tasks carried out by GovCERT include training programmes, the coordination of theme-specific working groups, regular awareness-building measures, the further development of Austria's CERT system as well as the participation in national and international cyber security exercises.

CERT.at is Austria's CERT, and its tasks can best be described as those of an »Internet fire brigade«. First and foremost, CERT.at becomes active when acute security threats arise – based on internal investigations / observations and threat detection or after notification by the bodies affected. As an information hub for cyber security issues, CERT.at is also an important point of contact to which third parties may report acute security problems. Other responsibilities of CERT.at include preventive measures such as the early detection of threats, preparations for tackling incidents and cyber attacks, PR work and consulting as well as networking with foreign CERTs.

GovCERT and CERT.at cooperate closely to fulfil these tasks.

In 2013 GovCERT and CERT.at became active due to several incidents, e.g. problems affecting the control systems of Austrian energy suppliers (May), a number of DDoS attacks catching the attention of the media (April), a wave of website intrusion and defacement attacks (January to March), attacks against the energy and environmental services provider EVN during public unrest in Bulgaria in February, in-situ support during a cyber incident in a federal office (March) as well as the case of an APT attack against a ministry in summer, which was countered in close cooperation with international GovCERT partners.

4.1.2 Austrian Trust Circle

The Austrian Trust Circle (ATC) founded in 2010 is an initiative of CERT.at and the Federal Chancellery. The primary goal is to build confidence between the responsible persons and organisations in individual sectors of strategic infrastructures so as to facilitate the exchange of security-related experience and ensure that swift and joint action will be taken in the concrete case.

At present the ATC addresses the sectors energy, financial affairs, health, industry, transport and communication. Sector-specific meetings of the ATC are held at quarterly intervals. A cross-sectoral meeting is organised once a year.

4.1.3 CERT Alliance

The CERT Alliance was founded in 2011 to enhance cooperation of Austrian CERTs in the public as well as the private sector. Its aim is to bundle available resources and to use the joint know-how optimally in order to ensure maximum ICT security. The members of the CERT Alliance are as follows: A1-CERT, ACOnet-CERT, BRZ CERT, CERT.at, GovCERT, milCERT, R-IT CERT, Vienna CERT.

4.1.4 milCERT

The military Computer Emergency Readiness Team (milCERT) is operated by the Defence Agency (Abwehramt) and the Command Support Centre (Führungsunterstützungszentrum) of the Federal Ministry of Defence and Sports (BMVLS). At present, it is dealing mainly with internal affairs of the BMVLS. Thanks to its process-oriented structure, it meets all essential requirements to carry out tasks of the BMLVS and the Austrian Armed Forces (ÖBH) at national level.

Among its – predominantly military – key tasks are the following:

- to prepare periodic and incident-related operational cyber situation reports as well as to contribute to situation reports on cyber security,
- to evaluate attack and defence technologies and to draft conceptual recommendations based on them,
- to implement technical and organisational security checks,
- to perform penetration testing[11] and security audits of applications and systems,
- to conduct a static and dynamic code analysis during possible malicious code testing and to develop countermeasures,
- to develop comprehensive security systems for networks, servers and user equipment,
- to respond to and handle IT security incidents,
- to observe and evaluate defence and attack technologies,
- to develop and implement cyber defence measures.

The main objective of milCERT is the proactive and early identification as well as analysis of weaknesses and vulnerabilities of ICT systems. The underlying aim is to minimise risks and to counter weaknesses before security problems and concrete threats occur.

4.1.5 Army Intelligence Office (HNaA)

The Army Intelligence Office (Heeresnachrichtenamt / HNaA) has the task of preparing reports on the strategic situation, by taking into account international actors and trends. The contribution of the HNaA is fed into a situation report which covers all sectors of the Austrian state and is used as a basis for decision-making by the senior political and military leadership. Moreover, the HNaA is responsible for the early detection of potential cyber threats from abroad. In the event of a large-scale cyber attack against national infrastructures, it helps to identify the attackers by applying the methods available to it.

4.1.6 Cyber Crime Competence Center (C4)

The Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior (BM.I) is the national coordination and reporting body for combating cyber crime. C4 is staffed with highly specialised technology and other experts of the Federal Criminal Police Office (Bundeskriminalamt). The development of the Centre in terms of organisational, staffing and technical matters was continued and completed in 2013. Within the framework of implementing the ÖSCS as well as the Cyber Security Strategy of the BM.I, the C4 will be upgraded and strengthened.

[11] Testing for potential security risks

4.1.7 ICT Security Portal

The ICT Security Portal is a measure defined in the Austrian Cyber Security Strategy. It was launched as an interministerial initiative in cooperation with the Austrian economy. The aim of the Web platform, which went online in 2013, is to raise awareness and serves as a valuable source for information and communication for different target groups (www.onlinesicherheit.gv.at).

4.2 Implementation of the ÖSCS

The implementation of the measures enshrined in the ÖSCS (adopted by the federal government in March 2013) to increase national cyber security are monitored by the **Cyber Security Steering Group** (consisting of members liaising with the National Security Council as well as the cyber security experts of all ministries). At the operational level, a core group is in charge of planning and giving the respective instructions. The ÖSCS is realised in accordance with an **implementation plan**, which was adopted by the Cyber Security Steering Group in June 2013.

In the process of adopting this plan, an agreement was reached on four prioritised implementation projects. Several interministerial project groups worked on them during the year 2013. These projects are as follows:

1. Development of **permanent coordination procedures and structures at the operational level** (by April 2014, under lead of the BM.I and BMLVS).
2. **Report on the regulatory framework** (by December 2014, under the lead of the Federal Chancellery and the BM.I).
3. Development of a concept and rules of procedure for a **Cyber Security Platform;** cooperation with the operators of critical infrastructures and other economic sectors (by March 2014, under the lead of the Federal Chancellery and the BM.I).
4. **Cyber Security Communication Strategy** (by December 2014, under the lead of the Federal Chancellery and the BM.I)

5 Cyber exercises

5.1 NATO exercise »Cyber Coalition 2013«

In 2008 NATO launched a series of annual cyber defence exercises to test decision-making processes, technical and operational procedures as well as cooperation between the participants. Under the aegis of MilCERT and with the support of GovCERT, Austria has participated in the Cyber Coalition since 2013. The national experts delivered an excellent performance on a par with their international counterparts. Austria's participation in this exercise through MilCERT and GovCERT can also be deemed successful as the national goal of establishing an emergency communication structure between MilCERT and GovCERT was achieved.

5.2 Combined Endeavor (CE)

The Combined Endeavor has been held annually since 1995 under the leadership of USEUCOM (United States European Command). It is the globally largest interoperability exercise for command support professionals. Up to 43 different nations (including Austria) and organisations from Europe and North America took advantage of this event to activate, test and, based on the test results, further develop their C4 (command, control, communications and computer) systems in various multinational operational networks.

5.3 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise« (CWIX)

The exercise held in Poland in June 2013 provided an opportunity to perform technical and operational tests with deployment-oriented systems, services and applications. This event is one of several measures taken to ensure the capability »interoperability« in current and future international operations. The aim of Austria's participation (four representatives of MilCERT) was to explore and test the effects of cyber threats on the systems used in operations. Important conclusions were drawn, which facilitate the assessment of protection mechanisms against internal and external attacks and the safe operation of command information systems.

6 Summary / outlook

The most important development observed in 2013 was the significant increase in cyber espionage and cyber-criminal activities. Attacks are becoming more tailored, and they are also expected to focus more strongly on »cloud«[12] services in the near future. As the »success rates« of the perpetrators are by no means negligible, all the respective actors will invest even more in the research and development of targeted capabilities in the future – regardless of their motivation (e.g. to obtain financial resources, to procure information or to impair the operational readiness of the enemy). Relevant methods and resources are being further developed, research on weaknesses is being intensified. It can be assumed that cyber attacks will increase in quantitative terms, while the capabilities used for attacks will be upgraded in qualitative terms. But as these attacks are individualised and some of the malware is highly developed, it is extremely difficult to detect attacks of this kind.

As cyber attacks will be geared to specific types of data processing and storage, they will concentrate mainly on cloud services and social networks in the next years. The steady increase in mobile Internet usage via smartphones and tablets will reinforce this trend.

In view of these developments, adequate protection and cooperation on information and communication technology as well as the data processed with ICT systems is of growing importance. Comprehensive approaches involving state and non-state actors are becoming indispensable. Coordinated, large-scale technical as well as organisational measures play a vital role in detecting processing anomalies and developing appropriate countermeasures.

Currently, there is an international trend towards centralising national cyber security control and coordination through newly established cyber security centres. In general, governments are expected to show a growing interest in cyber security issues, which will be reflected in the publication of new national strategy documents as well as the establishment of relevant control and coordination structures. Cyber security is likely to take centre stage in multi-national and institutional discussions.

Existing activities and structures in Austria provide a sound basis for responding to the challenges mentioned in this Report. Technical, organisational and social capacity building must, however, go on.

[12] Umbrella term for applications and data storage media which are not provided through local but remote networks. Just like a local resource, they are accessed through local networks.