DIGITAL AUSTRIA

ICT Security

National ICT Security Strategy Austria

Publishing information

Media owner, publisher and editor:
Federal Chancellery, Digital Austria,
Ballhausplatz 2, 1014 Vienna
www.digitales.oesterreich.gv.at

Authors: Economic, scientific and public administration experts
Overall concept: ICT Strategy of the Federal Republic of Austria
Editing and layout: Federal Press Service, Division VII/5
Translation: Heidemarie Markhardt
Cover design and graphical support (printed version): Federal Chancellery | ARGE Grafik
Photo credits: photos.com (Cover)
Printers: BM.I Digitalprintcenter
Vienna, 2012

Copyright and disclaimer:
Excerpts from this publication may not be reprinted unless the source is quoted, all other rights are reserved. It should be noted that though the authors have made every effort in preparing this publication all information is provided without warranty. Neither the Federal Chancellery nor the authors assume any liability. Any legal arguments contained herein are solely the non-binding opinions of the respective authors and will by no means prejudge the decisions of any independent courts.

Feedback:
If you have any comments on this publication,
please email them to ikt@bka.gv.at.

National ICT Security Strategy Austria

Vienna, 2012

Table of contents

Introduction

ICT security is a common objective—and as the challenges faced by ICT security are of increasing frequency and scope, a coordinated approach has become indispensable. However, due to the dynamic nature of these challenges, conventional strategies have been subjected to extreme stress. A more long-term and international perspective is required in order to stabilise this situation.

Austria's ICT Security Strategy therefore has to define its position within a European context as an important reference for further action. It must also give Austria a stronger voice in the concert of EU Member States in the field of ICT security. Hence, Austria's firm commitment to the sustainable development of this sector in Europe is absolutely essential.

Due to general priorities, the "security poverty line" in the SME sector and private sphere is low. As Austria is a country with a particularly high proportion of small and medium-sized enterprises (SMEs), it is necessary to focus on the requirements of these sectors.

Critical information infrastructures and their protection are core objectives of ICT security strategies. On this basis, it is necessary to implement consolidation measures and plotlines ensuring the calculability of risks.

Reactive strategies such as cyber security or cyber defence measures are vital and integral elements. However, they cannot be applied effectively unless complemented by proactive strategy elements on a large scale. The latter are usually characterised by a significantly higher cost/effectiveness factor.

This fact poses special challenges to formal and non-formal types of education, preparatory phases of labour market reintegration as well as to the media, especially radio and TV. This mandate must go beyond the scope of current incident reports since not even the most fundamental efforts have been made to realise the potential in this area. Interest representations such as chambers are equally challenged to bundle and intensify their existing activities across sectors.

To ensure the calculability of risks in all areas, there must be considerably more cooperation between the economy and security research. Highly visible best practices ("lighthouses") of competent implementation (e.g. integral security in Austria's e-government system) have to be established in other areas at transnational level in order to ensure the long-term viability of the Austrian economy. The aim of coordinating cooperation with education and research is to respond to dynamic developments, to identify new trends in due course through technology monitoring and to improve resilience.

To increase general ICT risk awareness beyond the level of specific incidents, the public administration will not only have to take ICT security seriously within its own purview but also to implement it in a competent manner. Based on the useful approach embodied in the ICT Consolidation Act, there is a need for action in other areas as well.

CIIP Action Plans define a common roadmap and establish a comprehensive and logical sequence of steps to be taken on the basis of ICT exercises. In line with these plans, protection profiles will have to be created for technologies used in critical infrastructures within the framework of international cooperation (e.g. by involving ENISA/CEN/ETSI ...). It will also be necessary to arrive at a common understanding of examination/certification and monitoring processes.

A start has been made by developing a process-oriented approach. On this basis, it will be possible to formulate an overall strategy, to identify the stakeholders and create an institutional framework for the continuing commitment and cooperation of these players with a view to achieving the goals.

Reinhard Posch,
Chief Information Officer of the Federal Republic of Austria

Summary

The development of modern information and communication technologies (ICT)—and above all the Internet—has led to an unprecedented transformation of social and economic life. In Austria about three quarters of the population currently use the Internet regularly, and one in every two persons does so daily. The economy heavily depends on ICT in order to take advantage of e-commerce and ensure the efficiency of internal procedures. For the public administration ICT is indispensable when it comes to making its services available to a broad public through non-traditional channels.

Today the general welfare of the state depends to a considerable extent on the availability and proper functioning of cyberspace. While growth rates in Internet usage, e-commerce and e-government are significant and cyber crime (in particular hacking and phishing offences) is on the rise, the Internet and computer skills of the users have remained virtually unchanged. This has led to dramatic disparities between actual ICT usage, increasing IT crime, necessary IT knowledge and risk awareness.

Attacks from cyberspace pose a direct threat to our safety and security and to the functioning of the state, the economy and our society, and may therefore severely affect our daily lives. One of Austria's top priorities is to tackle cyberspace security using every means available at national and international level. A first step is to define a strategy to ensure cyberspace security.

The ICT Security Strategy is a proactive concept designed to protect cyberspace and human beings in this virtual space by taking into account their fundamental rights and freedoms. This strategy will not only improve the security and resilience of Austrian infrastructures and services in cyberspace but also create awareness and trust among Austrian citizens.

The strategy addresses a wide range of issues—from different aspects of creating ICT security knowledge and ICT security awareness to proactive and reactive cyber incident management. The spectrum covers education, research, sensitisation, case law, technical and organisational issues of Austrian enterprises as well as the protection of strategically important Austrian institutions.

ICT security is regarded as a common key challenge. As far as an implementation strategy is concerned, a bottom-up approach has been chosen—with a broad base involving all relevant stakeholders. Hence, the strategic objectives and measures for implementation of the Austrian concept may be divided into five key areas:

- Stakeholders and structures
- Critical infrastructures
- Risk management and status quo
- Education and research
- Awareness

In order to achieve the Austrian goals, the Action Plan described below will increase the effectiveness of both sector-specific and trans-sectoral measures, which will be implemented by taking into account timelines and responsibilities.

Overview

Stakeholders and structures
- Optimising the cyber landscape in Austria
- Establishing networks between stakeholders and structures
- Enhancing the legal framework for cyber security in Austria
- Promoting international cooperation

- Public cyber partnership
  - Cyber Security Steering Group
  - Cyber Crisis Management
  - Cyber Security Platform
- Cyber Situation Centre

Critical infrastructures
- Improving cyber crisis management
- Enhancing risk management and information security
- Information exchange between public and private stakeholders

Risk management and status quo
- Identifying core enterprises in the respective sectors
- Comprehensive risk and security management across sectors
- Ensuring minimum standards and managing risk acceptance in core enterprises
- Establishing crisis and emergency management in ICT and non-ICT sectors
- Assessment and management of the situation

Education and research
- Education/training relating to ICT, ICT security and media skills in early grades at school
- Compulsory ICT training for all students of teacher training programmes
- Increased training of ICT security specialists in the tertiary sector
- ICT security as an important element of adult education and training
- ICT security research as a basis for national competence
- Increased coverage of ICT security topics in applied ICT research
- Active theme leadership in international research programmes

Awareness
- Strengthening Austria's ICT security culture
- Positive positioning of ICT security
- Harmonised and coordinated approach
- Effectiveness and sustainability of awareness measures

Legal framework

International cooperation

Cyber competence

Standardisation and certification

Uniform terminology and common language

Information and communications platform for all fields of action and target groups (Cyber Security Platform)

Stakeholders and structures

Initial situation

A country's specific approach to cyber security is linked very closely to its existing stakeholders and structures. The term "cyber security" refers to organisations, institutions or persons with a vested interest in cyber security, or particularly severely affected by it.

An insight into the present quality of cyber security in Austria was obtained by examining a total of 200 stakeholders and structures and analysing the 80 currently most important ones.

By sectors. Actions related to cyber security in Austria focus on the public sector, notably institutions at federal level and publicly financed institutions. The public administration set up specialised institutions with different responsibilities and target groups in several ministries. These institutions have been optimised for their respective sphere of activity and make a substantial contribution to cyber security in Austria.

The Länder (federal provinces), cities and municipalities operate on a smaller scale, and have only very few overarching structures. The private sector usually has good cyber structures at corporate level. The larger the enterprise, the greater the possibilities to take preventive and protective measures. Private-sector cyber security interest representations are only now emerging on a broader basis. There are only very few interest representations exclusively geared towards the needs of the citizens, who must resort to the institutions of the public administration.

By areas of activity. Stakeholders and structures acting on a trans-sectoral basis are distributed quite evenly over the following areas of activity: sensitisation, research, prevention, emergency and crisis management. The highly specialised areas of public information services and criminal prosecution fall exclusively within the purview of the ministries responsible.

However, education sector takes only very little action in the field of cyber security; there are hardly any stakeholders offering cyber security programmes. However, this would be of vital importance for the qualitative (further) development of human resources familiar with cyber security issues—both in enterprises and public authorities. The education sector has huge a potential for the future.

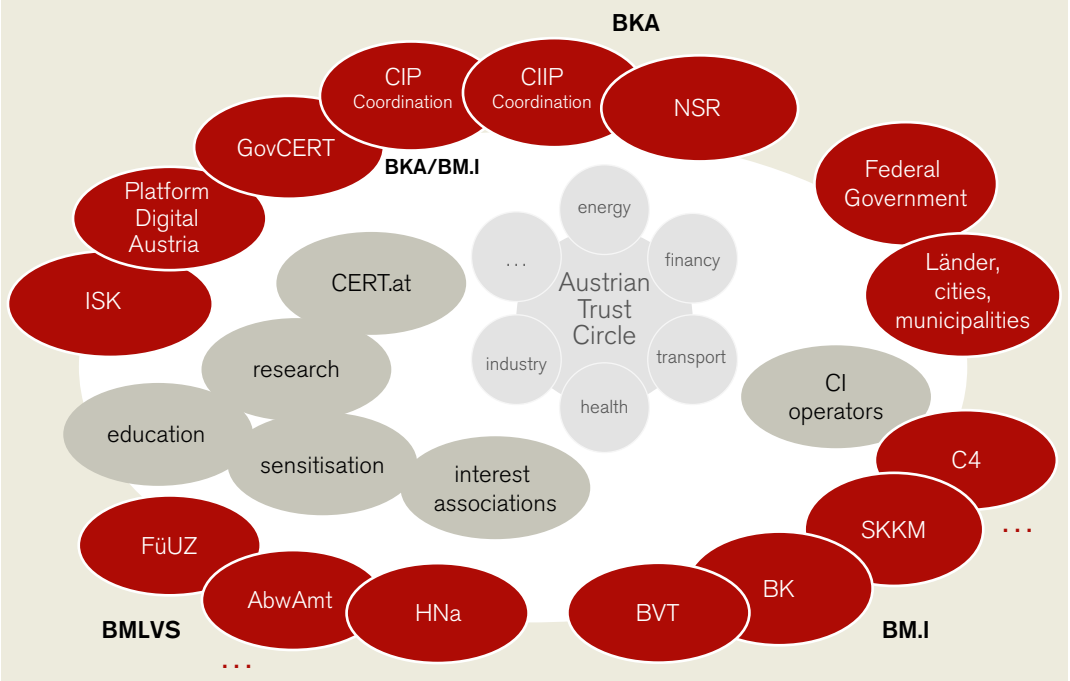
By level of customer orientation. The government and business sectors receive an almost equal level of support as the clients of Austrian stakeholders. It must be emphasised that there are only very few citizens' interest representations (lacking visibility). Another striking fact is that cyber stakeholders show little customer orientation towards the citizens.

Cyberspace is an area in which many Austrian structures and stakeholders are active separately and highly independently. Several trans-sectoral organisations exclusively specialised in cyber security are already playing an important role in Austria, e.g. the well-established CERTs (Computer Emergency Response Teams).

However, processes suitable for the control of cyber incidents are implemented predominantly at local level. Overarching cyber security procedures have not been harmonised or defined in detail. While other areas benefit from institutionalised and process-controlled mechanisms to tackle incidents, cyber incident management in Austria relies predominantly on a personal network of contacts.

It is remarkable that two essential elements are either lacking completely or are insufficiently developed in the Austrian structures:

- a central Situation Centre for Austria; the responsibilities of such a centre are currently exercised by CERTs;
- the sector of public administration affected by cyber security; this includes public stakeholders, their specialised institutions and above all processes of cooperation in the framework of a



Cyber incident stakeholders in Austria

CIP – Critical Infrastructure Protection

CIIP – Critical Information-Infrastructure Protection

ISK – Information Security Commission

FüUZ – Command Support Centre

AbwAmt – Military Counter-Intelligence Service

HNa – Military Intelligence Service

BVT – Federal Agency for the Protection of the Constitution and the Combat of Terrorism

BK – Federal Criminal Office

BKA – Federal Chancellery

CERT – Computer Emergency Response Team

C4 – Cyber Crime Competence Center

NSR – National Security Council

GovCERT – Government Computer Emergency Response Team

BMLVS – Federal Ministry of National Defence and Sport

BM.I – Federal Ministry of the Interior

comprehensive cyber security concept. An overarching structure for cyber security management is largely lacking.

While Austria's cyber security landscape has reached an appropriate degree of maturity in some areas, there is an urgent need to catch up in others.

Strategic objectives and measures

Objective 1: Optimising the landscape of "cyber security stakeholders and structures" in Austria

Hypothesis: At first glance, Austria's current cyber security landscape appears to be tightly knit and comprehensive. Looking at individual sectors more closely, one can identify smoothly functioning structures and others that function less well. While it might be useful to know about the former, the latter pose a risk to our country. A quality-based and comprehensive approach to cyber security management in Austria may be ensured only by means of a dense network of cyber security stakeholders and structures.

Strategic objective:
A dense network of cyber security stakeholders and structures in Austria must cover all areas, fields of activity and target groups relating to cyber security and must take into account the short innovation cycles of ICT. In order to implement this objective, it will be necessary to consolidate the strengths of Austria's present cyber security landscape by ensuring a high level of quality, to eliminate its weaknesses on a long-term basis and to optimise existing structures so as to enhance flexibility.

Measures

Establishing a public cyber partnership:
It is impossible for a single body to cover all aspects of cyber security today. A structure is therefore necessary that will bundle Austria's cyber security activities, promote cooperation, avoid duplication of effort, take advantage of synergies and facilitate initiatives. Since this is a topic of vital national interest, the state and its institutions have to assume responsibility

for overarching coordination. The cyber partnership comprises:

- *Public Cyber Crisis Management*
- *a Cyber Security Steering Group*
- *an information exchange centre for cyber security*

Establishing a Cyber Situation Centre: In order to obtain an overview of the cyber situation, the available information will need to be collected, bundled and evaluated on an ongoing basis. In Austria these tasks are to a large extent carried out by different institutions, in particular CERTs. No centrally managed Cyber Situation Centre has been established to date in Austria.

For further information on standardisation see chapters 'Critical infrastructure' and 'Education and research'.

Creating structures for standards, certification and quality assessment: The constant availability of reliable ICT systems and components may be ensured by using components (especially in sectors deemed critical for security) subject to certification ("supply chain security"). Austria plans to establish a certification body for cyber security products and cyber security assessors. A centralised body will therefore be established which will be responsible for coordinating the publication of quality standards for cyber security in Austria and of minimum requirements for conducting reviews of cyber security quality standards.

The significant structural measures in Austria are described in greater detail below.

Public cyber partnership

The cyber partnership must extend to crisis-coordinating, strategic-political and advisory-operational level. A central contact for public cyber security matters will be created by establishing the position of a Chief Cyber Security Officer in Austria, who will act in close cooperation with the Chief Information Officer of the Federal Republic.

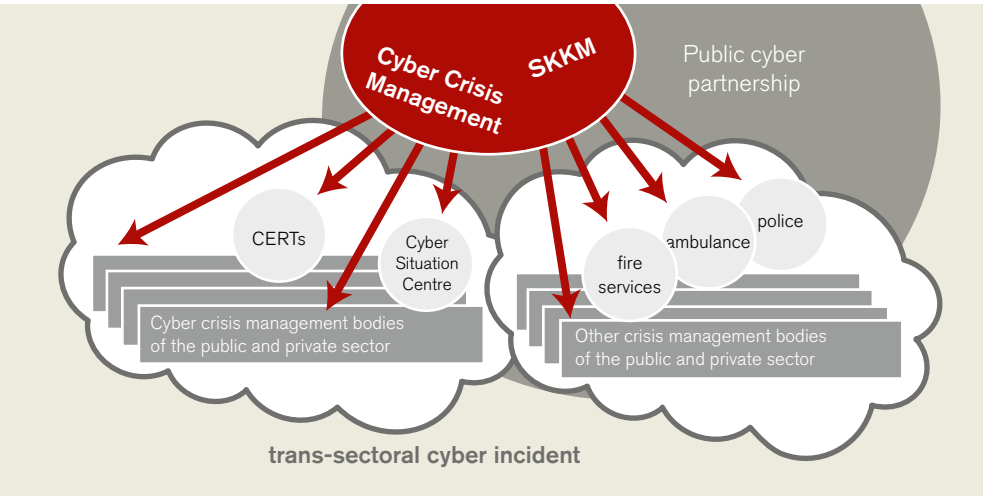
Public Cyber Crisis Management (crisis-coordinating level)

A Cyber Security Crisis Management appropriate for all cyber incidents will be defined for Austria by taking into account existing cyber structures (e.g. CERTs).

Cyber Crisis Management will consist of representatives of the state and the critical infrastructures. Rules and procedures will have to be agreed upon to facilitate cooperation between public and private crisis centres.

In the event of a cyber incident with potentially harmful local effects, institutions of the relevant ministries or private entities will be responsible for crisis management in cooperation with CERTs. These facilities have to be closely geared to the specific requirements of cyber security threats. To be suitably prepared for such emergencies, crisis management bodies and CERTs conduct joint exercises on a regular basis.

Crisis management in the event of cyber incidents affecting various sectors and posing a severe threat to the security of supply in Austria is based on existing crisis and civil protection structures (Krisen- und Katastrophenschutzstrukturen/SKKM). Through complementary cooperation with crisis and civil protection structures correlation of cyber security expertise (serving as Austria's national cyber crisis management) has to be ensured to tackle any cyber issue. In Austria cyber security



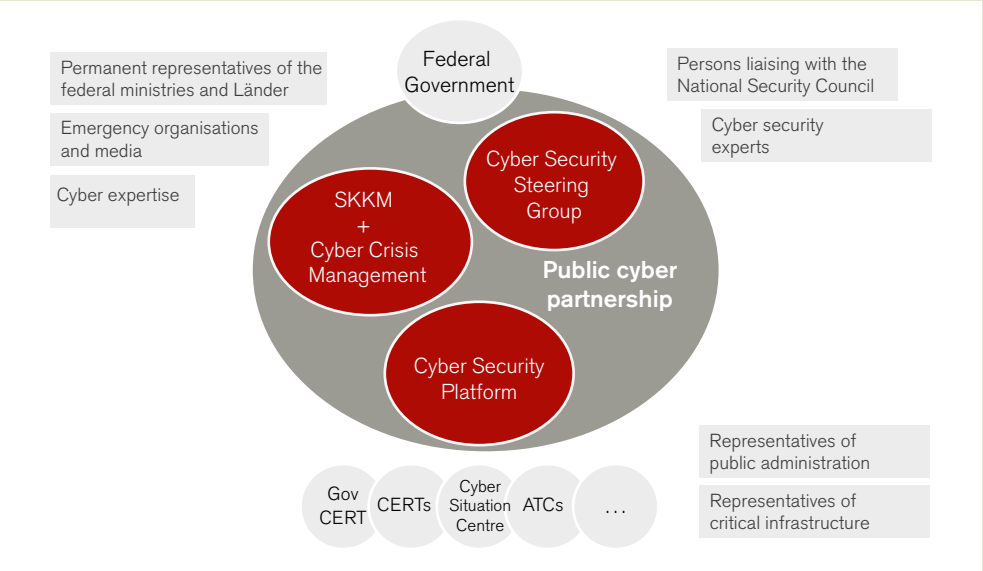
experts act as the National Cyber Crisis Management.

Cyber Crisis Management requires a clearly defined line of responsibility for cyber crisis events. Crisis management plans define how crisis management bodies must deal with the most important cyber threats. They must be jointly prepared for all known cyber incidents. In addition, they must be adapted to the latest threat scenarios on an ongoing basis. Special cyber exercises must be organised in order to test cyber crisis management. Crisis management plans are adopted by the Cyber Security Steering Group.

Cyber Security Steering Group (strategic-political level)

The strategic-political level is the state's highest level for evaluating and deliberating on cyber security issues. The Steering Group is set up at this Cyber Partnership level as the federal government's central advisory body for all matters involving Austria's cyber security.

This advisory body focuses on integrated approaches, strategies, crisis management, inter-governmental cooperation and Austria's active participation in matters involving cyber security. It adopts Austria's comprehensive



Public cyber partnership / based on existing structures

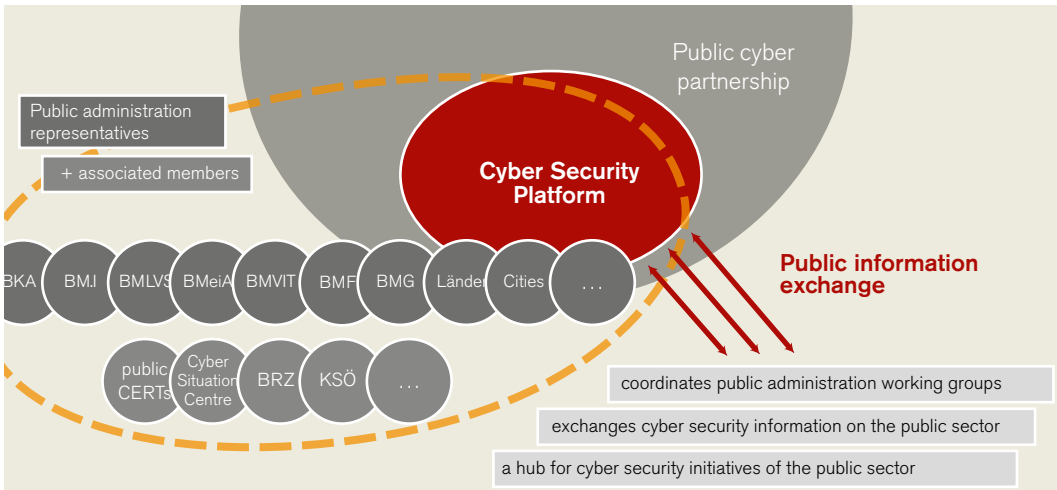
SKMM – Public Crisis and Civil Protection Management

ATC – Austrian Trust Circle

CERT – Computer Emergency Response Team

GovCERT – Government Computer Emergency Response Team Austria

Cyber Security Platform
Information exchange between public sectors



Cyber Security Strategy, monitors its implementation and takes corrective action if necessary.

Organisational underpinning will be provided by the Board of Liaison Officers (responsible for communication with the National Security Council). The top cyber security experts of public administration and the Chief Cyber Security Officer will be members of this Steering Group. Permanent active involvement of the private sector in Austria's top-level cyber decision-making group is highly recommended.

Information exchange on cyber security (advisory-operational level)

The ongoing exchange of information between Austria's public cyber structures and public administration on the one hand, and representatives of the critical infrastructures, business, the cyber experts and private crisis centres on the other, will be institutionalised by launching the Cyber Security Platform (public-private partnership on cyber security).

All important public stakeholders will participate on an equal footing. An integrated approach—taking into account all aspects of the Austrian society relating to cyber security—should be pursued. The fundamental values of the Austrian society in dealing with cyber activities will serve as a basis for all activities on the Cyber Security Platform. The relative fundamental values will be defined in a preamble that must be formally adopted at political level.

Within the framework of the Cyber Security Platform, regular meetings ensure an exchange of information among all public sectors as well as between public and private sectors. Representatives of education, research and development have to be involved in this exchange to an increasing extent. Working groups and initiatives will tackle current challenges of cyber security in Austria.

A web platform serves as a central point of contact for all issues relating to ICT security and the key information and communication base concerning all awareness-raising measures for all target groups in Austria.

A Cyber Competence Centre is to be set up to complement the activities of the Cyber Security Platform.

Opportunities for the confidential exchange of information outside the publicly accessible Cyber Security Platform open up new vistas of cooperation in the areas of cyber security, cyber crime, cyber defence and cyber diplomacy.

For further information on the web platform see chapter 'Awareness'.

Cyber Situation Centre

The planned Cyber Situation Centre will be responsible for tackling major cyber incidents in the public administration as well as for special crisis and disaster situations at national level. The services of the Austrian Federal Army (Österreichisches Bundesheer/ÖBH) will round off the activities of the Cyber Situation Centre.

In "normal operations", the Cyber Situation Centre prepares public and non-public analyses on network security in Austria and is responsible for simulations and reporting. Early warning is one major task of the Cyber Situation Centre. The capacity for forensic activities will be created to support enterprises on request. It is therefore necessary to monitor the situation 24 hours a day, 7 days a week (24/7) to ensure that clients, notably critical infrastructures (also usually operating 24/7) obtain the required information on time.

The networks of public administration and critical infrastructures are equipped with sensors in order to gather security-relevant information in real time. Networks without such sensor systems will be obliged to report cyber anomalies (to be defined).

The legal framework will need to be analysed and adapted as a first step. Legal provisions have to be adopted defining the responsibilities and powers of Cyber Situation Centres, their reporting duties and requirements concerning data disclosure.

Stakeholders playing similar roles are to be involved in the organisation of Cyber Situation Centres. Strategic and organisational decisions must be taken jointly by a Situation Council together with the most important public cyber security stakeholders. The involvement of private stakeholders is highly recommended.

The main recipients of services provided by Cyber Situation Centres are various bodies of the public administration and critical infrastructure enterprises.

Objective 2: Networking of stakeholders and structures

Hypothesis: Cyber security is important where ICT systems are connected to the Internet—and this means practically everywhere since connected digital devices are used directly or indirectly in our information society. Unfortunately such digital omnipresence also provides a fertile breeding ground for all kinds of criminal wheeling and dealing. The establishment of networks among all stakeholders and cyber structures is essential in order to react fast after the occurrence of harmful incidents, or to disseminate the lessons learned after overcoming harmful incidents. Only by establishing a tightly knit network of contacts between stakeholders will Austria be able to benefit from robust cyber security structures.

Strategic objective:

Incentives, support measures and a legal basis must be created to promote densely knit networks between Austrian cyber security stakeholders and structures. The aim is to establish an automated cyber networking procedure so as to promote a comprehensive and self-learning cyber security culture in Austria based on information-exchanging control loops.

Measures

Promoting existing and new networks between stakeholders and structures in Austria: Fostering networking between stakeholders—within cyber activity areas by means of focused expert meetings; beyond the boundaries of activity areas (sensitisation, education, research and development, security prevention, emergency and crisis management, public information and criminal prosecution) and across sectors (public administration, economy, universities, interest representations, citizens). Exchanges between cyber security stakeholders with representatives of sectors with only indirect or no cyber security responsibility must be

intensified. Existing events, congresses and initiatives devoted to cyber security will continue to be supported and promoted.

Examining existing control loops to strengthen cyber security competence: Cyber security strategies must be adapted to both constant and unpredictable changes of technologies, applications and markets. They need to update their cyber security competence on an ongoing basis. The exchange of information at national and international level as well as the establishment of control loops supplying one another with new knowledge and findings will prove useful in this context. Studies will have to be carried out in order to comply with the latter mandate. Moreover, the necessary processes (feedback and learning loops) will also have to be initiated.

Objective 3: Enhancing the legal framework for cyber security

*Hypothesis: I*t is vital to regulate cyberspace so as to give people a feeling of security and confidence when using integrated digital technologies. All types of digital information and communication technology (ICT) existing in Austria must be taken into account. In Austria the legislator reacted at an early stage to the specificities of ICT by laying down rules in different laws. Legislators have been faced with new national and global challenges due to the ICT penetration throughout the world. To keep abreast with fast-moving technological and social processes on the Internet, adjusted processes have to be created to establish *legal certainty reflecting the "state of the art"*.

Strategic objectives:
Austria's legal framework for cyber security must be adapted to or developed in line with the objectives and requirements of the existing Cyber Security Strategy. The aim is to ensure that legislation keeps abreast of the changes in cyberspace to create legal certainty in Austrian cyberspace. Austria's position is contributed actively to international working groups of lawmakers.

Measures

Analysing the status quo of current legal provisions relating to cyber security and filling gap in Austrian legislation: All areas of Austrian cyberspace that need to be regulated by issuing ordinances in Austria will be analysed. Which areas are already covered by which laws? Which ordinances governing the same matters complement one another or exist in parallel? Which areas are currently regulated inadequately or not at all? Contradictory provisions in different laws will be eliminated, while new laws will be drafted for relevant issues not previously covered. The enormous responsibility of operators of critical infrastructures must be taken into account in this context.

Establishing a flexible structure for legislators of cyber security: All the options for establishing a new and flexible structure for the legislators of cyber security matters must be analysed. The aim will be to set up and promote a legal structure for cyber security that keeps pace with developments in cyberspace.

Participating in the development of an international legal framework for cyber security: Austria must actively participate in the discussion and development of international regulations/recommendations on cyber security by forming alliances with other nations so as to contribute fundamental Austrian values to international legal instruments.

Objective 4: Promoting international cooperation

Hypothesis: The Internet is a global phenomenon—like the threats posed by the Internet. The international dimension of the cyber threat is growing at an alarming rate. A stringent and consistent strategy with an

international focus will be required in order to make a national digital society robust. Global networking is a central element of such a cyber security strategy. Today international organisations make intensive efforts to ensure that the fundamental values of our society (such as the right to privacy or the protection of personal data) are also effectively upheld online. It is only through comprehensive and active participation in international processes that Austria will be able to develop the cyber security expertise required to create the necessary trust and safety in using digitally networked structures.

Strategic objective:
Participation of the public sector in international organisations regarding the subject "cyber security" will be institutionalised and become mandatory. In addition, the participation of private-sector interest representations in international associations will need to be encouraged by means of publics-sector incentive systems. International findings and recommendations will be taken into account in national processes.

Measures

Active participation of the public administration in international cyber security developments (OSCE, OSCD, EU, NATO, …)

Promoting the participation of the private sector in international cyber security events and developments

Establishing bilateral and multilateral networks to counter Internet threats: Cyber security partnerships and networks (e.g. CERT networks), intensive networking in the German-speaking area (Germany, Austria and Switzerland, referred to as "DACH") and bilateral cyber security relations with all neighbouring countries; participating more actively in international organisations to establish cyber security networks.

Joint development of international strategies to protect fundamental transnational rights in the use of digital information and communication: Austria's fundamental values relating to the use of digital information and communication as well as of digital networks (e.g. free, unlimited Internet access and freedom of expression on the Internet) are advocated and implemented in international forums.

Active participation in transnational cyber exercises: Austria will be actively involved in planning the most important international cyber exercises and will also take part in them. The experience gained in such international exercises will be applied directly to national exercises.

Critical infrastructure

Initial situation

The term "critical infrastructure" or "strategic infrastructure" describes those parts of all public or private infrastructures that are of crucial importance for maintaining vital societal functions. Their disruption or destruction has a major impact on the health, security or economic and social wellbeing of the citizens or the effective functioning of state institutions.

Today most critical infrastructures increasingly depend on specialised IT systems which are expected to guarantee services as smoothly, reliably and continuously as possible. The ICT sector itself (and its IT and telecommunications networks with their various components and providers) as well as the ICT-based infrastructures of all other sectors not only permit sectoral production, but also keep the trans-sectoral flow of information going. In more general terms, these are also referred to as *critical information infrastructures (CII)*. The protection of critical information infrastructure (CIIP) is therefore not just a task for the ICT sector alone, but has increasingly become a concern of other economic sectors.

One particular characteristic of critical information structures is their susceptibility to different types of cyber attacks. This is reflected in the fact that CIIs themselves can be actively abused as "attack channels" against other critical infrastructures. Unlike failures of electricity or water supply, cyber attacks may cause lasting—"sustainable"—damage, e.g. through the targeted destruction or manipulation of machine control data.

In Austria cyber security goals pursued to protect critical information infrastructures must be coordinated with the proven *Austrian Programme for Critical Infrastructure Protection (APCIP)*. An overarching objective therefore correlates with this programme as follows:

"The APCIP programme must be complemented by cyber security measures within and between the sectors; national capacities to support information security and cope with national crisis and disaster situations have to be built up."

Strategic objectives and measures

Objective 1: Cyber crisis management

Hypothesis: Cyber crises and disaster situations may have fatal effects on the state, the economy and public life. At international level it has become an established practice to build up special overarching structures for events of this kind to complement existing crisis management structures.

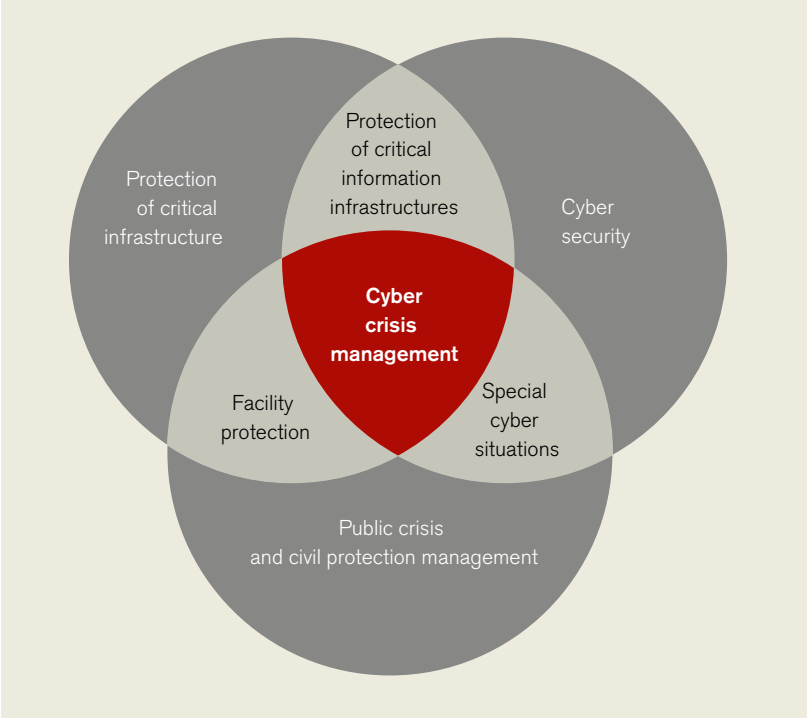
Strategic objectives:
To further develop reactive tools for a country-wide disaster and crisis management relevant to cyber security (cyber crisis management) to protect the state, economy and public life from harm. National cyber crisis management is an important element of national security.

Measures

Establishing a structure for national cyber crisis management: The factors distinguishing national cyber security management ("cyber crisis management") from conventional public disaster and crisis management are, on the one hand, the special requirements and overlapping areas of cyber security, and on the other constant cooperation with programmes protecting critical infrastructures. Another difference between cyber crisis management and conventional public disaster and crisis management is the degree of networking required at national and international level. Cyber crises at a domestic level may be coped with only with the aid of governmental (public) and non-governmental (private) stakeholders and depend on international cooperation in almost all cases.

Establishing a Cyber Situation Centre: see chapter 'takeholders and structures'.

Establishing a viable crisis communication system: Communication with the organisations and companies responsible for operating key networks needs to be strengthened. A functioning and properly secured communication system with public and private stakeholders abroad has to be ensured in acute cases. The establishment of an "emergency network" (e.g. with the aid of DVB-T technology) should be guaranteed at any time. Other options of fail-safe communication (e.g. VHF radio) will also have to be taken into consideration. In a crisis situation, it is also essential to verify the identity of participants. A suitable legal basis is required, especially for passing on information.



Objective 2: Risk management and information security

Hypothesis: One of the most effective methods of promoting cyber security and facilitating day-to-day operations is to encourage self-protection by proactive risk minimisation at the level of the enterprise or organisation (risk management and information security).

Strategic objective:
To ensure that risk management and information security methods are applied are as far-reaching and differentiated as possible within the critical infrastructures identified. Services of special general interest require a higher level of protection.

Measures

Promoting risk management within CI: The establishment of ICT-related risk management (generally also referred to as "information security") is regarded as one of the most important measures which CI operators can take to protect themselves. In the context of national cyber security it is of fundamental importance that all stakeholders responsible take *information security or ICT-related risk management measures* in their respective sphere of responsibility. The government supports them by providing information on joint risk analysis, accreditation of different risk management methods, harmonisation of training measures as well as technology assessment analyses. Sanctions and incentives promote the use of risk management methods in the private sector.

Establishing a Cyber Competence Centre: The Cyber Competence Centre is part of the Cyber Security Platform and is the central point of contact for all operators of critical infrastructure and also for enterprises interested in risk management/information security management (RM/ISM). It provides information on different RM/ISM approaches and accreditation procedures, e.g. based on the Security Manual 2010 or ISO 27000. Together with the Cyber Situation Centre, quantitative information is processed for specific cyber security risk analysis.

For further information on Cyber crisis management see chapter 'Stakeholders and structures'.

Maintaining and updating the Information Security Manual to ensure basic protection: The "Austrian Information Security Manual" (Österreichisches Informationssicherheitshandbuch/SIHA) was revised and reorganised in 2012. The Manual describes and supports procedures for the establishment of comprehensive information security management system in enterprises and the public administration. SIHA 2010 has been tailored to the needs of small and medium-sized enterprises implementing ISM measures. Complying with international requirements, its structure and content facilitate the implementation of the ISO/IEC 27000 series of standards. The internationally recognised manual makes an important contribution to ensuring a minimum level of protection, and is updated on a regular basis.

See also chapter 'Education and research'.

Conducting technology assessments: Radical technology changes are likely to occur every two to three years in the field of cyber security. It is therefore necessary to monitor present and future technology trends, and to assess their possible impact on the social and economic life. Technology assessment must be tackled within the framework of a research programme which may be linked with existing initiatives (e.g. KIRAS).

Voluntary registration system: Like voluntary fire services, ICT specialists may sign up via a registration system (of the Cyber Competence Centre), providing information on their technical skills, identity and certificates and/or quality certification (e.g. security screening pursuant to the Security Police Act [Sicherheitspolizeigesetz/SPG]). Organisations and enterprises have fast and unbureaucratic access to qualified personnel in an emergency with due regard for legal requirements.

Objective 3: Information exchange of public and private stakeholders

Hypothesis: Information exchange is regarded as the most important element of national cyber security. Since the wide diversity of stakeholders coupled with the growing importance of the private sector make a purely public centralised management impracticable, a continuous exchange of information (particularly threat-related) is necessary to strengthen the self-protection of different stakeholders. The major goal in this context is to ensure consistency with the *Austrian Programme for Critical Infrastructure Protection (APCIP)*.

Strategic objectives:

The exchange of information takes place between governmental stakeholders, between non-governmental stakeholders and between governmental and non-governmental stakeholders. One of the crucial goals of all programmes protecting critical infrastructures is to support public-private partnerships (PPPs) as a general organisational framework for cooperation between governmental and non-governmental stakeholders. The need for information exchange must be reconciled with confidentiality and data protection requirements.

Measures

Supporting public-private partnerships (PPPs): To an increasing extent, the protection of critical information infrastructures and cyber security is coordinated by "trusted" public-private partnerships (PPPs). Examples of existing PPPs are CERT.at as a "community-based PPP" and the Austrian Trust Circle, which exchanges information between private bodies.

Legal certainty with respect to reporting duty: Operators of critical infrastructures have a special responsibility which must receive due consideration whenever

regulatory measures are taken. On the one hand, CI face increasing regulatory requirements. For example, it is recommended that if possible all CI operators (particularly those responsible for the protection of critical information infrastructure) be legally obliged to take risk management and information security measures. On the other hand, the private sector itself often addresses questions relating to its duty to report cyber attacks, as in many instances CI operators were prevented from "voluntary reporting" for reasons of data protection.

Human Sensor Project: ICT system administrators receive gradual ICT security training and are taught to detect anomalies in their ICT systems and report them to their ICT security officers. The data thus obtained are forwarded to the Cyber Situation Centre and the Cyber Competence Centre, where they are processed to gain a more profound insight into the situation. :

Risk management and situation assessment

Initial situation

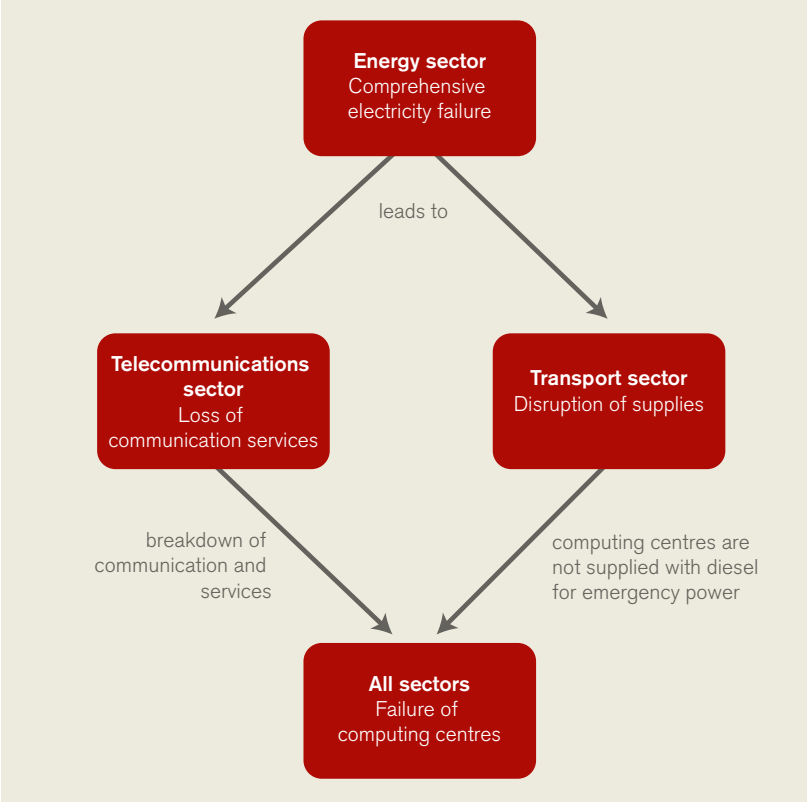
Today's digital society has led to a high penetration of ICT in all areas and ICT now plays a major role in traditional sectors such as energy supply, transport and industry. Exclusively ICT-based sectors take advantage of networks of extensive services and infrastructures controlled through ICT components and processes. Links between individual sectors resulting from the interdependence of services and products leads to a chain reaction in security-relevant scenarios.

Based on these considerations, risk and situation assessments must cover all sectors, although the sectors of information infrastructures, telecommunications, energy, healthcare, transport, monetary transactions and public administration will need to be examined more closely. Each individual sector has a well-developed risk management system. However, the main risks are identified in areas outside the control of individual enterprises. This suggests that the level of interconnectedness among sectors and beyond organisational units is extremely high and that an overarching risk assessment is required.

Due to the strong interdependence of sectors, ICT risks are embedded in the context of upstream or downstream risk situations. It is therefore understandable that a considerable number of risks cannot be managed and tackled by an individual enterprise but only collectively or with the support of the state.

It is of vital importance that non-ICT risks and scenarios are covered by up-to-date emergency and crisis management plans. This is an important requirement for avoiding overlapping risks and scenarios in interlinked systems.

The issue of risk and security management in individual enterprises is another relevant aspect. It will be necessary to resort to best practices in this area, and to create suitable framework conditions. In many cases, it may even become necessary to define minimum standards for these core



Example of a failure chain

infrastructures, which will also require government regulation.

Strategic objectives and measures

Objective 1: Identification of core enterprises in the sectors

Hypothesis: There are risks that can be managed by individual enterprises, and there are risks that need to be addressed collectively or with the support of the government. Assessments of the residual risks to be accepted by an enterprise or of the economic viability of possible counter-measures must take into account the impact on other sectors.

Strategic objective:
Core sectors and relevant enterprises must be identified. There is a small number of core infrastructures or core enterprises the disruption of which will have an impact significantly beyond the scope of the individual enterprise. These need to be considered in analyses and taken into account in risk assessments.

Objective 2: Comprehensive risk and security management across sectors

Hypothesis: ICT risks may not be considered separately due to global interconnectedness.

Strategic objective:
A comprehensive risk and security management system must cover all risks and address all sectors and core enterprises. Minimum standards defining organisational aspects and processes will have to be defined.

Measures

Consolidating the risk catalogue together with selected sector representatives at expert level.

Defining minimum standards for risk and security management taking into account specificities of the sector and standards as well as processes in the area of risk and incident management.

Objective 3: Ensuring minimum standards and managing risk acceptance in core enterprises

Hypothesis: Due to growing competition, the risk to be accepted by core enterprises is increasingly determined by financial factors. This could have an impact considerably exceeding the scope of the enterprise involved, especially in the case of core enterprises with major knock-on effects; this must be taken into account in any risk assessment. Minimum standards of risk prevention must be ensured if a major impact on other sectors is likely.

Strategic objective:
Risk acceptance in core enterprises is determined at a higher level so as to avoid major harmful effects resulting from a lack of risk prevention for financial considerations. In this context, minimum standards will have to be defined and examined. Other options may be explored so as to achieve the desired risk control effect.

Measures

Discussing risk acceptance in critical core enterprises at a higher level of responsibility and clarifying which is the most appropriate way of defining minimum standards (in laws, directives, standards, etc.), which institution is in charge of verifying compliance, and the extent to which best practices of a specific sector may be applied.

Raise this issue at an EU level in order to address matters relating to the distortion of competition.

Objective 4: Establishing a crisis and emergency management system in the respective sectors

Hypothesis: Due to the high degree of interconnectedness, ICT risks must be examined and assessed comprehensively with a view to identifying strategies for coping with them. Emergency and crisis plans are necessary in ICT-related and non-ICT areas.

Strategic objective:
to review public crisis and emergency management processes, to identify risks arising from the increasing ICT dependence of many core processes; to ensure the availability of crisis organisations and processes at public and private level, including contacts in enterprises (e.g. crisis and business contact managers) as well as emergency and contact lists.

Measure

To check whether the government's crisis and emergency plans as well as their procedures for updating and testing them are up-to-date; to establish a connection to the Situation Centre; to review crisis organisations and processes at a public and private level, to interconnect them and, if required, create other appropriate crisis organisations and processes.

Objective 5: Situation assessment and management

*Hypothesis: A*ll sectors and/or organisational units are currently assessed and appraised individually. A personal network is responsible for trans-sectoral risk evaluation. A permanent institution must be established in order to handle interlinked structures.

Strategic objective:
to set up a Situation Centre which will optimise collaboration among sectors. Management responsible for reporting will be informed of incidents and pass this information on to enterprises with critical infrastructures. The Situation Centre must never be a "one-way street", a reciprocal exchange of information is the only way to ensure that information is made available in a timely, comprehensive and targeted manner. The experience gained will be incorporated into long-term awareness measures.

Measure

Creating a Cyber Situation Centre with appropriate means of situation monitoring, including necessary and relevant processes, e.g. reporting obligation or information requirements of the individual stakeholders.

Furthermore information on the Cyber Situation Centre see chapter 'Stakeholders and structures'.

Education and research

Initial situation

Education and research are basic requirements for successful implementation of the National ICT Security Strategy. In this context, attention is drawn to two key issues: *training in ICT security and media competence* and *national ICT security competence in teaching and research*.

Today the use of ICT may be described as the "4th cultural technique" (besides reading, writing and arithmetic). ICT and, closely associated with it, ICT security, and media competence should therefore be covered in early schooling. ICT (security) skills need to be incorporated into courses and curricula of teaching colleges and universities as well as further education and training programmes.

ICT security issues often reflect a lack of know-how of the developers involved. As ICT is an area in which knowledge becomes obsolete very rapidly, continuous further training and qualification programmes are a prerequisite for ICT employee retention and productivity, but are also important for target groups in the private sector, sole proprietorships and small and medium-sized enterprises not involved in the technology sector. The training of ICT security specialists in the tertiary education sector is another area of crucial importance; Austria is able to build on existing high-quality study and training programmes.

A successful ICT Security Strategy is also reflected in research. On the one hand, research serves as a basis for training at the highest international level of qualification ("research-driven teaching"). On the other hand, the availability of know-how in a country is a prerequisite for sustaining developments important for national needs and preparing decision-making processes in matters of national interest. It is therefore important to increase the number of security research institutes, to intensify networking, and to ensure that ICT security issues are incorporated into applied ICT research to a greater extent. Austria's advance to become a knowledge and innovation-based society will be supported by the creation of structures complementing existing comprehensive security research programmes such as KIRAS (an Austrian programme promoting security research) as well as active theme leadership in EU research programmes. This will help establish ICT security as an "export product".

Strategic objectives and measures

Objective 1: Education in ICT, ICT security and media competence in early school grades

Hypothesis: Attacks on ICT infrastructures through inadequately protected private systems as well as the individual's loss of privacy may be prevented on a long-term basis only if the citizens have a wider understanding of ICT security and ample skills in using the new media. This understanding needs to be developed at school as early as possible.

Strategic objective:
ICT and ICT security must be incorporated to a greater extent into school curricula and daily teaching practices from primary school level onwards. It is a medium-term goal that each individual's familiarity with the use of modern media can be taken for granted—this is not only in the interest of the citizens but also the basis for protecting national infrastructures.

Measures

Incorporating ICT, ICT security and media competence in curricula to a much greater extent: The use of ICT and new media as well as ICT security have to become an integral part of the curricula of all types of schools. These issues must be covered by a compulsory subject to improve media

skills in all areas. As children interact with new media at a very young age, this issue must be suitably addressed even at primary school level. The introduction of ICT-focused curricula in specific types of schools (comparable to today's sport, music or ICT secondary schools) is recommended.

Defining educational standards for ICT and ICT security: A meaningful and adequate level of ICT competence must be ensured across all types of schools.

Objective 2: Compulsory ICT training for all teacher training students

Hypothesis: Schools will not succeed in teaching a creative, safe and critical approach to ICT and new media unless teachers receive adequate training.

Strategic objective:
It is an important prerequisite for teaching the relevant skills that ICT (security) competence becomes part of the curricula of teacher training colleges and universities. Adequate in-service training programmes for fully-fledged teachers will ensure that ICT training can be implemented fast, effectively and on a sustainable basis.

Measures

Compulsory ICT training of all students of teacher training (at all pedagogical colleges and universities): All students undergoing teacher training require ICT training to enable them to use new technologies and media safely in their fields. They will also feel more confident using applications and services relevant to their areas of specialisation (e.g. Mathematica, GeoGebra, Google Earth, location-based applications) in daily teaching practice. Particular attention should be paid to the training of teachers in the ICT sector (ICT teacher training studies) as they will be responsible for teaching the general subject "ICT" as well as for the safe and professional use of ICT. It is therefore of vital importance to develop suitable teacher training programmes, and to address the ICT security issue appropriately in these programmes.

In-service training of teaching staff: The sustainable ICT competence of teachers must be ensured in programmes offered by teacher training colleges and universities.

Further development of training programmes for adults, especially parents: Special programmes have to be developed for parents within the school system which will help them to become a knowledgeable source of advice for their children and to examine their use of new media and the media skills.

Objective 3: Improving training structures for ICT security specialists in the tertiary sector

Hypothesis: In an area as sensitive as national security, specialised technical know-how and skills must be available in a country. This can be ensured by offering specific education and training programmes at tertiary level.

Strategic objective:
Existing study and training programmes—offered as a specialisation of general ICT studies as well as specific ICT security studies—will be further developed on a proactive basis. Networking and cooperation between educational organisations will be promoted (e.g. joint courses or interdisciplinary programmes).

Measures

National know-how in the area of ICT security: Strengthening and establishing national interdisciplinary competence centres in the area of ICT security as well as general, state-of-the art training in this field.

Promoting networking among individual educational organisations: Active cooperation among all educational institutions in Austria is of crucial importance. Curricula must be harmonised to achieve synergies and to use resources economically. Special attention has to be paid to the interface between identification of threats and response to system-specific risks.

Consideration of security aspects in ICT training: "Security by design"—as a guiding cross-cutting theme—means that security issues should be taken into account in all areas of ICT training.

Objective 4: ICT security as an important element of adult education/further training

Hypothesis: Today much of specialised knowledge becomes obsolete very rapidly, particularly in the ICT sector. Continuous further training and qualification programmes are therefore an important prerequisite for employee retention and productivity. ICT users, e.g. in small companies or in the private sector, pose a potential threat to the entire ICT infrastructure (discussed under the heading "bot networks") if they operate poorly secured systems. They must therefore be sensitised to the problem and receive suitable training.

Strategic objective:
All sectors of the population need to have a basic knowledge of ICT security: programmes must be developed and interlinked for specific target groups. The key target groups include employees of the IT and ICT sectors for whom continuous further training is essential, sole proprietorships as well as small and medium-sized enterprises not active in the technology sector as well as private persons (e.g. the 65+ generation).

Measures

ICT security in adult education: To enhance the integration and coordination of existing programmes, many of which are excellent. One of the main goals is to reach out to educationally disadvantaged groups. It is recommended to take advantage of resources (rooms, ICT resources) available in schools and local adult education centres. Company premises and public libraries could be used as teaching venues. Standardised training modules, such as ECDL und ECDL Security, should be promoted.

Continuous target-group-specific further training programmes: The continuous further training of employees in the ICT sector—and also in other sectors with a strong focus on technology and innovation—requires a variety of measures, e.g. fostering the development of programmes for specific target groups, enhancing self-directed learning skills ("lifelong learning") as well as taking ICT security issues into consideration as a cross-cutting theme in non-ICT-specific occupations. Networks among adult education organisations have to be enhanced, while further training programmes in the tertiary sector will be increased in cooperation with business and industry (study programmes and courses for working people, specific company-related training programmes, etc.).

Objective 5: ICT security research as a basis of national competence

Hypothesis: State-of-the-art competence must be ensured in the sensitive area of ICT security at national level to prepare decision-making processes and consequently to engage in development.

Strategic objective:
to promote the establishment of security research institutes as well as to strengthen networking among research organisations.

Measures

National know-how in ICT security research: to strengthen national competence centres active in ICT security research, to establish new ones, to create facilities complementing comprehensive security research programmes such as KIRAS (with a "communication and information" research sector) with a view to optimising resources; to promote a broad approach to security research and foster measures enhancing the national thematic priority of "protection of critical infrastructures"; to establish new research topics (e.g. development of robust applications and systems, improvement of network resilience as well as social and political resilience in the event of ICT-based attacks); to develop "common terms of reference" jointly with standardisation initiatives.

Promoting networking between individual research organisations: to make greater use of existing networking instruments, e.g. Security Research Map or KIRAS Innovation Platforms. Coordination and exchange of experience between ICT security research stakeholders to bundle the measures required to implement the findings of security research.

Objective 6: Covering ICT security to a greater extent in applied ICT research

Hypothesis: ICT security is an integral part of IT products, systems and solutions. Security aspects must therefore also become an integral part of ICT research projects. On the other hand, findings of other scientific disciplines (e.g. biology or psychology) should be taken into account in ICT security research to a greater extent than in the past.

Strategic objective:
Applied ICT research as well as other research areas should increasingly cover ICT security issues; this will strengthen ties with other scientific disciplines and promote practical application.

Measures

Security aspects in applied ICT research: to examine, if possible, in all ICT research projects which aspects relevant to ICT security have to be taken into account, e.g. by establishing additional evaluation criteria (similar to gender aspects, aspects of humanities, social and cultural sciences in KIRAS projects or security considerations involving RFCs). Cooperation between political decision-makers and research institutions active in technology assessment may be institutionalised, similarly to TAB in Germany or POST in England.

Promoting interdisciplinary approaches in security research and practical implementation: Findings and technologies from other areas (e.g. biology) are applied to ICT security research. To develop creative solutions to security problems, a research line on ICT security should be established in which other research disciplines participate on a mandatory basis. An institution responsible for evaluating and implementing findings of security research projects must be set up. Measures must be taken to improve the implementation of findings from security research in industry as well as in concrete projects. An "incentive system" (based on the model of the "Innovation

Cheque") is to encourage the development of ideas.

Objective 7: Active theme leadership in international research programmes

Hypothesis: In order to position Austria's strengths more effectively, Austrian delegates should increasingly address security research issues of national interest in European and international programmes.

Strategic objectives:
Austria strives for active theme leadership in EU research programmes.

Measures

Contributing themes considered important by Austria to research programmes: Austria should continue its efforts to contribute security research themes to European and international programmes (SECURITY, ICT, HORIZON 2020) with a view to highlighting the country's strengths. Austrian programme delegates should be involved in a timely manner as this will increase the likelihood of their being able to successfully contribute security research topics.

Accompanying measures

Firmer commitment to international standardisation and certification activities: In some selected standardisation areas such as the further development of ISO/IEC 27001 Austria is playing an active role. However, it should also participate more actively in other ICT security areas, e.g. ISO/IEC JTC1 WG 27 and CEN, the Common Criteria and European standardisation initiatives in the field of security research (Mandate M/487 to CEN, CENELEC and ETSI, etc.).

Maintaining and updating the Austrian Information Security Manual: The Austrian Information Security Manual supports efforts to ensure a uniform terminology and approach in establishing ICT security—both in public administration and business. Serving as a strategic framework for ICT security in Austria, the Manual is updated on an ongoing basis to meet constantly changing technical requirements and to respond to new developments in international standardisation.

Awareness

Initial situation

Security studies and situation reports on ICT security illustrate very clearly that human error facilitates or even causes a substantial proportion of all security-related incidents. Though incomprehensible at first glance, many issues can be explained when ICT security is examined more closely. It is based on three key pillars: technology, organisation and the human factor.

Human factor: Despite security-related progress and organisational rules which emerged in the industry and as a result of standardisation in the past few years, the human factor is still an important—probably the most important pillar—of ICT security. Ultimately, all technical and organisational security measures taken must be accepted and supported by human beings. After all it is the individual—the ICT user—who should be at the centre of all activities.

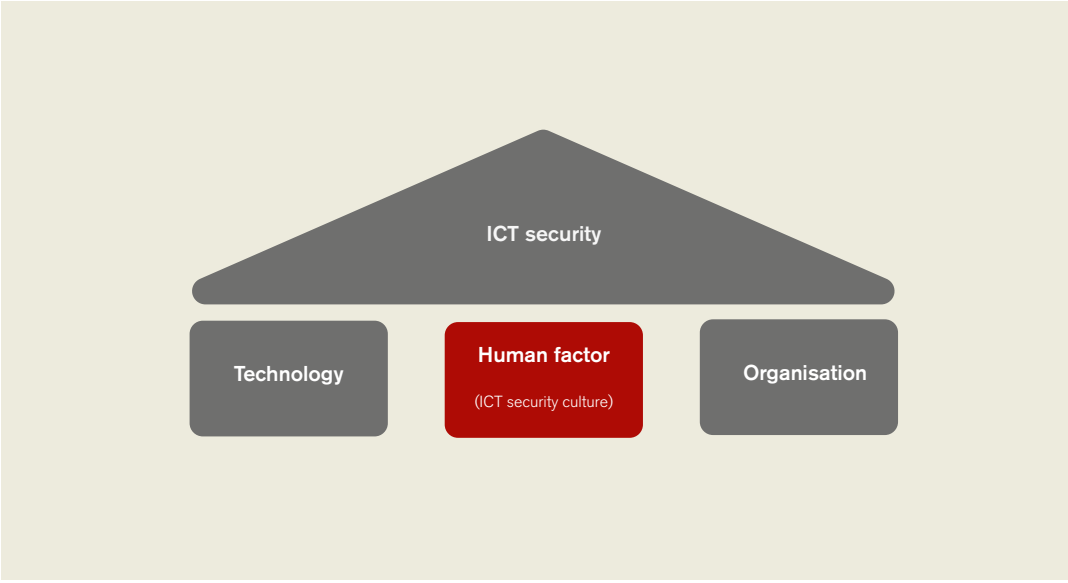
ICT security culture: A future-oriented ICT security approach must therefore be human-centred and based on strengthening ICT security culture. The ICT security culture will determine the perception, understanding, personal attitude and knowledge necessary for security-conscious action.

Despite all technical and organisational security measures available, sensitisation and awareness-raising as well as the knowledge of all target groups are crucial requirements determining the benefits and success of ICT security.

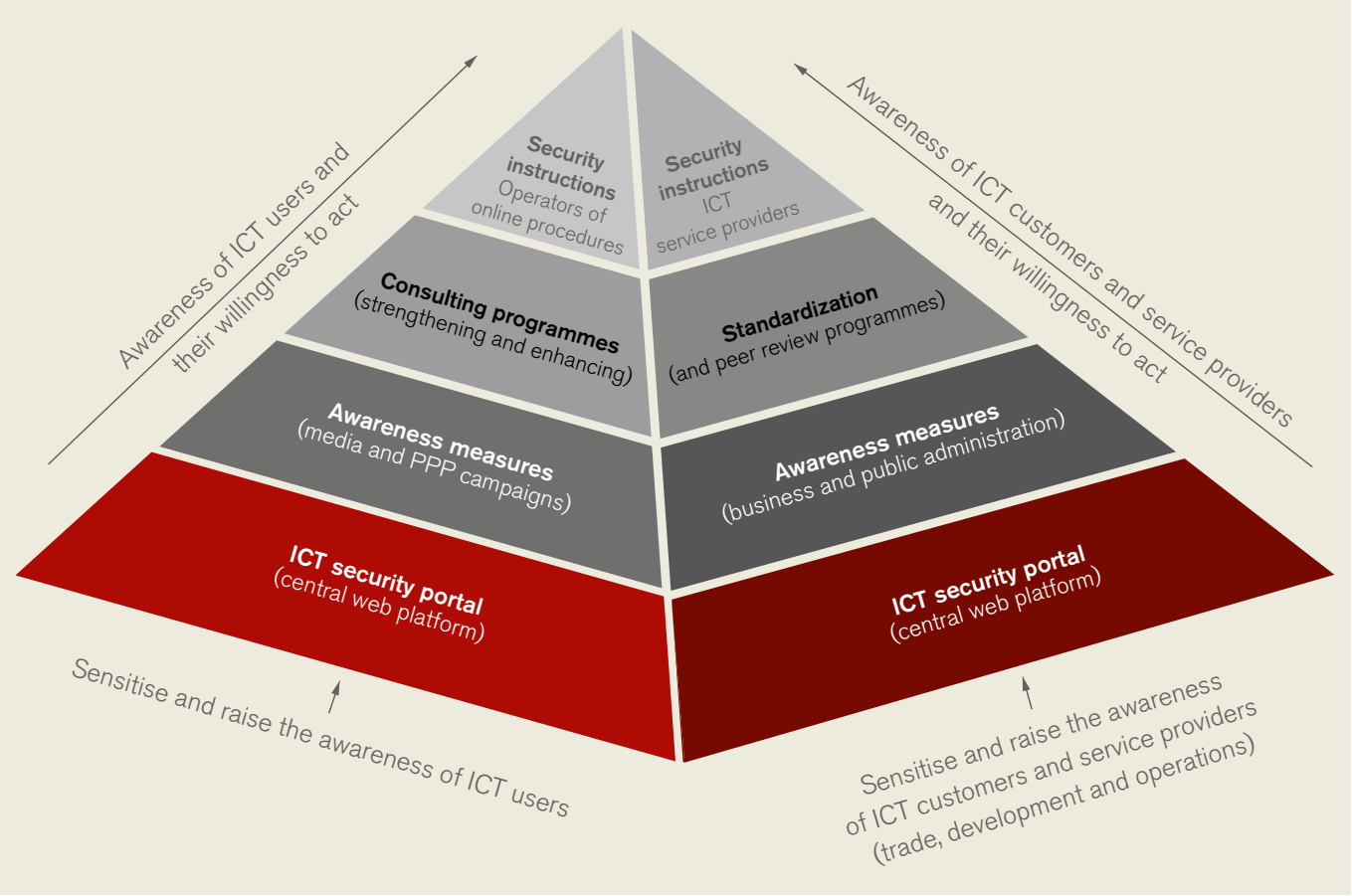
Three main goals of awareness-related measures:

- to strengthen the perception of ICT security as an important issue, to arouse personal interest in and attract attention to ICT security (sensitisation of the target group),
- to create positive personal attitudes and develop an understanding of the need for ICT security (raising awareness at different levels) and
- to promote knowledge about security-conscious action and the responsible use of information and ICT through concrete and specific recommendations for action for each target group.

Awareness-related measures have to be differentiated on the basis of action fields (such as citizens, economy, administration, education and research, CI) and target groups (in any case users, developers and operators of ICT).



Pillars of ICT security



Awareness measures

Strategic objectives and measures

Objective 1: Strengthening ICT security culture in Austria

Hypothesis: Many ICT users, customers and service providers (in trade, development and at operational level) are not aware of the threats arising in the context of ICT. They often lack the understanding and knowledge required for security-conscious action in cyberspace.

Strategic objective:
Well-aimed awareness measures in all relevant target groups and fields of action will promote and strengthen ICT security culture in Austria. ICT security culture ensures that the people involved act by giving due consideration to the threat situation in each case. As the third pillar of effective ICT security, ICT security culture ensures that the activities of all persons involved will be security-conscious and commensurate with the threat situation in each case.

Objective 2: Positive positioning of ICT security

Hypothesis: People often perceive the negative aspects of ICT security, e.g. additional workload, extra costs and restrictions on users, developers and operators. If no information is provided about the extent to which ICT security measures are necessary and/or appropriate, this will produce generally negative attitudes. Emphasis must be placed on positive aspects such as compliance with legal and contractual provisions and requirements, confidentiality, integrity,

availability of the information processed, avoidance of security incidents and consequential damages.

Strategic objective:
Within the framework of awareness campaigns, accompanying marketing measures ensure the positive positioning of ICT security and the initiatives of the National ICT Security Strategy. In the future the relevant target groups will perceive ICT security as a positive and necessary added value.

Objective 3: Harmonised and coordinated approach

Hypothesis: There are already some awareness initiatives in Austria. However, the various stakeholders coordinate them only to a limited extent. Various stakeholders have to collaborate in different fields of action in order to implement planned awareness measures within the framework of the National ICT Security Strategy.

Strategic objective:
The awareness measures planned in the framework of the National ICT Security Strategy are implemented on the basis of an approach developed jointly by the respective stakeholders. This ensures the necessary transparency, optimal use of synergy potential and maximum efficiency of initiatives.

Objective 4: Effectiveness and sustainability of awareness-raising measures

Hypothesis: Various statistical databases and studies provide sufficient data on the acceptance and use of ICT in Austria. There is, however, only rudimentary information on the present ICT security culture (sensitisation, awareness, knowledge and security-conscious action) as well as security incidents that really occurred (including causes and damage).

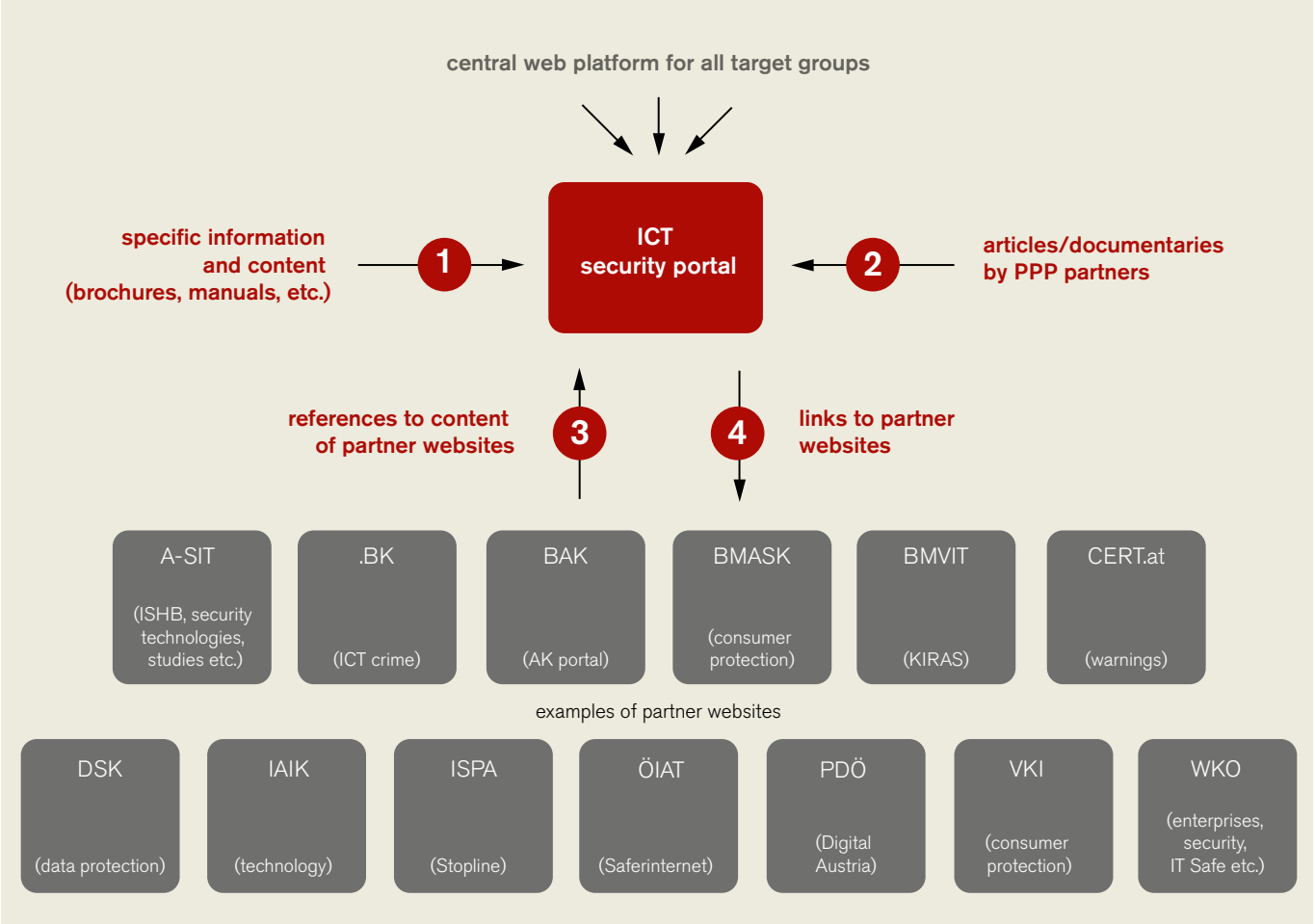
Strategic objective:
To ensure sustainability, Austria will in the future apply a measuring tool to evaluate the effectiveness of awareness measures on a regular basis. Moreover, it will be used to examine the effect of these measures on reducing security incidents. If required, operational measures will be taken to make the necessary readjustments.

Measures to achieve strategic objectives

The existing concept for achieving the strategic objectives focuses on targeted awareness measures to strengthen ICT security culture in Austria. To advance from sensitisation and awareness building to truly security-conscious action, information and communication should preferably take place when the individual's attention is high. A multi-tier information and communication concept is therefore required that reaches different target groups in different life situations and uses different media and channels for this purpose.

Setting up an ICT security portal: Designed as a web platform, the ICT security portal serves as the central point of contact for all target groups in ICT security issues and as a fundamental basis for information and communication for all awareness measures. The target groups comprise ICT users on the one hand and ICT customers and ICT service providers (trade, development and operations) on the other.

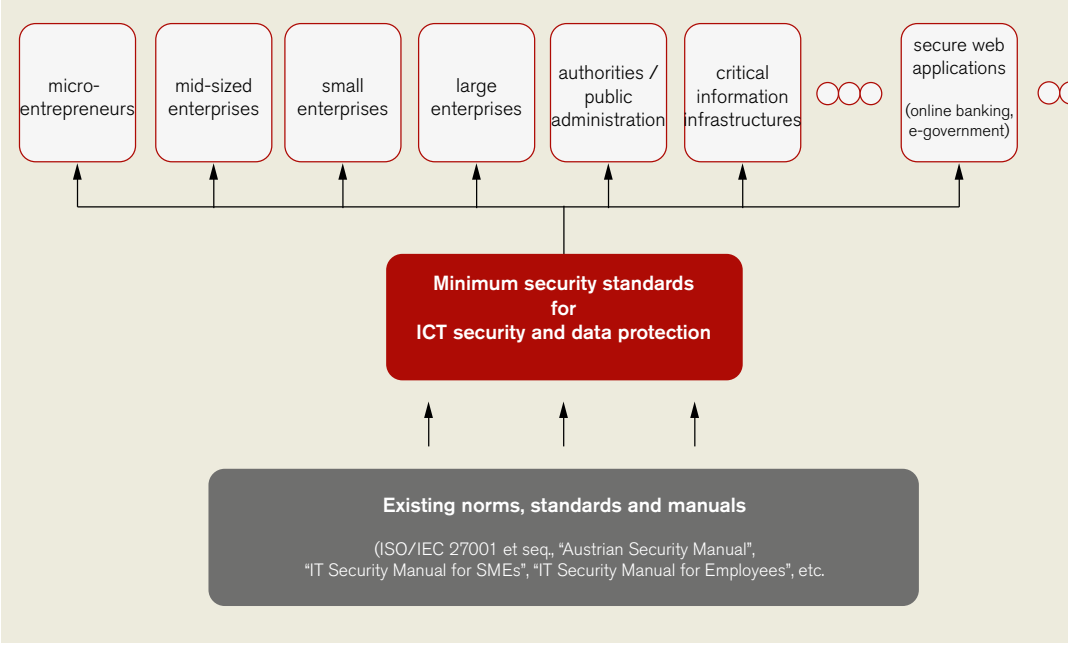
Awareness campaigns: Active information and communication is to enhance Austria's ICT security culture. Taking existing campaigns and initiatives into account, theme and target specific campaigns will be developed, coordinated and implemented together with stakeholders. ICT security is examined from different perspectives, relevant threats are pointed out, possible effects and damages highlighted and appropriate and meaningful security measures recommended. These recommendations have to be appropriate



ICT security portal
The central web platform for all target groups

and describe the benefits of ICT security based on different motivations for individual target groups (personal, economic and legal aspects). Such awareness campaigns include: articles/documentaries in existing formats (to fulfil an educational mandate) as well as information and communication by PP partners in the area of public administration, interest representations and the business sector. The campaigns will be complemented by e-learning programmes. The following themes have been proposed for campaigns: ICT security in private households, data protection for persons affected, data protection for young people, safe online banking, Internet guide for senior citizens, safe use of social media and networks, social media guide for parents, Warning: Internet Fraud!, consumer protection on the Internet, data protection provisions for customers, data protection provisions for service providers, Austrian Trust Circle, IT emergency management in enterprises, ICT security in enterprises, developing and operating safe online procedures, Attention: Industrial Espionage, ICT security compliance (check) in enterprises.

Consulting programmes: More profound and customised consultation by PP partners for different target groups, if required: citizens and private consumers, enterprises and start-ups, ICT service providers, organisations in the area of public administration as well as enterprises with critical infrastructure. The existing range of services is to be increased and expanded.



Minimum security standards for ICT security and data protection

Standardisation: Clear minimum security standards for ICT security and data protection have to be developed and published to ensure effective security and, in particular, to reach a common understanding of present requirements. In accordance with different threat potentials, minimum security standards at different levels must be defined, e.g. based on company size and sector. The development of standards will be based on the Information Security Manual and take into account other existing norms, standards, frameworks and manuals. Voluntary security peer review programmes by recognised Austrian universities and research institutions have to be set up and promoted. In evaluating the quality and security of their ICT services and ICT products, Austrian enterprises and organisations may be supported by external quality testing procedures. Such a certificate will allow them to demonstrate (competitive advantage) and prove (tender procedures) to the public (their customers) that their ICT security has been tested and conforms to security standards. The participating (recognised) institutions of the security peer review programmes will be published on the ICT security portal.

Examples of using existing structures and synergy potential

Awareness campaigns

- Articles/documentaries (educational mandate) in existing formats (e.g. Newton, Thema, Konkret das Servicemagazin, ATV report, etc.)
  - broadcasting (e.g. ORF and ATV channels) as well as print and online media
- Information and communication (active reference to the theme ICT security, distribution of brochures and providing information on websites) by
  - PP partners in the public administration with office hours for the public (police services, Advisory Service of Criminal Police, finance and customs offices, federal army, regional administration, district commissions, schools, municipal offices, etc.)
  - PP partners in the area of interest representations (WKO, AK, VKI, etc.)
  - PP partners in the business sector with customer service points (banks, Internet service providers, ICT retail store chains, ICT service providers, etc.)

Examples of using existing structures and synergy potential

Consulting programmes

- Advisory services for citizens and private consumers (e.g. by .BK, Advisory Service of Criminal Police, AK, VKI, OCG, etc.)
- Consulting of enterprises and start-ups as well as customised consulting and training programmes (including possible certification services) for ICT service providers in the framework of the WKO's special association for "consultancy and IT" (UBIT) (e.g. by the start-up service of the WKO, .BK, BMWFJ, A-SIT, etc.)
- Consulting of organisations in the field of public administration (e.g. by PDÖ, A-SIT)
- Specific consulting services on critical infrastructure to enterprises (e.g. by .BK, WKO, BMWFJ, A-SIT, etc.)

Security instructions: ICT users are highly aware of ICT security issues when registering and using online applications. This is relevant to ICT customers when purchasing ICT products and ICT services, awarding contracts for developing products or services or operating ICT applications or ICT infrastructure. To this end, compliance with security instructions is to become compulsory for operators of online applications and ICT service providers (trade, development and operations). Clearly structured and comprehensive security instructions will be developed, coordinated and made available to operators of online applications as well ICT service providers—in cooperation with interest representations and taking national and European legislation into account. The ultimate goal of the security instructions is to protect ICT users and ICT customers.

Accompanying measures

ICT Security Encyclopaedia: Finding a common language. As a first step, the ICT Security Encyclopaedia will explain the technical terms used in the context of the ICT Security Strategy. It has to be revised and updated on a regular basis.

Developing and implementing a marketing concept: In the framework of a marketing and media concept, the brand and a style guide will be developed to ensure the positive positioning of ICT security, professional presentation as well as the highest possible level of awareness and recognition.

Establishing public-private partnerships: Different media and, in particular, different communication channels are required to implement the planned awareness campaigns. Multipliers for the information and communication required will be found by establishing public-private partnerships with other stakeholders in Austria. These stakeholders will be published as PP partners on the ICT security portal.

Establishing a coordination structure: An appropriate coordination structure covering all stakeholders involved must be developed so as to ensure a harmonised and coordinated approach (management and control) within the framework of comprehensive awareness measures. Coordination and communication channels have to be established between individual stakeholders, the responsible points of contact as well as implementation plans.

Developing and implementing monitoring measures: Monitoring measures must be developed and used regularly with a view to ensuring the effectiveness and sustainability of the measures taken. To this end, suitable monitoring measures and responsible stakeholders have to be defined. Existing instruments and structures must be used, and suitable projects should be continued or extended.

Abbreviations and glossary

ATC
: Austrian Trust Circle, sector-specific network of critical information structures in Austria

CERT
: Computer Emergency Response Team, e.g. http://www.cert.at/

GovCERT
: Austria's Government Computer Emergency Response Team, http://www.govcert.gv.at/

SKKM
: Staatliches Krisen und Katastrophenschutzmanagements / Governmental crisis and civil protection management, http://www.bmi.gv.at/cms/BMI_Zivilschutz/mehr_zum_thema/SKKM.aspx

OSCE
: Organisation for Security and Cooperation in Europe, http://www.bmeia.gv.at/aussenministerium/aussenpolitik/europa/osze.html

OECD
: Organisation for Economic Cooperation and Development, http://www.oecd.org/home/

KIRAS
: Nationales Programm zur Förderung österreichischer Sicherheitsforschung / National Security Research Promotion Programme , coordinated by BMVIT, http://www.kiras.at/

TAB
: Büro für Technikfolgenabschätzung / Office for Technology Assessment in Germany, http://www.tab-beim-bundestag.de/de/index.html

HORIZON 2020
: New Framework Programme for Research and Innovation of the EU, http://forschungsrahmenprogramm.de/horizon2020.htm

ISO
: International Organisation for Standardisation, http://www.iso.org/iso/home.htm

IEC
: International Electrotechnical Commission, http://www.iec.ch/

CENELEC
: European Committee for Electrotechnical Standardisation, http://www.cenelec.eu/

CEN
: European Committee for Standardisation, http://www.cen.eu/

ETSI
: European Telecommunications Standards Institute, http://www.etsi.org/

SIHA
: Österreichisches Informationssicherheitshandbuch / Austrian Information Security Manual, https://www.sicherheitshandbuch.gv.at/downloads/Sicherheitshandbuch%20V3-1-001.pdf

CIP
: Critical Infrastructure Protection, division of the Federal Chancellery and the BM.I ensuring the comprehensive protection of Austria's strategic infrastructures

CIIP
: Critical Information-Infrastructure Protection, coordination of the strategic information infrastructures of Austria

ISK
: Information Security Commission, division of the Federal Chancellery, National Security Authority in Austria

FüUZ
: Führungsuntertützungszentrum / Joint Mission Support Command, department of the Austrian Federal Army

AbwAmt
: Abwehramt / Military Counter-Intelligence Office, department of the Austrian Federal Army

HNa
: Heeresnachrichtendienst / Army Intelligence Office, department of the Austrian Federal Army

BVT
: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung / Federal Office for the Protection of the Constitution and Counter-Terrorism, department of the BM.I, protects state institutions and their ability to act

BK
: Bundeskriminalamt / Federal Criminal Police Office, department of the BM.I, countrywide combat of penal offences http://www.bmi.gv.at/cms/BK/

C4
: Cyber Crime Competence Centre, department of the BM.I, coordination and reporting centre for cyber crime of the BM.I

Acknowledgements

This paper has been prepared by experts within the framework of five working groups. Working for many hours on a voluntary and unpaid basis, the experts contributed their expertise and extensive experience to this project.

The Federal Chancellery therefore warmly thanks all those involved, especially the heads of the working groups.

Working Group on Risk Assessment / Management – Status quo, Situation Monitoring and Conclusions – Threat Situation
Robert Schischka – CERT.at
Thomas Stubbings – Raiffeisen International

Working Group on Critical Infrastructure
Paul Karrer – Cyber Security Austria
Alexander Pschikal – Bundeskanzleramt

Working Group on Education and Research
Ingrid Schaumüller-Bichl – FH Hagenberg / OCG
Walter Seböck – Donau-Universität Krems

Working Group on Stakeholders and Structures, National and International Networks
Daniel Konrad – A-SIT
Wilfried Wöber – Univie/ACOnet

Working Group on Awareness
Martina Ertler – Wirtschaftskammer Österreich
Markus Kloibhofer – BMF
Hans-Jürgen Pollirer – Wirtschaftskammer Österreich
Josef Schröfl – BMLVS

Support to the heads of working groups: Helmut Hummer – Bundeskanzleramt, Alexander Klimburg – OIIP, Roland Ledinger – Bundeskanzleramt, Timo Mischitz – Bundeskanzleramt, Franz Vock – Bundeskanzleramt

Working group participants:

Gerhard Bisovsky
Thomas Bleier
Erwin Bosin
Stefan Brandl
Christian Braunsteiner
Ronald Bresich
Michael Brugger
Gerd Brunner
Barbara Buchegger
Michael Butz
Michael Danzl
Friedrich Dozler
Gerhard Dyduch
Christoph Eberl
Martin Ebner
Ralph Eckmaier
Kurt Einzinger
Rainer Eisenkirchner
Mathias Fahrner
Paul Falb
Eveline Fegerl
Martin Fellhofer
Stefan Fenz
Erhard Friessnik
Andreas Fritz
Anita Fröhlich
Gernot Fuchs
Christian Fuernweger
Thomas Geretschläger
Robert Gottwald
Ernst Graumann
Johann Haag
Helmut Habermayer
Harald Haselbauer
Wolfgang Haumann
Markus Hefler
Sandra Heissenberger
Otto Hellwig
Marcus Hild
Franz Hoheiser-Pförtner
Herbert Höllebauer
Manfred Holzbach
Thomas Hrdinka
Christian Hribernig
Matthias Hudler
Bernhard Jungwirth
L. Aaron Kaplan
Ernst Karner
Nieves Erzsebet Kautny
Joachim Klerx
Roman Kobylka
Leopold Koppensteiner
Manuel Koschuch
Klaus Kraner
Gerhard Krenn
Marco Lang
Martin Langer
Ulrich Latzenhofer
Thomas Latzer
Christoph Lechner
Josef Lechner
Franz Lehner
Wolfgang Liedermann
Jürgen Mang
Johannes Mariel
Georg Melzer
Alexander Mense
Thomas Menzel
Christian Minarovits
Joachim Minichshofer
Philipp Mirtl
Michael Müller
Rupert Nagler
Markus Narrenhofer
Markus Necker
Renate Neumüller
Andrea Nowak
Gerald Obernosterer
Lendl Otmar
Christian Pennerstorfer
Thomas Pfeiffer
Joe Pichlmayr
Helmut Pizka
Ralph Pöchhacker
Christian Polnitzky
Lukas Praml
Manfred Pregartbauer
Karl Preszl
Christian Proschinger
Günter Reiser
Wolfgang Resch
Philipp Reschl
Markus Robin
Karl Rossegger
Wolfgang R. Ryvola
Lambert Scharwitzl
Philipp Schaumann
Manfred Schleinzer
Matthias Schmidl
Rupert Schmutzer
Reinhard Schönthaler
Maximilian Schubert
Jan Schubert
Rainer Schügerl
Helmut Schwabach
Erich Schweighofer
Christian Schwertberger
Armin Selhofer
Alexander Siedschlag
Florian Skopik
Werner Spies
Werner Sponer
Johann Starlinger
Manuel Stecher
Wolfgang Steiner
Jörg Steiner
Barbara Steiner
Jaro Sterbik-Lamina
Matthias Straubinger
Alexander Szönyi
Alexander Talos-Zens
Alfred Tanzer
Simon Tjoa
Wolfgang Trexler
Gerald Trost
Thomas Von der Gathen
Christian Wagner
Thomas Wanasek
Edgar Weippl
Heinz Weiskirchner
Andreas Wespi
Christian Wiesener
Michael Wiesmüller
Martin Winkler
Christian Zagler
Christian Zmaritz