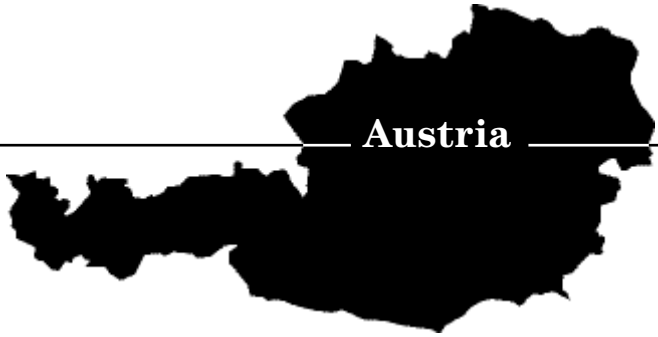
CIIP Country Surveys



Austria

The Country Survey of Austria 2004 was mainly written by Thomas Pankratz, Austrian Federal Ministry of Defence, Bureau for Security Policy. Dr. Pankratz wants to express his gratitude for the research assistance of Martin Leithner. In addition, Gerald Torst, Stabsstelle IKT-Strategie des Bundes, Federal Chancellery of the Republic of Austria and Otto Hellwig, Former Official of the Federal Chancellery, provided valuable input.

Austria

Critical Sectors

Austria as a modern society and as a small state is particularly vulnerable in the area of information. This includes both the military and the civilian sectors and, increasingly, business and industry as well.[74] Strictly speaking, there is no stringent, congruent, coordinated, CII/ CIIP-concept designated as such in Austria.[75] The following are seen in Austria as critical sectors:[76]

- (Tele)Communication,
- Banking and Finance,
- Broadcasting,
- Emergency Services,
- Energy,
- Information Services,
- Military Defense,
- Police Services,
- Post Systems,
- Public Administration,
- Public Health,
- Social Welfare,
- Transportation,
- Utilities,
- Water Supply.

74 Resolution by the Austrian parliament – Security and Defense Doctrine; Security and Defense Doctrine: Analysis- Draft expert report of 23 January 2001.

75 There is also no clear definition of CII/ CIIP, and the terms "CII/ CIIP" are not commonly used in Austria. Therefore, these terms are used in a broad sense for the purposes of this contribution.

76 Pankratz Thomas, Information warfare – Eine Bedrohung der 'wired society', in: Gärtner Heinz/ Höll Otmar, *Comprehensive Security* (Vienna, 2001).

Initiatives and Policy

There have been several substantial organizational and procedural efforts since the 1990s to manage CII(P) in Austria. The issue of CIIP has mainly been addressed by the government, especially by the *Ministry of Internal Affairs*, the *Ministry of Defense*, the *Federal Chancellery*, and the *Ministry of Public Service and Sports*.

Security and Defense Doctrine 2001

According to the principle of comprehensive security, the Security and Defense Doctrine[77] recommends the development of the existing *Comprehensive National Defense Program* into a system of *Comprehensive Security Provision* by focusing on the new risks and threats and by amending legal provisions.[78] This also includes all measures referring to CIIP.[79] The Doctrine clearly stresses that for small states, full and unimpaired access to the required information is a basis for their freedom of action in security matters.[80]

The implementation of Austria's security policy within the framework of the Comprehensive Security Provision relies on systematic co-operation among various policy areas on the basis of appropriate sub-strategies.

In addition to the sub-strategies, which are mentioned in the doctrine and are currently being elaborated, it was decided to work out a specific sub-strategy dealing with IT security. A project team under the lead of

77 http://www.bka.gv.at/bka/sicherheitspolitik/doktrin.html.

78 Resolution by the Austrian parliament- Security and Defense Doctrine; Security and Defense Doctrine: Analysis – draft expert report of 23 January 2001.

79 The concept of Comprehensive National Defense as developed from 1961 onwards was embedded in the Constitution in 1975. Under Article 9a of the Austrian Constitution, the role of Comprehensive National Defense is to "maintain [Austria's] independence from external influence as well as the inviolability and unity of its territory, especially to maintain and defend permanent neutrality". Together with the constitutional amendment, the Austrian parliament unanimously adopted a resolution in 1975 "on the fundamental formulation of Comprehensive National Defense in Austria" (defense doctrine). These were the foundations of the current national defense plan, which was adopted by the Austrian government in 1983 and identified the "protection of the country's population and fundamental values from all threats" as a basic goal of Austrian security policy.

80 Security and Defense Doctrine. Analysis – draft expert report of 23 January 2001.

the *Chief Information Office Austria*[81] in close co-operation with the *Federal Chancellery* and the *Ministry of Internal Affairs* was set up for this purpose.

Y2K Efforts

A special working group under the lead of the IT coordinator was established in the Federal Chancellery in order to sensitize and mobilize governmental authorities for problems anticipated in connection with Y2K. This group coordinated and monitored the preparedness of the critical infrastructures (e.g. energy, transport, banking). A special working group of the Federal Chancellery called *Federal Crisis Management* was ready for emergencies. From 31 December 2000 until 3 January 2001, the special "Info point 2000" was in charge of gathering status reports and reports on severe problems from all other ministries, the federal counties, and other relevant institutions, namely the critical infrastructures.[82] Yet, all these efforts had only limited consequences for CIIP in the following years. It should, however, be noted that the CIRCA warning system uses comparable structures and methods for its work.

E-Government Program

The government program of the year 2000 recommends the implementation of so-called "e-Government" in Austria. E-Government[83] refers to two channels of communication: First, electronic communication between citizens and public administration (G2C),[84] and secondly, communication between different branches of public administration (G2G).[85] To make the Austrian e-Government secure, the Austrian seal of approval for e-Government was developed by the IKT board.[86] This seal of approval is issued by the Federal Chancellor Office only under certain conditions that have to be fulfilled for three years. After that period, approval can be renewed.

81 http://www.cio.gv.at.

82 *Zivilschutz aktuell*, No. 4/ 1999; pp. 13–19; Anfragebeantwortung 6111/ J XX. GP.

83 On the implementation of e-Government in Austria, see http//www.bka.gv.at and http://www.cio.gv.at/egovernment.

84 Methodology, basic principles, structure, and examples of this topic, see: Hollosi Arno. *Sicherheit mit offenen Standards für die Verwaltung* (Vienna, 2002).

85 E-Government in Austria also includes the pilot project "Bürgerkarte" (citizen card): see below.

86 http://www.cio.gv.at/egovernment/.

One essential part of the whole project is the guideline paper on "Network Safety in the Field of e-Government".[87] This guideline is currently being developed and will mainly deal with the technical aspects of network safety. It will be published after completion by the IKT-Staff Unit and after having passed the IKT-Board.

Official Austrian Data Security Website

The official Austrian data security website,[88] which is coordinated by the Federal Chancellery, serves as an information desk for citizens in important matters such as data security, the Schengen Information System, etc. It also informs the public about the work of the *Commission on Data Protection*. The reports of this commission are available on the website.

Pilot Project Citizen Card

The aim of this pilot project, which was launched in January 2003, is to reconsider the concept of "Bürgerkarten" (Citizen Cards). This is a chip card with encrypted information of the central registration office. This test run was initiated by the national provider of digital signature cards (a.trust), the Austrian Computer Society, and the IKT board of the Federal Chancellery.[89]

Organizational Overview

Public Agencies

Currently, the main responsibility for CIIP lies within the public sector. So far, no single authority is responsible for CII/ CIIP.

Generally speaking, all ministries have their own specific security measures to defend against outside attack and to prevent the unauthorized usage of data, and all ministries have special departments for Information

87 "Netzwerksicherheit im Bereich e-Government".
88 http//www.bka.gv.at/datenschutz/index.
89 *Kurier* newspaper, 28 November 2002.

Technologies. A Chief Information Officer (CIO) leads these departments.[90] Ministerial security concepts rest on two pillars: Pillar 1 refers to organizational and procedural measures to protect the internal network in general. Pillar 2 refers to technical means for the protection for sensitive data.

Ministry of Internal Affairs

Several divisions of the Ministry of Internal Affairs deal with CII/CIIP, especially with aspects of data security and cyber crime. Division V/8, for example, is responsible for data security in general.[91] The Criminal Police's homepage issues information on Internet security. The *Center for the Fight against Internet Crime*[92] was established in August 1999 under the auspices of the Ministry of Internal Affairs.[93] Austrian "Cybercops" represent Austria in the *European Network of Forensic Science Institute on Computer Crime* (ENFSI).[94] As medium-term measures to combat cybercrime more efficiently, the following steps are planned:

- an increase of the personal staff in the department II/BKA/16,
- further rationalization,
- stronger cooperation with the Austrian economy/private sector,
- more information for the public.[95]

Ministry of Defense

In the framework of the Ministry of Defense, Department II (the so called control- department) is responsible for matters concerning all aspects of information warfare. It fulfills its duties in close cooperation with the newly established "Leadership Support Command" and the two military intelligence services.[96]

According to the Austrian constitution, the Austrian army is not only responsible for national defense, the maintenance of internal order, and internal

90 *The Security Handbook of the Federal Government* provides guidelines for CII security measures; these measures are implemented and realized by the ministries at their own discretion. The complete handbook is available at http//:www.cio.gv.at/securenetworks/sihb/.

91 Interview with a BMI representative; see also the portfolio of the Ministry of Internal Affairs.

92 Zentralstelle zur Bekämpfung der Internetkriminalität.

93 The Center for the Fight against Internet Crime has been part of the Federal Criminal Office since 2001.

94 http://www.bmi.gv.at/web/bmiwep.nsf/A11Pages/BMI020211131?OpenDocument.

95 http://www.bmi.gv.at/web/bmiwep.nsf/A11Pages/BMI020211131?OpenDocument.

96 "Heeresnachrichtenamt" and "Heeresabwehramt". Interview with a representative of the Ministry of Defense, December 2002.

security, but also for the protection of the constitutional institutions, their capacity to take legal actions, and the democratic freedom of the Austrian citizens. These duties also include the protection of critical information infrastructures. These protective measures have been subjected to several exercises held in close co-operation with the civilian institutions.

Board of Information and Communication Technology Strategy (IKT Board)

The *Board for Information and Communication Technology Strategy*[97] (IKT Board) was established in July 2001 as part of the *Chief Information Office* and was based on a decision of the Council of Ministers of 6 June 2001 referring to a "restructuring of the government's IT strategy". It is located at the *Ministry of Public Service and Sports*. This institution deals primarily with all aspects of e-Government; including security measures, such as the Austrian IT Security Handbook for the public administration[98] and the seal of approval for secure and trustworthy e-Government.[99]

Government Headquarters for Information and Communication Technology Strategy

The *Government Headquarters for Information and Communication Technology Strategy* was established in July 2001. The main task of this institution is the coordinated implementation of e-Government at all levels of the public administration. It is also responsible for IT security in these areas. Several working groups are tasked with analyzing and advancing awareness of these topics. The *Government Board for Information and Communication Technology Strategy* published an updated version of the IT Security Handbook in 2001. This handbook gives an overview of IT security in general and informs readers in a broad and comprehensive way about fundamental aspects and measures in the field of IT.[100]

Commission on Data Protection (DSK)

The *Commission on Data Protection* (DSK) serves as independent control authority that deals with data processing in the public as well as in the private sector. The DSK is located at the Federal Chancellery; it is chaired by a judge. All citizens have the right to appeal to this commission in case of a (supposed) violation of their rights in the field of data security. The

97 Stabsstelle IKT-Strategie des Bundes.
98 http://www.cio.gv.at/securenetworks/sihb.
99 http://www.guetesiegel.gv.at.
100 The complete handbook is available at http:www.cio.gv.at/securenetworks/sihb/.

commission verifies these claims and takes measures to remedy confirmed violations. A Data Processing Register located at the DSK is the central collecting point for personal data that has to be reported.

Public Private Partnerships

"Security in the Internet" Initiative

The cooperative initiative between the Ministry of Internal Affairs and the chamber of commerce was launched in October 2002. The main aim is to improve the prerequisites for IT infrastructure and to foster the confidence of enterprises and costumers in the Internet.

A first step was the establishment of a common expert working group, composed of representatives of the Ministry of Internal Affairs and 80 of Austria's top 500 companies. Further steps include an information campaign in 2003 ("Telefit-road-show") and further research in the field of the Internet and the economy.[101]

Center for Secure Information Technology Austria (A-SIT)

A-SIT was founded in May 1999 as an association supported by the Austrian National Bank, the Ministry of Finance, and the Graz University of Technology. Its tasks include general monitoring of IT security[102] and the evaluation of encryption procedures.[103]

Early Warning Approaches

Austria has an early warning system for nuclear catastrophes[104] and natural and technical disasters that is primarily based on bilateral treaties and national (public and private) efforts.[105] However, to date, no comprehensive and coordinated early warning system for attacks on critical information systems is in place or planned.

101 Die Bundepolizei, No. 6/ 2002; p. 78, *Die Presse* newspaper, 18 September 2002.

102 A-SIT makes tools and demonstration examples available at the homepage of A-SIT: http://demo.a-sit.at.

103 http://www.a-sit.at/asit/asit.htm.

104 This is primarily provided by the so called "Strahlenfrühwarnsystem", which is in the responsibility of the Ministry for Enviroment and Argiculture.

105 The central institution is the so called Bundeswarnzentrale (Federal Emergency Operations Center), located at the Ministry of Internal Affairs.

Computer Incident Response Coordination Austria (CIRCA)

Computer Incident Response Coordination Austria (CIRCA) is Austria's main organization in the field of IT early warning systems. It is a public private partnership whose main actors are the Federal Chancellery, the *Federation of the Austrian Internet Service Providers* (ISPA), and the *Center for Secure Information Technology Austria* (A-SIT). It is a web of trust between Internet Service Providers (ISPs), IP network operators from the public and private sectors, and enterprises in the field of IT security. The electronic communication network of the private sector is run by ISPA, whereas in the public sector the Federal Chancellery has the lead.

The aim of this Austrian security net is to provide an early warning system against worms, viruses, DDOS attacks, and other threats that endanger IP networks and their users. Therefore, CIRCA issues alerts and risk assessments and provides information about precautionary measures.

The organizational platform was established after the "Love Bug" virus caused significant damage to Austrian IT systems. It took some time to identify the main actors that would be willing to participate in a warning system. The next steps involved the construction of a technical system and a pilot phase.

This pilot system consists of two list servers run by the Federal Chancellery and the ISPA. Depending on the severity of the incident, warning or alarm messages can be released to the subscribers of the system. The subscriber base (between 12 to 15 individuals) is limited to persons that are able to contribute to the system. Furthermore, a help forum and a discussion list have been implemented. In this setting, the system allows specialists to communicate about incidents, be they in the private or the public field. After an assessment, countermeasures can be discussed and put in place.

One important measure in the establishment of a reporting system is to agree on codes of conduct. These rules govern the behavior of the participants and especially the handling of sensible information provided by the system. Since members include competing companies, it has to be clear that the messages and information that circulate on the CIRCA system have to be treated confidentially. If this rule were flaunted, nobody would report really interesting facts.

The system is now switching to standard operation, and the positive effects of expert communication in different fields of IT security on the evaluation of incidents and possible countermeasures are evident. The next step is to place more sensors in the net to be able to react faster to possible attacks.

The members of CIRCA participated in the European Commission's efforts to establish a *European Warning System*. CIRCA can be seen as the Austrian part of an international system, and CIRCA will cooperate in the setting of the *European Network Security Agency* (ENISA).

In the aftermath of 11 September 2001, a preliminary crisis group was established that could deal with a situation where the main ISPs or even the net itself would not be operational. The goal was to be able to coordinate measures to minimize the possible Internet downtime.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger