CIIP Country Surveys

Germany

Germany

Concept of CIIP and Description of System

The main premise underlying CIIP in Germany is that the government and society as a whole heavily depend on a secure infrastructure to function. Infrastructure that meets this definition is defined as critical.[1] The following infrastructure sections are defined as critical in Germany:[2]

- Banking and finance,
- (Tele-) Communications,
- Energy and utilities,
- Public administration,
- Public health,
- Rescue services,
- Transport.

CIIP Initiatives and Policy

CIIP Initiatives

AG KRITIS

Initiated by the report of the President's Commission of Critical Infrastructure Protection (PCCIP) in the US, an inter-ministerial working group on CI (AG KRITIS) was established in 1997 by the Federal Minister of the Interior.[3] It consisted of the ministerial representatives, a steering committee, and a permanent office at the Federal Agency for Security in Information Technology (see below).

The mandate of AG KRITIS was:[4]

- To describe possible threat scenarios for Germany,
- To conduct a vulnerability analysis of Germany's crucial sectors,

1 http://www.bsi.de/literat/faltbl/kritis.pdf.
2 http://www.bsi.de/literat/faltbl/kritis.pdf, and http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, 6.
3 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, 6.

- To suggest countermeasures,
- To sketch an early warning system.

The objective was to deliver the results in a report. The following findings are taken from a draft version of this report;[5] the report itself was never published.[6] In the first half of 1998, AG KRITIS conducted a survey of the federal public administration with a focus on the identification of the specific CII situation in the individual administrative agencies, an analysis of the IT dependency of each infrastructure sector, and an assessment of possible damages.[7] The following is an overview of the main results:[8]

- The awareness of IT threats varies heavily from agency to agency,
- There was a strong reluctance among the interviewees to reveal vulnerabilities in the IT security structure,
- Generally, the main threats for the IT systems are hacking and unauthorized access to data.

The creation of AG KRITIS was an important basis for all the later activities of public agencies in Germany. Its work is carried on, e.g., by the Federal Agency for Security in Information Technology.[9] Furthermore, the Y2K rollover together with the "Melissa" and "I Love You" virus incidents have increased public awareness.

Enquête Commission

In mid-1998, the so-called Enquête Commission on "The future of the media in business and society – Germany's progress towards the information society"[10] issued its fourth progress report, "Security and Protection in the Internet" (Sicherheit und Schutz im Netz).[11] The commission contributed to the collection and assessment of major risks linked to the

4 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, and http://ww.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld003.htm.
5 See, e.g., http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, also available at http://cryptome.org/Kritis-12-1999.html or http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.
6 Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Germany.* (version April 2002).
7 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html.
8 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html.
9 http://www.bsi.bund.de/fachthem/kritis/index.htm (in German) or (in English) http://www.bsi.bund.de/literat/faltbl/kritis_e.htm.
10 The commission was established by the German Bundestag (federal parliament).
11 http://www.bundestag.de.

new information technologies. Furthermore, it made some important proposals for risk management.[12]

Campaign "Security in the Internet"

The campaign "Security in the Internet"[13] is a combined initiative by the Ministry of the Interior, the Ministry of Economics and Technology and the Federal Agency for Security in Information Technology (since 2000). Its main objectives are to promote awareness among citizens and companies, to recommend improvements to Internet security for private and corporate users, and to act as a forum for information-sharing.[14]

Task Force "Secure Internet"

As a reaction to the DDoS-attacks in February 2000 against commercial Internet sites like yahoo.com, cnn.com, ZDNET.com, etc., an inter-ministerial task force called "Secure Internet" was established. Its main goals are to identify possible threats and to study countermeasures. By June 2002, its publications included recommendations on protection against DDoS-attacks and information on 0190-dialers.[15]

Comprehensive Threat Analysis

In the fall of 2001, a comprehensive threat analysis for Germany was published by the Ministry of the Interior.[16] Besides other threats, information security is defined as crucial for the security of the society and the success of the economy. The risk management approach for information security as proposed in this paper assumes responsibility will be mainly delegated to the company providing information infrastructure services.

Infrastructure Analysis Studies

In mid-2002, the Ministry of the Interior and the Agency for Security in Information Technology (see below) launched a series of studies to systematically analyze the CI/CII sectors. These will give an overview of each sector and its internal structures, identify the critical processes,

12 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html.

13 http://www.sicherheit-im-internet.de.

14 http://www.sicherheit-im-internet.de/home/home.phtml, and http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld005.htm.

15 http://www.bsi.de/taskforce/index.htm.

16 Bundesministerium des Innern. *Zweiter Gefährdungsbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grosskatastrophen und im Verteidigungsfall*. (Berlin, October 2001).

name the dependencies within and across sectors, and list preventive measures. The results of this comprehensive, structured analysis will be used as an important knowledge base for further activities and deeper research.

Further Activities

Besides the above-mentioned activities, the armed forces (Bundeswehr)[17] have initiated various steps within the field of CIIP.

Presently, there are no comprehensive interdependency studies publicly available in Germany.[18] A survey of representatives of CI/CII business sectors was taken in an initial step to systematically collect threats and expected damages to CII. The collected data was summarized in a matrix.[19] Some sector-specific studies have been published in the meantime, e.g. for the financial sector.[20]

CIIP Policy

Though CIIP is a growing issue in Germany, a comprehensive policy document was still lacking by mid-2002. But priorities are named in the framework of the different initiatives mentioned above. Generally speaking, they are:[21]

- To identify new vulnerabilities in Germany's national security,
- To conduct a detailed analysis of IT threats,
- To develop appropriate detection measures,
- To push the process of information-gathering,
- To upgrade the IT basic security (Grundschutz).

Concept "Critical Infrastructure"

The Federal Agency for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI) has defined a security concept "Critical Infrastructure" that includes possible measures going beyond basic IT security measures. Though the importance of such mea-

17 http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.

18 Interview with a representative of the consulting company Industrieanlagen-Betriebsgesellschaft (IABG), May 2002.

19 For details see Hutter, Reinhard. "Cyber-Terror: Risiken im Informationszeitalter". In: *Aus Politik und Zeitgeschichte* (vol. 10/11, 2002): 36.

20 Bundesamt für Sicherheit in der Informationstechnik (BSI). *IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft.* (Ingelheim, 2002) http://www.bsi.de/presse/pressinf/itkredit.htm.

sures is well recognized, they have to be limited to a selection of issues due to cost and effectiveness constraints. To define these issues, the BSI recommends the following step-by-step procedure:[22]

- To define a business strategy for trade using CII,
- To assemble a stock of IT techniques and components in consideration of mutual dependencies,
- To define the criticality,
- To verify and facilitate decision-making,
- To define appropriate measures and concepts.

Combating Terrorism

The events of 11 September 2001 made additional resources available under the heading of the "campaign against terrorism". Part of these additional funds will be used for combat against cyber terrorism in the future. Thanks to these additional resources, current and probably also new initiatives in Germany will be funded.[23]

Law and Legislative Action

Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations[24]

The purpose of this law is to create the conditions for electronic signatures. This law deals with issues such as technical security, voluntary accreditation, supervision, liability, and data protection.

Information and Telecommunications Services Act[25]

The Information and Telecommunications Services Act of 1997 was the starting point for the liberalization of the German telecommunications market.[26]

21 http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.
22 http://www.bsi.de/literat/faltbl/kritis.pdf.
23 Dependability Development Support Initiative, Country report Germany (version April 2002).
24 http://www.iid.de/iukdg/gesetz/Signaturg_engl.pdf.
25 http://www.iid.de/iukdg/gesetz/iukdge.html.
26 Interview with a representative of the consulting company Industrieanlagen-Betriebsgesellschaft (IABG), May 2002.

Act on the Utilization of Teleservices[27]

This act will be the basis for the establishment of uniform economic conditions for the various applications of electronic information and communication services.

Teleservices Data Protection Act[28]

The purpose of this act is to define provisions for the protection of teleservice users' personal data within the framework of the Act on the Utilization of Teleservices, which governs the collection, processing, and utilization of such data by service providers.

Electronic Signature Act[29]

In May 2001, this act (which conforms to EU regulations) replaced the existing pioneer Digital Signature Act of 1997. The main purpose of the act is to define a framework for the handling of electronic signatures.

Organizational Analysis

Public Agencies

Ministries and Agencies

The main ministries involved in CIIP at the national level in Germany are the Ministry of the Interior, the Ministry of Economics and Technology, and the Ministry of Defense. They are supported by the Agency for Security in Information Technology (BSI) and the Reg TP (regulation authority for telecommunications and postal services).

Agency for Security in Information Technology[30]

One of the most important agencies dealing with CIIP in Germany is the Federal Agency for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI), which was founded in 1991. The agency is subordinated to the Federal Ministry of the Interior. Its technical leadership is widely accepted and recognized. Within the BSI, there is a section responsible for CII. This section focuses its work on

27 http://www.iid.de/iukdg/aktuelles/fassung_tdg_eng.pdf.
28 http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf.
29 http://jurcom5.juris.de/bundesrecht/sigg_2001/inhalt.html.
30 http://www.bsi.bund.de.

the dependability of CII in the work of the government and the public administration. Efforts are being made in the field of vulnerability and threat assessment. A CERT (called CERT-Bund) is also part of the Federal Agency for Security in Information Technology.

Further Important Actors

Further actors involved within the Federal Administration are the Federal Law Enforcement Agency (Bundeskriminalamt, BKA)[31] and some other ministries.[32] The Federal Intelligence Service (Bundesnachrichtendienst, BND)[33] is responsible for compiling threat analyses.

Cooperation between Public and Private Sectors

The prevalent premise in Germany is that cooperation between the public and the private sectors is the best strategy.[34] In general, the private sector sees little need for initiatives that focus on the private sphere only. The most important input from the private sectors is given in the context of cooperation with actors from the public sector. There are several cooperation initiatives in Germany between public and private actors related to CIIP.

Initiative D21[35]

The Initiative D21 is the largest private-public partnership in Germany. This economic initiative also deals with dependability issues. The Initiative D21 is a neutral platform, independent of party allegiance or the industrial sector. The work of the Initiative D21 is based on the premise that the transition of the country from an industrial society to an information society is a task for both politics and the economy.

D21 is a model of an "activating government". There are 226 participants; all sectors of industry (not only IT providers), institutions, and politics are represented.[36] The Initiative D21 has formed 5 task forces and 15 sub-task forces. In the task forces, important topics are discussed and

31 http://www.bka.de.
32 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld004.htm.
33 http://www.bundesnachrichtendienst.de/start.htm.
34 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld009.htm.
35 http://www.initiatived21.de.
36 Including 94 member companies, 33 sponsors, 59 supporters, and 43 advisory council members.

agreements are implemented. Some of the main activities of the task force on "Security and Trust in the Internet" include:

- The campaign "Internet for Everyone" with the aim of promoting trust and confidence,
- The study "Internet Access in Germany",[37]
- Recommendations for linking up the different CERTs.

Partnership for Secure Internet Business

The Partnership for Secure Internet Business ("Partnerschaft Sichere Internet-Wirtschaft") is supported by the Ministry of Economics and Technology (Bundesministerium für Wirtschaft and Technologie, BMWi)[38] and was founded in May 2000. The partnership was initiated by the Minister of Economics and Technology together with ten prominent trade associations and companies.[39] The main actors in the "Partnerschaft Sichere Internet-Wirtschaft" are the Ministry of Economics and Technology from the public sector, and up to 40 trade associations and companies from the private sector.

The purpose of the "Partnership for Secure Internet Business" is to ensure a secure and trustworthy Internet for e-business and to promote security as a quality factor. Some of the objectives set until the end of 2002 are:

- A comprehensive awareness campaign on typical security-relevant business mishaps,
- Better transparency through security-relevant standards,
- Observation of trends in sensitive infrastructure as well as increasing awareness of the dangers presented by industrial espionage,
- Improvement of precautionary measures and assistance for small and midsize companies through suitable CERT structures (Computer Emergency Response Teams).

Working Group on Infrastructure Protection (AKSIS)[40]

Based on the premise that the increasing dependability of society on CII means the linked risks must be studied in a comprehensive approach, the Working Group on Infrastructure Protection (Arbeitskreis zum Schutz

37 This was adapted from Tony Blair's "Digital Divide" study.
38 http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=48&tdid=1616.
39 See http://www.sicherheit-im-internet.de.
40 See http://www.aksis.de, and http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld010.htm.

von Infrastrukturen, AKSIS) was established in 1999 on the initiative of the Zentrum für Strategische Studien (ZES), which belongs to the company IABG (Industrieanlagen-Betriebsgesellschaft). The main purpose of AKSIS is to provide a forum for information exchange to analyze and to assess the dependability of CI/CII sectors. AKSIS has no official government or industry mandate. It is purely voluntary and informal. There are two meetings per year at which representatives of the public and private sectors (ministries, armed forces, police, telecommunication, energy, transport, banks, academia, etc.) participate.

In November 2001, AKSIS organized the Cyber Terror Exercise (CYTEX) at IABG in Ottobrunn near Munich. Participants came from several federal ministries, other bodies of the public administration, and the industry. The core element of the exercise was a scenario of a series of attacks on the abovementioned public and private actors' IT systems and a large bank in the Berlin area with possible blackmail.[41]

Early Warning

The study "CERT Infrastructure Germany"[42] was published in January 2002. It determined that besides the already existing CERTs (such as dCERT,[43] DFN-CERT,[44] S-CERT,[45] secu-CERT,[46] Telekom-CERT,[47] CERT-Bund,[48] etc.), a CERT following the needs of SME was required. This is being established together with the industrial association "BITKOM".[49]

CERT-Bund

The so called "Referat CERT-Bund" was established on 1 September 2001 at the Agency for Security in Information Technology. The CERT-Bund is a central contact point charged with the security of data processors and networks of the federal public administration. The CERT-Bund also offers

41 For details see Hutter, "Cyber-Terror", 37–38.
42 See http://www.initatived21.de.
43 http://www.dcert.de/index_e.html.
44 http://www.cert.dfn.de.
45 http://www.s-cert.de.
46 http://www.secunet.de.
47 http://www.telekom.de/dtag/home/portal.
48 http://www.bsi.de/certbund/index.htm.
49 http://www.bitkom.org.

some of its services to clients from the private sector. However, several services are only available to the federal administration (e.g., incident response).[50] The CERT-Bund's main tasks include warning and information-sharing, data collection, analysis and processing of information, documentation and dissemination, sensitization of IT decision makers, and cooperation with existing CERTs.[51]

Research and Development

In 2000, the Federal Ministry for Education and Research (BMBF) published its "Concept for action – Information technology in education". The concept is a core element in the implementation and strategic refinement of the action program "Innovation and Jobs in the Information Society of the 21st Century". Likewise, the concept is the BMBF's contribution to the implementation of the EU's action plan within the framework of the eEurope Initiative.[52]

Research and development (R&D) related to the field of CIIP is mainly done at universities. Some of the most important of these are the Technical University Munich (Computer Sciences),[53] the University of Hamburg (Computer Sciences),[54] and the Fachhochschule Bonn-Rhein-Sieg (Applied Computer Sciences and IT Security).[55] Furthermore, at the Ruhr University of Bochum, the faculty for electrical engineering and information technology offers a special academic program for IT security.[56] The Institute for Information, Telecommunications, and Media Law (ITM) at the University of Münster focuses on legal problems concerning the information society.[57]

50 Ennen, Günther. "CERT-Bund – eine neue Aufgabe des BSI". In: *KES Zeitschrift für Kommunikations- und EDV-Sicherheit*. Bundesamt für Sicherheit in der Informationstechnik (BSI). (Bonn, June 2001): 35 and http://www.bsi.bund.de/certbund/index.htm.
51 Ennen, CERT-Bund, 35.
52 http://www.bmbf.de/pub/itkon_e.pdf.
53 http://www.tu-muenchen.de.
54 http://www.uni-hamburg.de.
55 http://www.fh-rhein-sieg.de.
56 http://www.eurubits.de.
57 http://www.uni-muenster.de/Jura.tkr/betaversion/oer/schwerpunkte/index.htm.