CIIP Country Surveys

Germany

The Country Survey of Germany 2004 was written with the help of Willi Stein, Dirk Reinermann, and Stefan Ritter, Federal Office for Information Security (BSI) as well as Thomas Beer, IABG.

Germany

Critical Sectors

The main assumption underlying CIIP in Germany is that both the government and society as a whole depend heavily on a secure infrastructure. Any elements of the infrastructure whose failure would result in supply shortages or other dramatic consequences for large parts of the population are defined as critical.[159] The following are the principal infrastructure sections defined as critical in Germany:

- Banking, Finance and Assurance,
- Emergency Services,
- Energy Supply (Electricity, Oil, Gas),
- Government and Public Administration (including Law Enforcement, Custom, and the Federal Armed Forces),
- Health Care (including Food and Water Supply),
- Telecommunications (Information and Communication Technologies),
- Transport.[160]

Generally, the awareness of the necessity to improve the safety and security of IT-dependent critical infrastructures, and the willingness to implement necessary measures, have slowly but steadily improved in Germany. The events of 11 September 2001 have added a certain sense of urgency, and international dialog has intensified.[161]

[159] Federal Office for Information Security (BSI). *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit "Kritische Infrastrukturen in Staat und Gesellschaft"* (January 2002), http://www.bsi.de/literat/faltbl/kritis.pdf and Federal Ministry of the Interior: http://www.bmi.bund.de/dokumente/Artikel/ix_93830.htm.

[160] http://www.bsi.bund.de/fachthem/kritis/kritis.htm.

[161] http://www.bmi.bund.de/dokumente/Artikel/ix_93830.htm.

Initiatives and Policy

In the past five to ten years, many activities directly or indirectly related to the issue of critical infrastructure protection have been undertaken. They emerged from inter-ministerial activities begun in 1997 at the initiative of the federal minister of the interior, motivated in part by the study produced by the *US President's Commission on Critical Infrastructure Protection*. Since then, co-ordination and reporting have taken place at the ministerial level on a regular basis.

The strategy to protect IT-dependent critical infrastructures became more distinct during 2002 and was materializing in 2003. Responsibility for overall coordination remains with the federal Ministry of the Interior, which will call in the *Federal Office for Information Security* (BSI), the *Federal Law Enforcement Agency* (BKA),[162] the *Federal Office for Civil Protection and Disaster Response* (BBK), and the governmental disaster relief organization *Technisches Hilfswerk* (THW).[163] Besides those agencies, the *Office of the Chancellor of the Federal Republic of Germany*,[164], the *Federal Ministry of Justice*, the *Federal Ministry of Economics and Labour*, and the *Ministry of Defense* are involved.

CIIP strategy and methodology will be developed in close cooperation with private infrastructure providers. Public private partnerships will be supported in response to the need for joint efforts to enable adequate protection at the governmental and private-sector levels. A national protection plan will be developed by the government; international cooperation (within the G8, the EU, etc., as well as on a bilateral basis) will be expanded.

AG KRITIS

Initiated by the report of the *President's Commission on 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.[165] It consisted of the ministerial representatives, a steering committee, and a permanent office at the *Federal Office for Information Security* (BSI).

[162] "Bundeskriminalamt": www.bka.de.

[163] http://www.thw.de/english/.

[164] Bundeskanzleramt.

[165] http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, 6.

The mandate of AG KRITIS was:[166]

- To describe possible threat scenarios for Germany,
- to conduct a vulnerability analysis of Germany's crucial sectors,
- 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.[167] 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 risks.[168]

Here is an overview of the main results:[169]

- 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 considered to be hacking and unauthorized access to data.

The creation of the *AG KRITIS* was an important basis for all further activities of public agencies in Germany. Its work is carried on, e.g., by the *Federal Office for Information Security* (BSI).[170]

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"[171] issued its fourth progress report, *Security and Protection in the Internet* ("Sicherheit und Schutz im Netz").[172] The commission contributed

[166] http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, and http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld003.htm.

[167] AG KRITIS. *Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS.* (Entwurfsversion 7.95, December 1999). 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. The report itself was never published.

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

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

[170] http://www.bsi.bund.de/fachthem/kritis/index.htm (in German) or (in English) http://www.bsi.bund.de/literat/faltbl/kritis_e.htm.

[171] The commission was established by the German Bundestag (federal parliament).

[172] http://www.bundestag.de.

to the collection and assessment of major risks linked to the new information technologies.[173]

Campaign for "Security in the Internet"

The campaign for "*Security in the Internet*"[174] is a combined initiative undertaken by the Ministry of the Interior, the Ministry of Economics and Labor, and of the Federal Office for Information Security.[175] 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.[176]

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 were to identify possible threats and to study countermeasures. By June 2002, the task force's publications included recommendations on protection against DDoS-attacks and information on 0190-dialers.[177] In 2003, a bill was introduced in both chambers of the parliament that will restrict the distribution of dialers.[178] This law will only permit dialers certified through the Regulatory Agency for Telecommunications and Posts[179] to operate.

Comprehensive Threat Analysis

In the fall of 2001, a comprehensive threat analysis for Germany was published by the *Ministry of the Interior.*[180] The IT section in this report is an

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

[174] http://www.sicherheit-im-internet.de.

[175] Bundesamt für Sicherheit in der Informationstechnik, BSI since 2000.

[176] http://www.sicherheit-im-internet.de/home/home.phtml, and Jantsch, Susanne. "Critical Infrastructure Protection in Germany". ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead. (Zurich, 8–10November,2001).http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld005.htm

[177] http://www.bsi.de/taskforce/index.htm.

[178] http://www.bundestag.de/presse/hib/2003/2003_117/03.html.

[179] http://www.regtp.de/en/index.html.

[180] Bundesministerium des Innern. *Zweiter Gefährdungsbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bev-*

attempt to answer the questions identified by the *AG KRITIS* study. Besides other threats, information security is defined as crucial for security of the German society and the success of its economy. It states that all measures, techniques, and instruments necessary for the protection of the vital infrastructure systems that rely on information technology are available. Rigorous application of those measures would eliminate a vast proportion of the threat, and it now remains only to implement those instruments. The risk management approach to information security proposed in this paper delegates the responsibility to the individual company providing information infrastructure services.

Infrastructure Analysis Studies

In mid-2002, the *Ministry of Interior* and the *Federal Office for Information Security* (BSI) commissioned a series of systematic studies of the CI/CII sectors. These studies have been completed and are currently used to support the establishment of a database for instant information access in case of an emergency related to information infrastructures, and for continuous situation evaluation. The database is currently in the making and may become the foundation for interdependency research in and between different CI/CII sectors. This database contains basic information on the infrastructure sector gained through interviews, workshops, and standardized questionnaire. The *Federal Office for Information Security* (BSI) has established its own department for the protection of critical infrastructures.[181]

International Outreach

An initiative between the *German Ministry of the Interior*[182] and the *US Department of Homeland Security*[183] at the ministerial level established the basis for future cooperation to enhance the protection of computer systems and networks. As a mid-term measure, a joint early-warning system should be created.[184] This bilateral initiative is a complement to the already ongoing counter-terrorism efforts. Additionally, a joint exercise will simulate an international IT-security violation event. Furthermore, both parties agreed

ölkerung bei Grosskatastrophen und im Verteidigungsfall. (Berlin, October 2001). http://www.bzs.bund.de/bzsinfo/broschur/zsforschung/gefahrenbericht_2.pdf.

[181] http://www.bsi.de/fachthem/kritis/index.htm.

[182] http://www.bmi.bund.de.

[183] http://www.dhs.gov.

[184] http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_92348.htm.

to foster regular consultations in international organizations in order to enhance multilateral cooperation.

Federal Office for Civil Protection and Disaster Response (BBK)

In order to facilitate cooperation between the different levels of public authority, a *Federal Office for Civil Protection and Disaster Response* (BBK)[185] will be established.[186] One of the main functions of this agency will be information-sharing and resource allocation in case of an emergency. A public relations and information website has already been established.[187] This *German Emergency Preparedness Information System* (deNIS) provides general information about organizations, emergency potentials, and web links on emergency precaution and preparedness.[188]

Moreover, decision-makers at the federal and state levels will be enabled to pool, process, and distribute resources in cases of wide-ranging catastrophes. This is an attempt to overcome the problems of the federal structure, where responsibility for civil protection lies with the federal authorities in cases of armed attack, and with the state-level authorities in cases of catastrophes. In particular, securing the energy and food supply and a smooth functioning of the information infrastructure are regarded as elementary.[189] In a further stage of development, a secure and classified system called *deNIS II* will be established.[190] Every international request for emergency support from Germany will be handled through *deNIS*.[191]

Kirchbach Report

The *Kirchbach Commission*, established after the devastating flood of 2002 in the Free State of Saxony, analyzed the overall structure of the *German Emergency Protection System*. Besides the focus on the flood disaster, it

[185] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

[186] http://www.bmi.bund.de/dokumente/Rede/ix_92444.htm.

[187] http://www.denis.bund.de.

[188] Zentralstelle für Zivilschutz. *Leistungspotenziale im Zivilschutz. Deutsches Notfallvorsorge-Informationssystem*. (Februar 2003). http://www.denis.bund.de/imperia/md/content/intern/1.pdf.

[189] http://www.bmi.bund.de/dokumente/Rede/ix_92444.htm.

[190] Zentralstelle für Zivilschutz. *Leistungspotenziale im Zivilschutz. Deutsches Notfallvorsorge-Informationssystem*. (Februar 2003). http://www.denis.bund.de/imperia/md/content/intern/1.pdf.

[191] http://www.bzs.bund.de/index2.html; Zentralstelle für Zivilschutz.

included a comprehensive analysis of existing facilities, and recommendations for future capacities to secure information and communications technology in cases of emergency.[192] This disaster and the conclusions of the Kirchbach report triggered a broad range of measures in a variety of ministries and agencies.

Guideline "Critical Infrastructure"

The *Federal Office for Information Security* (BSI) has published a security guideline on "Critical Infrastructure" that includes options going beyond basic IT security measures. Though the importance of such measures 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:[193]

- Define a business strategy for treatment of enterprise critical infrastructure,
- Assemble a stock of IT techniques and components in consideration of mutual dependencies,
- Define the criticality of processes and components,
- Verify and facilitate decision-making,
- Define appropriate measures and concepts.

Secure E-Government and BundOnline 2005

The *Federal Office for Information Security* (BSI) is supporting the e-Government initiative and the *BundOnline 2005*[194] program. The e-Government initiative aims at a consistent use of modern information and communications technology in order to make administrative processes more efficient and to facilitate an exchange between the business community, the public, and the administration.

The objective of the BundOnline 2005 initiative is to make about 400 federal administration services available online by 2005. Under this plan, the BSI was charged with developing the basic IT security component and

[192] *Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002.* (2nd ed. 2003). http://www.sachsen.de/de/bf/hochwasser/programme/download/Kirchbach_Bericht.pdf.

[193] Bundesamt für Sicherheit in der Informationstechnik (BSI). *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit "Kritische Infrastrukturen in Staat und Gesellschaft"*. (January 2002). http://www.bsi.de/literat/faltbl/kritis.pdf.

[194] http://www.bund.de/Service/english-.6118.htm.

with setting up the data security competence center. The BSI also published the e-Government manual covering all aspects of the subject of secure e-Government and presenting pragmatic approaches to their solution.[195]

Further Activities

Besides the above-mentioned activities, the *German Armed Forces* (Bundeswehr)[196] have initiated various steps within the field of CIIP. Most of these measures have concentrated on the vulnerabilities and response to potential information attacks, and on the active exploitation of information operations by the armed forces.

Currently, there are no comprehensive studies available to the public in Germany that analyze complex interdependencies between critical infrastructures. A survey for representatives of CI/CII business sectors was taken at an early stage of *AKSIS* (→ for more details see Part II) to systematically collect threats and expected damages to CII. The collected data was summarized in a matrix.[197] Some sector-specific studies have been published in the meantime, e.g., for the financial sector.[198]

Organizational Overview

An organizational analysis reveals that the professional lead for CIIP lies at the *Federal Ministry of the Interior* (BMI). The reason for the BMI's responsibility for CIIP is mainly historical. Out of the *Central Cipher Agency*,[199] which was tasked with computer security in 1986, an inter-ministerial board for security evolved with the acronym ISIT. The board was chaired by the Federal Ministry of the Interior. In 1989, the *Central Cipher Agency* was transformed into the *Central Authority for Security in Information Technology*, reflecting the increased significance of information systems for the functioning of the state and the economy. The development of a framework that would guarantee the safe and secure application of information

[195] http://www.bsi.de/fachthem/egov/index.htm and http://www.bund.de/Service/English/BundOnline-2005-Model-Projects-.6131.htm.

[196] http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.

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

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

technology was seen for the first time as a matter requiring urgent action. The main requirements of the framework were outlined as follows:

- Action to improve safety and security was urgently needed,
- Threat reduction is a task that lies within the responsibility of public authorities, and
- A federal agency should be in charge of risk analysis and the derivation of security concepts.

Therefore, a law was passed in 1990 establishing the *Federal Office for Information Security* (17.12. 1990, BGBl. I S. 2834 ff).[200] Germany's Minister of the Interior Otto Schily reorganized the agency in 2001, making it the central IT security service agency for all federal authorities.

The events of 11 September 2001 caused the government to make additional resources available under the heading of the "campaign against terrorism". Some of these additional funds were used to combat cyber-terrorism. Those funds were partly used for additional personnel in the *Federal Office for Information Security* (BSI).[201]

Public Agencies[202]

Federal Ministry of the Interior (BMI)

As the government agency responsible for ensuring Germany's internal security, the *Federal Ministry of the Interior* (BMI) is closely involved with CIP/CIIP.[203] This is where the relevant topics are dealt with and coordinated, such as physical protection within the context of civil protection and disaster response, threat prevention within the context of law enforcement, and all areas of IT and IT dependence. The authority in charge of IT-related issues with regard to CIP is Department IT 3 (Security of Information Systems) under the *Federal Ministry of the Interior's Chief Information Officer*.

The Federal Office for Information Security (BSI)

The Federal Office for Information Security (BSI), one of the agencies under the *Federal Ministry of the Interior*, plays an especially important role in CIP. The BSI deals with all areas related to security in cyberspace

[199] Zentralstelle für Chiffrierwesen.

[200] http://www.jura.uni-sb.de/BGBl/TEIL1/1990/19902834.1.HTML.

[201] Information provided by a representative of IABG.

[202] Information provided by a representative of BSI.

[203] http://www.bmi.bund.de/dokumente/Artikel/ix_93830.htm.

and takes preventive action in the form of analyzing IT weaknesses and developing protective measures, including the following:

- Internet security: analyses, concepts, advising;
- Management of the computer emergency response team (CERT) and virus center;
- Network security and cryptology, public key infrastructure (PKI) and biometrics;
- Critical infrastructure.

Federal Office for Civil Protection and Disaster Response (BBK)

In the area of physical security, the *Federal Office for Civil Protection and Disaster Response* (BBK) will be responsible for developing measures to improve physical protection.[204] Currently, this responsibility is discharged in cooperation with the *Federal Office of Administration* (BVA) under the heading of civil protection and disaster preparedness.

The Federal Bureau of Criminal Investigation (BKA)

The *Federal Bureau of Criminal Investigation* (BKA)[205] is responsible in the first instance for prosecuting crimes against the internal or external security of the Federal Republic of Germany and crimes involving damage to or the destruction of critical infrastructures that could result in a serious threat to life, health, or the functioning of society. Further, the BKA is the central agency for investigating crimes involving information and communications technology.

Federal Ministry of Economics and Labor (BMWA)

Since more than 90 per cent of Germany's critical infrastructure is in private hands, the *Federal Ministry of Economics and Labor* (BMWA)[206] also plays a role as its brief includes economic policy. With regard to the energy sector, one of the BMWA's tasks is developing the framework for securing the energy supply. According to Article 87f of the German constitution, the BMWA is also responsible for ensuring the availability of adequate telecommunications infrastructure and services.

[204] http://www.bmi.bund.de/Annex/de_25112/Gesetzentwurf_fuer_die_Einrichtung_des_Bundesamtes_fuer_Bevoelkerungsschutz_und_Katastrophenhilfe.pdf.

[205] http://www.bka.de.

[206] http://www.bmwa.bund.de.

Regulatory Authority for Telecommunications and Posts (RegTP)

As part of this effort, the *Regulatory Authority for Telecommunications and Posts* (RegTP), within the remit of the BMWA, is responsible for enforcing the relevant regulations to ensure the reliability and security of telecommunications networks. According to the amended *Telecommunications Act*, telecommunications companies are obliged to take appropriate technical and other measures to protect software-driven telecommunications and data processing systems against unauthorized access and disturbances that can cause significant disruptions of telecommunications networks.

Other ministries involved

The *Federal Ministry of Justice* (BMJ)[207] is responsible for relevant legislation, in particular ensuring that national laws comply with the cybercrime agreement of 23 November 2001.

The *Federal Ministry of Defense* (BMVg)[208] is involved in the context of its responsibility for national defense and for maintaining troop readiness and performance.

The *Federal Chancellery* plays a coordinating role at the ministerial level. Additional ministries are also involved in CIP in connection with particular areas of responsibility.

Responsibilities are also distributed among the agencies within the remit of the various ministries. The *Federal Intelligence Service* (BND) and the *Federal Office for the Protection of the Constitution* (BfV) provide important information regarding the threat situation and possible domestic targets.

Public Private Partnerships

The prevalent assumption in Germany is that cooperation between the public and the private sectors is the best strategy.[209] There are several cooperation initiatives in Germany between public and private actors related to CIIP.

[207] http://www.bmj.bund.de.

[208] http://www.bmvg.de.

[209] Jantsch, Susanne. "Critical Infrastructure Protection in Germany". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead*. (Zurich, 8–10 November 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld001.htm.

Initiative D21

The *Initiative D21*[210] is the largest public private partnership in Germany. This economic initiative also deals with information security. The *Initiative D21* is a neutral platform, independent of party allegiance and of individual industrial sectors. Its work is based on the assumption 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" with 226 participants; all sectors of industry (not only ICT providers), institutions, and politics are represented.[211] The Initiative D21 has formed 5 task forces and 17 subtask forces. In the task forces, important topics are discussed and agreements are implemented. Some of the main activities of the task force on *e-Government/Security and Trust on the Internet* include:

- Composition of a networked D21-CERT;
- The *Federal Ministry of the Interior* and D21 support middle class enterprises in the application of IT security criteria. The taskforce has developed a code of practice for IT security criteria and their application;
- Composition and completion of an administrative public key infrastructure according to the signature law;
- Promotion, standardization, and distribution of chip cards.[212]

Partnership for Secure Internet Business

The *Partnership for Secure Internet Business*[213] is supported by the *Ministry of Economics and Labor* and was founded in May 2000. The partnership was initiated by the ministry together with ten prominent trade associations and companies.[214] The main actors in the *Partnership for Secure Internet Business* are the *Ministry of Economics and Labor*, from the public sector, and up to 40 trade associations and companies from the private sector.

[210] http://www.initiatived21.de.

[211] Including 94 member companies, 33 sponsors, 59 supporters, and 43 advisory council members.

[212] http://www.initiatived21.de/english/index.php.

[213] Partnerschaft Sichere Internet-Wirtschaft.

[214] See http://www.sicherheit-im-internet.de.

Working Group on Infrastructure Protection (AKSIS)

Based on the assumption that the increasing dependability of society on CII means the associated risks must be studied in a comprehensive approach, the *Working Group on Infrastructure Protection* (AKSIS)[215] was established in 1999 on the initiative of the Center for Strategic Studies (ZES),[216] which belongs to the company IABG (*Industrieanlagen-Betriebsgesellschaft*).[217] The main purpose of AKSIS is to provide a forum for information exchange to analyze and 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 bringing together representatives of the public and private sectors (ministries, armed forces, police, telecommunication, energy, transport, banks, academia, etc.). Models for close cooperation between the government's CII protection initiative and AKSIS are currently being discussed.

Early Warning Approaches

CERT-Bund

The *Referat CERT-Bund* (CERT-Bund Unit) was established on 1 September 2001 at the *Federal Office for Information Security* (BSI). CERT-Bund is a central contact point charged with the security of data processors and networks of the federal public administration. CERT-Bund also offers some of its services to clients from the private sector. However, several services are only available to the federal administration (e.g., incident response).[218] CERT-Bund's main tasks include warning and information-sharing, data collection, analysis and processing of information, documentation and dissemination, sensitization of IT decisionmakers, and cooperation with existing CERTs.[219]

[215] Arbeitskreis zum Schutz von Infrastrukturen, AKSIS.

[216] Zentrum für Strategische Studien (ZES).

[217] See http://www.aksis.de, and http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld010.htm.

[218] 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.

[219] Ennen, CERT-Bund, 35.

Mcert

The study *CERT Infrastructure Germany*[220] was published in January 2002. It determined that a CERT addressing the needs of small and middle enterprises (SMEs) was required in addition to the existing CERTs (such as dCERT,[221] DFN-CERT,[222] S-CERT,[223] secu-CERT,[224] Telekom-CERT,[225] and CERT-Bund[226]). This gap was closed with the collaborative establishment of Mcert between the *Federal Ministry of Economics and Labour*, the *Ministry of the Interior*, and the non-profit organization BITKOM.[227] Some major IT players in Germany are already members and sponsors of this new body. Mcert addresses SMEs without in-house IT departments or security resources and provides them with a suitable warning service. Mcert was founded in May 2003, and services will be available beginning in December 2003 at www.mcert.de.

[220] See http://www.initiatived21.de.
[221] http://www.dcert.de/index_e.html.
[222] http://www.cert.dfn.de.
[223] http://www.s-cert.de.
[224] http://www.secunet.de.
[225] http://www.telekom.de/dtag/home/portal.
[226] http://www.bsi.de/certbund/index.htm.
[227] http://www.bitkom.org.

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