

Germany Country Report



About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>



Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Dan Cimpean, Immanuel Walpot and Johan Meire.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

GERMANY	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
NIS GOVERNANCE	12
OVERVIEW OF THE KEY STAKEHOLDERS	12
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	14
FOSTERING A PROACTIVE NIS COMMUNITY	18
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES	20
SECURITY INCIDENT MANAGEMENT	20
EMERGING NIS RISKS	20
RESILIENCE ASPECTS	21
PRIVACY AND TRUST	21
NIS AWARENESS AT THE COUNTRY LEVEL	23
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY	25
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	25
RELEVANT STATISTICS FOR THE COUNTRY	27
INTERNET ACCESS OF POPULATION AND ENTERPRISES	27
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	28
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	29
OTHER STATISTICS	30
APPENDIX	31
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	31
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	32
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	37
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	39
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	44
REFERENCES	46

Germany

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader on the following Network and Information Security (NIS) related topics:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
 - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
 - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
 - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
 - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
 - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

The German National Strategy for Critical Infrastructure Protection (CIP Strategy) of Germany was published already in June 2009¹ by the Federal Ministry of the Interior - *Bundesministerium des Innern* (BMI) and summarizes the objectives as well as the political-strategic approach as it is already common practice and pursued e.g. by the National Plan for Infrastructure Protection (NPSI) for the area of ICT.

For the implementation of the National Critical Infrastructure Protection Strategy, an extensive set of instruments is available in the form of:

- Programmes and plans (e.g. the National Plan for Information Infrastructure Protection (NPSI) and the related implementation plans as a strategic concept for IT infrastructure protection);
- Specific recommendations for action, like for instance:
 - the national Baseline Protection Concept as a basic guidance to physical critical infrastructure protection;
 - the Risk and Crisis Management Guide for Critical Infrastructure Operators, or
 - the national special protection concepts as detailed recommendations for action for the protection of individual CI sectors and sub-sectors);
- Standards, norms and regulations (e.g. the BSI Information Security Standards as a basic recommendation for action addressed to critical infrastructure operators.

In Germany, critical infrastructure protection is a task to be performed jointly by the government, companies and/or operators and also by civil society. The guiding principles regarding critical infrastructure protection are, in particular:

- Trusting co-operation between the state and business and industry at all levels; and
- The requirement for, and suitability and proportionality of, the measures taken and the use of resources made for increasing the level of protection.

As stated in the CIP Strategy, Germany acknowledges that for joint action to be successful, strategic guidelines are required which describe the basic philosophy, action and practices in all essential security-policy matters regarding critical infrastructure protection with reference to all relevant risks.

Early 2011, Germany published its new Federal Cyber Security Strategy for Germany². With the new German Cyber Security Strategy, the German Federal Government adapts measures to the current threats on the basis of the structures established by the CIP implementation plan and the implementation plan for the federal administration. The Federal Government will specifically focus on ten strategic areas:

1. Protection of critical information infrastructures: main priority of cyber-security, extends the cooperation established by the CIP implementation plan;

¹ http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

² http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Sicherheit/css_engl_download.pdf?__blob=publicationFile

2. Secure IT systems in Germany: joint initiatives involving groups from society will be organised in order to pool information and advice consistently. Availability of security tools will be enhanced;
3. Strengthening IT security in the public administration: a common, uniform and secure network infrastructure in the federal administration will be created, as a basis for electronic audio and data communication. Also, operational cooperation with the federal Länder will be further intensified by the IT planning council;
4. National Cyber Response Centre: will optimize operational cooperation between all state authorities and improve the coordination of protection and response measures for IT incidents;
5. National Cyber Security Council: intends to coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector. It will complement and interlink IT management at federal level, involving different ministries and federal offices;
6. Effective crime control also in cyberspace: involves the set up of joint institutions with industry and participation of competent law enforcement agencies for advisory. A major effort to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention will be made;
7. Effective coordinated action to ensure cyber security in Europe and worldwide: Germany's external cyber policy will be shaped so that German interests and ideas concerning cyber security are coordinated and pursued in international organisations;
8. Use of reliable and trustworthy information technology: Germany will continue and intensify research on IT security and on critical infrastructure protection. It will strengthen its technological sovereignty and economic capacity in the entire range of core strategic IT competences.
9. Personnel development in federal authorities: involves assessing whether additional staff and training is required in authorities in the interest of cyber security, as well as intensification of personnel exchange between federal authorities;
10. Tools to respond to cyber attacks: a coordinated and comprehensive set of tools to respond to cyber attacks must be created in cooperation with the competent state authorities.

The Federal Government aims at making a substantial contribution to a secure cyberspace, thus maintaining and promoting economic and social prosperity in Germany. Cyber security in Germany must be ensured at a level commensurate with the importance and protection required by interlinked information infrastructures, without hampering the opportunities and the utilization of the cyberspace. In this context the level of cyber security reached is the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity and confidentiality of data in cyberspace.

The regulatory framework

On November 25, 2010, the German data protection authorities responsible for the private sector (also known as the "Düsseldorfer Kreis") issued a resolution³ on the minimum requirements for the qualifications and independence of company data protection officers ("DPOs"). This initiative follows inspections carried out within companies that revealed a generally insufficient level of expertise among DPOs given data processing complexities and the requirements set by the Federal Data Protection Act. The DPAs recognize that a DPO's workload depends primarily on the size and number of data controllers the DPO supervises, industry-specific factors related to data processing and the level of protection required for the types of personal data being processed. Changes with respect to these factors frequently increase the burden on DPOs without a compensating increase in resources needed to ensure proper oversight.

BMI's 2010 Draft Law Regarding Data Protection on the Internet

On December 1st of December 2010, BMI issued a paper⁴ entitled "Data Protection on the Internet" which contains a draft law to protect against particularly serious violations of privacy rights online. This draft law covers the following relevant areas:

Regulation of Geo Data Services	<p>BMI's paper was developed in context of recent discussions regarding the regulation of geo data services. A draft data protection code for geo data services (the "Code"), prepared by businesses under the leadership of the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM), was also published on 1st of December 2010 and will be assessed by BMI.</p> <p>In its paper, BMI rejects the adoption of a specific law to regulate services such as Google Street View. BMI believes that, to the extent service providers implement sufficient technical and organizational measures to protect data, statutory regulation is not necessary.</p>
Regulation of the Publication of Personal Data Online	<p>BMI does, however, see a need for certain statutory rules to protect individuals from serious violations of their Persönlichkeitsrecht or "personality rights."</p> <p>In particular, the paper mentions Internet services such as facial recognition, search engine profiling and location-based services based on location information. According to the paper, the publication of comprehensive data of this nature, or data that describes an individual in a defamatory way, should be published online or made publicly available only if:</p> <ol style="list-style-type: none"> (1) there is a legal justification for the publication, (2) the individual in question consents to the publication, or (3) there is an overriding policy interest in publication of the data.
New Right to Claim Immaterial Damages	<p>For violations of this rule, the draft law suggests the implementation of a new right to claim "immaterial damages" to further deter violations. The penalty should equal the amount of the actual or expected profits by the company, thereby removing financial incentives to violate the law.</p> <p>BMI's objective is to promote self-regulation of Internet applications, and to avoid enacting laws that might stifle useful and necessary innovation. The Internet is viewed as a "public space" that should, in principle, be free of state restrictions.</p>

³ See:

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.pdf?__blob=publicationFile

⁴ See: *Datenschutz im Internet – Gesetzentwurf des BMI zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht* document available at: www.bmi.bund.de

BMWi Eckpunkte zur TKG-Novelle (2010)

This 2010 publication of the German Federal Ministry of Economics and Technology – *Bundesministerium für Wirtschaft und Technologie* (BMWi) provides an overview over the proposed changes to the telecommunication act TKG⁵, which are based on European Commission directive for a common regulatory framework for electronic communications networks and services (2009/140/EC). The proposed changes are currently under review of the authority of the BMWi.

This publication covers the following relevant areas of the EC directive:

Better Regulation	<ul style="list-style-type: none"> • Improvements of the conditions for infrastructure investments and competition as well as optimizing the regulatory framework: the new framework of the broadband expansion and investments of the next generation network (NGN) includes regulation principles regarding competitive encouragement of efficient investment and innovation of new and improved infrastructures. • Technology neutral design and flexibility of the bandwidth usage • Changes regarding broadcasting: includes the implementation of the European directives of digital television receiver (2002/22/EC) • Security and integrity of network and services: including an information and report system for security violation or the lost of integrity of public communication services. • General compliance with EC directives
Citizens' Rights	<ul style="list-style-type: none"> • Consumer rights: the telecommunication industry will be forced to provide information to the BNetzA (Bundesnetzagentur or Federal Network Agency) regarding e.g. price, network quality and end-user contract requirements. • Data protection and data security: increase the private data of the end-user.

BSI Act to Strengthen the Security of Federal Information Technology (2009)

On August 14th 2009 the Bundestag has passed the "Act to Strengthen the Security of Federal Information Technology". The law provides the details on the main tasks of the Federal Office for Information Security - *Bundesamt für Sicherheit in der Informations technik* (BSI).

It stipulates that BSI is the central reporting office for cooperation among federal authorities in matters related to the security of information technology (protection against malicious software and threats to federal communications technology, destruction of personal data, and warnings - security vulnerabilities). In addition, the act declares BSI as the national certification authority of the federal administration for IT security and acts as authority to issue statutory instruments.

eSignatures Legislation

The European Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures was transposed into German legislation through a series of acts:

- The 2001 law on the framework for electronic signatures and for amending other provisions – it regulates the necessary secure infrastructure for the use of electronic signatures;
- The Electronic signature ordinance ⁶of 16.11.2001, amended by Art. 2 law of 04.01.2005 - setting out standard requirements and responsibilities for certification authorities as well as minimum requirements for technical components used to create digital signatures;
- The first law amending ⁷the Signature Act (1. SigG) of 04.01.2005.

⁵ See: <http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/eckpunkte-tkg-novelle-2010,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf>

⁶ See more details at: <http://www.bundesnetzagentur.de/media/archive/893.pdf>

The German Federal Network Agency for Gas, Telecommunications, Post, and Railway – *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (BNetzA) is the competent authority on this topic. BNetzA supervises the certification service providers and in addition to its supervisory function is also an accreditation authority, recognises verification and confirmation agencies such as BSI.

BNetzA is also the root instance for accredited service providers.

eIdentification/eAuthentication⁸

The BMI i.e. the BSI Bundesamt für Sicherheit in der Informationstechnik and the BMG-Bund Bundesministerium für Gesundheit - The Federal Ministry of Health are the relevant authorities in Germany regarding the e-identity cards eID, ePass and eGK.

BMI – BSI Bundesamt für Sicherheit in der Informationstechnik

eID	<ul style="list-style-type: none"> • Electronic identity card • Introduced in November 1, 2010, equipped with a Radio Frequency Chip (RF chip) that includes personal data and a biometric photo of the eID owner • Fingerprints are not mandatory but could be included if the eID owner agrees • No central data storage of the eID information as covered by the act § 16 Datenschutzrechtliche Bestimmungen⁹ – <i>data protection regulation</i> even those were requested from the eID owner • The eID could be used for eID applications which are provided by eGovernment and eBusiness¹⁰ • Private service companies could request to read in specific information on the eID (e.g. online shopping). The authorization of the data is reviewed and is granted for a limited period of time¹¹ • The authorization is given through authentication certificates which are requested during the terminal authentication (TA)¹². The eID owner must enter the eID pin code before the encrypted data flows • The owner of the eID could request a signature function, which allows a digital signature. This signature has an official character and is implemented in the law of electronic signatures¹³
ePass	<ul style="list-style-type: none"> • Electronic passport¹⁴ • Introduced in November 1, 2005, equipped with a Radio Frequency Chip (RF chip) that includes personal data and a biometric photo of the ePass owner • Since November 1, 2007, the RF chip include mandatory and in line with the EC regulation nr. 2252/2004¹⁵ fingerprints of the ePass owner¹⁶

⁷ See the document at: http://bundesrecht.juris.de/siqg_2001/index.html

⁸ Source: Study on eID Interoperability for PEGS: <http://ec.europa.eu/idabc/servlets/Docb482.pdf?id=32522>

⁹ See:

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/PassVwV.pdf?__blob=publicationFile

¹⁰ See:

http://epractice.eu/en/factsheets/factsheet_all_chapters?filter=1&content_type=efactsheet_chapter&Countries=16&domain=10020&Factsheets_Topic=All&search=&op=Apply&form_build_id=form-bcfdd2855590fef21d1a4f9043b9c965

¹¹ See:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/Pressemappe_nPA/Innovationen_eID-Architektur_Deutschland.pdf?__blob=publicationFile

¹² See:

https://www.bsi.bund.de/cln_174/ContentBSI/Themen/ElekAusweise/Sicherheitsmechanismen/TA/sicherheitsmechanismenTA.html

¹³ See: http://www.gesetze-im-internet.de/siqg_2001/index.html

¹⁴ See: http://www.bamf.de/cln_118/DE/Infothek/FragenAntworten/eAufenthaltstitel/eAufenthaltstitel.html

¹⁵ See: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF>

	<ul style="list-style-type: none"> No central data storage of the ePass information exists, the act § 16 Datenschutzrechtliche Bestimmungen – data protection regulation does not allow the storage of fingerprints
EasyPASS	<ul style="list-style-type: none"> The BSI started the pilot-project EasyPass with the federal policy of the Frankfurt airport. The project consists of the (partly) automated border control process and the recognition of the biometric ePass photo. The process is not used by the BKA for dragnet investigations of the BKA or federal policy¹⁷. Core element is the biometric framework BioMiddle, which is the result of cooperation between the BSI and the secunet Security Networks AG.
eAT	<ul style="list-style-type: none"> Elektronische Aufenthaltstitel – <i>Electronic residence title</i> Currently under progress Includes biometric photo and two fingerprints of the owner of the eAT In line with the EC incentive 380/2008 and 1030/2002 In cooperation with the BMAF Bundesamt für Migration und Flüchtlinge – <i>Federal Office for Migration and Refugees</i> Excepted introduction date is September 01, 2011 Includes an online identification and qualified signature

Protection of the e-identities

The BSI provides several security mechanisms that are used for the eID, ePass, easyPass and eAT.

BAC Basic Access Control

- basic access control and prevents the reading of the RF chip from distance
- ePass

PACE Password Authenticated Connection Establishment

- access control and prevents the reading of the RF chip from distance
- ePass, eID

EAC Extended Access Control

- extended access control with different protocols
- are used together with the CA, BAC and PACE

CA Chip Authentication

- creation of a secured connection and identification of cloned RF chips (part of the EAC protocol)

TA Terminal Authentication

- Authentication of the RF chip reader (part of the EAC protocol)

PA Passive Authentication

- examination of the authenticity and rightness of the RF chip

PKI Public Key Infrastructure

- hierarchy of digital certificates

PKI CSCA Country Signing Certification Authority

- hierarchy of certificates to sign data in the ePass

PKI CVCA Country Verifying Certification Authority

- hierarchy of certificates to read data from the ePass

¹⁶ See:

https://www.bsi.bund.de/cln_174/ContentBSI/Themen/Elektausweise/Biometrie/BiometrieSeiteStart.html

¹⁷ See:

http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/Sicherheit/PasseundAusweise/EasyPass_FAQ.html?n=109628

Technical specification

The eID, ePass and the related eSign use the German Country Signing CA CSVA. In addition, all technical guidelines and security profiles in the context of the e-Identity, functional requirements for the technical realization of all processes (e.g. request process, security processes), technical guidelines for encryption in electronic identities, technical guidelines for the conformity of electronic identities and common criteria protection profile details are provided by the BSI.

BMG-Bund Bundesministerium für Gesundheit

The BFG covers the eGK and the related e-health initiative in the German health care sector.

eGK	<ul style="list-style-type: none"> • Elektronische Gesundheitskarte – electronic health card • The implementation of the eGK process is started on January 01, 2004 with the “basis rollout” which define that each stakeholder in the health sector (e.g. hospital and surgeries) must have a card reader and is planned to be finished in 2011 • The health insurances companies have to provide the eGK to their customers • Technical and security information are provided by the BSI¹⁸ • Secure storage of contractual and medical data, with respect to confidentiality, integrity and authenticity of these data Mutual Authentication between the eGK and a Health Professional Card (HPC) or a Security Module Card (SMC) • Mutual Authentication between the eGK and a security device (e. g. for online update of contract data in the card) E-health provide service in combination with the eGK for online health market • Authentication of the card using a private key and a X.509 certificate • Document content key decipherment using a private key • The legal framework is defined on the federal level in the Social Code V (§§ 290-291).
------------	--

Germany is also active member of the European project STORK¹⁹ (Secure idenTity acrOss borders linKed) that is aimed at enabling businesses, citizens and government employees to use their national electronic identities in any Member State.

The consortium members include national authorities, non profit organisations, private companies and academic partners from: Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, United Kingdom and Iceland.

¹⁸ See:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/PP0020_V2b_pdf.pdf?_blob=publicationFile

¹⁹ The STORK project consortium consists of 29 participants representing 13 Member States and Iceland. A full list of participants in the STORK project is available at www.eidstork.eu

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	<ul style="list-style-type: none"> • Federal Ministry of the Interior -Bundesministerium des Inneren (BMI) • Federal Ministry of Economics and Technology-Bundesministerium für Wirtschaft und Technologie (BMWi) • Federal Office for Information Security -Bundesamt für Sicherheit in der Informations technik (BSI) • BIT (Federal Office for Information Technology) • Federal Commissioner for Data Protection and Freedom of Information - Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit • Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen – Federal Network Agency for Gas, Telecommunications, Post, and Railway (BNetzA) • Federal Criminal Police Office - Bundeskriminalamt (BKA)
CERTs	<ul style="list-style-type: none"> • CERT-BUND • CERTBw • CERT Verbund – CERT Network • ESACERT • RUS-CERT • DFN-CERT • KIT-CERT • CERTCOM • ComCERT • CERT-VW • SAP CERT • Siemens CERT • SunCERT • Telekom-CERT • dCERT • PRE-CERT • S-CERT • secu-CERT • BFK • FSC-CERT
Industry Organisations	<ul style="list-style-type: none"> • BITKOM – German Association for Information Technology, Telecommunications, and New Media • eco (Verband der deutschen Internetwirtschaft e.V.) • VATM (Association of Telecommunications and Value-Added Service Providers) • VDE (Verband der Elektrotechnik, Elektronik und Informations-technik e.V.) • ZVEI (Zentralverband Elektrotechnik- und Elektronik-industrie e.V.) • IT Security Made in Germany (ITSMIG)
Academic Organisations	<ul style="list-style-type: none"> • University of Applied Sciences Gelsenkirchen, Faculty of Computer Sciences, Institut für Internet-Sicherheit if(is) – Institute for Internet-Security • University of Bamberg, Faculty of Information Systems and Applied Computer Sciences • University of Bonn, Institute of Computer Science IV, Communication and Distributed Systems • International School of IT Security (ISITS) • Technical University (TU) of Dresden, Faculty of Computer Science - Institute of Systems, Architecture - Chair of Operating Systems • University of Hildesheim, Institute of Computer Science • Leibniz University Hanover, Faculty of Law, Institute for Legal Informatics (IRI) • Leibniz University Hanover Research Initiative Safety & Security • TU Braunschweig - Institut für Betriebssysteme und Rechnerverbund • b-it (Bonn-Aachen International Center for Information Technology) • Universität Mannheim Lehrstuhl für Praktische Informatik 1 • Universität Karlsruhe, Fakultät für Informatik, Institut für Kryptographie und Sicherheit (IKS)/ Europäische Institut für Systemsicherheit (EISS) • LMU München Institut für Informatik • Fraunhofer Institute for Secure Information Technology (SIT) • Lehrstuhl Management der Informationssicherheit – Chair for IT-security Management of the University of Regensburg

- University of Wuppertal, Faculty D - Safety Engineering
- University of Freiburg, IMTEK - Institute for Microsystem Technology, Laboratory for Electrical Instrumentation
- Ruhr-University Bochum, Horst Grötz Institute for IT-Security (HGI)
- Institut für Sicherheit im E-Business (ISEB) – Institute for eBusiness Security
- Passau University, Institut für IT-Sicherheit und Sicherheitsrecht (ISL) – Institute of IT-Security and Security Law
- Technical University (TU) of Dortmund, Faculty of Computer Science, Information Systems and Security (ISSI)
- Technical University Hamburg-Harburg Information and Communication Systems "CIT - Communication and Information Technologies"
- University of Applied Science Ludwigschafen/Rhein Chair Information Management and Consulting "
- University of Applied Science Brandenburg Department of Business and Management
- Free University of Berlin - Institute of Computer Science Computer Systems and Telematics
- Technische Universität Berlin Fakultät IV für Elektrotechnik und Informatik
- Fraunhofer Institute for Secure Information Technology (SIT)
- Arbeitsgruppe Advanced Multimedia and Security, Fakultät für Informatik, Institut für Technische und Betriebliche Informationssysteme

Others

- Initiative D21
- TeleTrusT
- Klicksafe.de
- Gesellschaft für Informatik (GI) – Network for IT
- CAST
- ISACA Germany
- OWASP Germany
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
- vzbz (Verbraucher-zentrale Bundesverband e.V.)
- Stiftung Warentest
- Deutschland sicher imNetz e.V. (DsiN)

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"²⁰ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory²¹.

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

²⁰ The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

²¹ <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

New German Cyber Defense Center - "Nationale Cyber-Abwehrzentrum" (NCAZ)

At the end of 2010, the German Federal Ministry of Interior - Bundesministerium des Inneren (BMI) indicated that Germany will set up a new cyber defense center in response to growing threats. The new center will combine resources from various government agencies, including the federal police and foreign intelligence agency. It will also include participation from industry.

This initiative was taken in response to a surge in reported cyber attacks: for the first nine months of 2010, the German government recorded 1600 cyber attacks, compared with 900 cyber attacks in all of 2009²².

The German government decided on February 23, 2011 that the "Nationale Cyber-Abwehrzentrum" (NCAZ) – cyber-defense center will start its work on April 2011 in Bonn Mehlem and follows thereby the example laid out by NATO, the United States and Britain²³.

NCAZ will report to the Federal Office for Information Security (BSI) and cooperate directly with the Federal Office for the Protection of the Constitution (BfV) and the Federal Office of Civil Protection and Disaster Assistance (BBK). Cooperation in the National Cyber Response Centre will strictly observe the statutory tasks and powers of all authorities involved on the basis of cooperation agreements. The Federal Criminal Police Office (BKA), the Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND), the Bundeswehr and authorities supervising critical infrastructure operators all participate in this centre within the framework of their statutory tasks and powers²⁴.

The main task of the NCAZ is the transfer of information i.e. quick and close information sharing on weaknesses of IT products, vulnerabilities, forms of attacks and profiles of perpetrators and coordinated by a cyber security council under the responsibility of the Beauftragten der Bundesregierung für Informationstechnik (CIO Bund) – Federal Government Commissioner for Information Technology²⁵.

The Federal Chancellery and a State Secretary from each the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defense, the Federal Ministry for Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Education and Research and representatives of the federal Länder will participate.

²² Source: Deutsche Welle

²³ Source: http://www.bmi.bund.de/cln_183/SharedDocs/Kurzmeldungen/DE/2011/02/cyber_abwehr.html

²⁴ Source:

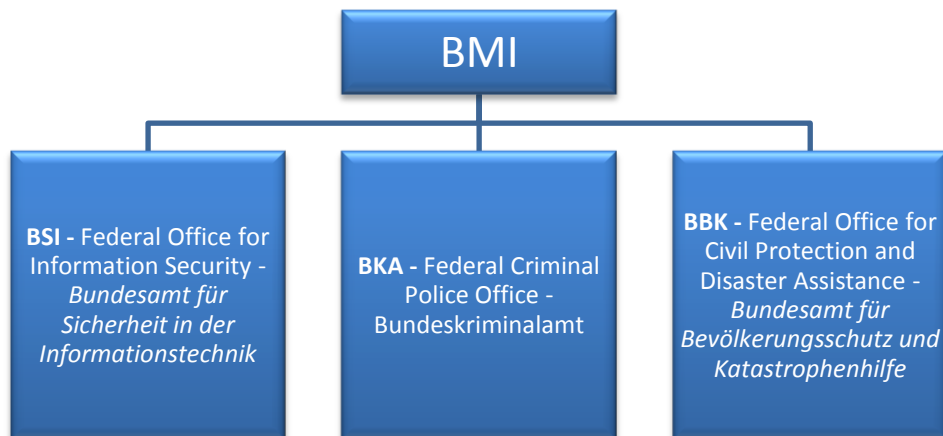
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile

²⁵ Source: http://www.cio.bund.de/cln_164/DE/IT-Sicherheit/it-sicherheit_node.html

Other co-operation via BMI and subordinated authorities

In Germany, the Federal Ministry of Interior - Bundesministerium des Inneren (BMI) is ultimate responsible in the fields of policy development and policy implementation.

It has a hierarchical relationship with several other authorities that work on the relevant NIS topics:

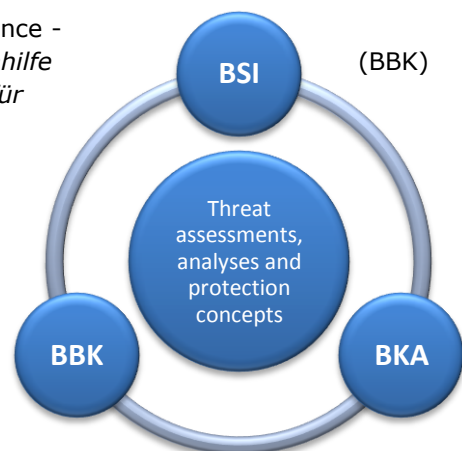


Threat assessments, analyses and protection concepts are developed by the key authorities supervised by BMI:

- Federal Office for Civil Protection and Disaster Assistance - *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*
- Federal Office for Information Security - *Bundesamt für Sicherheit in der Informationstechnik* (BSI)
- Federal Criminal Police Office – *Bundeskriminalamt* (BKA).

BBK closely cooperates with the BSI and BNetzA regarding security topics of the telecommunication- and information technology sector and related services. Studies²⁶ towards measurements and master plans are developed to protect the critical infrastructure.

BKA provides among other statistics on information and communication crime (i.e. the IuK report²⁷), preventive measurement against cyber crime and also it works closely with the BSI on cyber crime topics.



²⁶ See examples at: <http://www.bbk.bund.de>

²⁷ See an example of the IuK report issued by BKA at: http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

Co-operation via BSI

Cooperation and interaction between BSI, Datenschutz CERT and other organization e.g. IS-Bremen and Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) are performed on the IT Grundschatz Tag conference²⁸ covering current security topics.

1st IT Grundschatz-Tag 2010 (March 2010)	BSI, T-Systems and VMWare and the Networkers AG	<ul style="list-style-type: none"> Virtualization of IT-systems²⁹
2nd IT Grundschatz-Tag 2010 (September 2010)	BSI and HiSolutions AG	<ul style="list-style-type: none"> ISO 27001 certification topics³⁰
3rd IT Grundschatz-Tag 2010 (October 2010)	BSI and TÜV Informationstechnik GmbH (TÜViT)	<ul style="list-style-type: none"> Topics around IT security standards and IT-compliance³¹
4th IT Grundschatz-Tag 2010 (November 2010)	BSI and Fraunhofer SIT	<ul style="list-style-type: none"> Topics around security of Cloud Computing³²

The "IT-Grundschatz-Tag 2011" will take place on March 30th, 2011 in the office of IS-Bremen, the conference will be organized in co-operation by BSI, IS-Bremen, Wirtschaftsförderung Bremen GmbH, Universität Bremen, Niedersächsischer Verfassungsschutz and the Datenschutz Cert, under the slogan "Facebook, Cloud, Always-On, can we still feel safe?". See footnote³³.

In cooperation with the eco - Verband der deutschen Internetwirtschaft e.V. the BSI and BMI introduced a service portal towards the public on the thematic of botnets³⁴. The webpage www.botfrei.de provide general information on botnet and malware. In addition, further information and tools are provided to delete and prevent for botnet and malware infections.

BSI runs an information exchange with operators of CIIP (following the German CIP implementation plan). As the central IT security service provider, the BSI has several communication channels to other federal authorities, e.g. to IT security officers of the federal departments. A lot of this communication is unidirectional (recommendations or newsletters from the BSI), but there are also regular meetings or consultations.

²⁸ See: https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschatz/Aktuelles/aktuelles_node.html

²⁹ See more details at:

https://www.bsi.bund.de/cln_156/ContentBSI/Presse/Pressemitteilungen/Erster_IT_GrundschatzTag_180310.html

³⁰ See: https://www.bsi.bund.de/cln_174/ContentBSI/Aktuelles/Veranstaltungen/qstag/qstag_240910.html

³¹ See: https://www.bsi.bund.de/cln_174/ContentBSI/Aktuelles/Veranstaltungen/qstag/qstag_201010.html

³² See: https://www.bsi.bund.de/cln_174/ContentBSI/Aktuelles/Veranstaltungen/qstag/qstag_251110.html

³³ For more details on 1st IT Grundschatz Tag 2011 see:

https://www.bsi.bund.de/cln_156/ContentBSI/Aktuelles/Veranstaltungen/qstag/qstag_300311.html

³⁴ See: https://www.bsi.bund.de/ContentBSI/Presse/Kurzmitteilungen/Anti_Botnet_Initiative_150910.html

International co-operation

The German Federal Network Agency - *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (BNetzA) belongs to the scope of operation of the Federal Ministry of Economics (BMWi). In international relations, BNetzA partly acts on behalf of the Ministry, in particular as regards participation in European and international institutions and organisations. However, BNetzA has its own international functions on the basis of the Telecommunications Act or regulations of the European Communities.

An important area of international functions by its own right is the consolidation procedure according to art. 7 and 7a Framework Directive (2002/21/EG as amended by the Directive 2009/140/EC) in the telecommunications sector, which is a core element of the current regulatory framework.

Reporting duties mainly include collecting the reform package implementation reports for the telecommunications sector and the leased line report (comparable to the corresponding national papers in the benchmarking reports for the energy sector).

Cooperation with other regulating authorities mainly involves collaborating at operating and management level in European organisations, and bilaterally in a direct exchange of experiences with other national regulatory authorities such as the US Federal Communications Commission (FCC), and also Twinning and TAIEX projects.

In the field of market regulation of electronic communication networks and services, the BNetzA is a member of the Independent Regulators Group (IRG) and the new **Body of European Regulators for Electronic Communications (BEREC)**.

In the area of frequency regulation and technical regulation, the BNetzA takes part in organizations responsible for international frequency regulation and standardization.

These organizations include amongst others the European Conference of Postal and Telecommunications Administrations (CEPT), the Electronic Communications Committee, ECC), ITU Radio Communications (ITU-R), the International Telecommunication Union (ITU-T), the Telecommunication Development Sector of the ITU (ITU-D), and the European Telecommunications Standards Institute (ETSI) .

Co-operation and information exchange via German CERTs

The CERT-Bund, DFN Cert Services GmbH and Cert-Verbund have a co-operative or collaborative relationship, as it was also the case in 2009. The regular conferences like for example "Security in network systems" (May 2011) are based on corporation between the DFN-CERT, Telekom-CERT, RUS-CERT, CERT-Bund, Siemens CERT, Universität der Bundeswehr München, Leibniz-Rechenzentrum (LRZ), Dutch National Institute for Sub-atomic Physics and other key stakeholders³⁵.

The DFN-Cert work closely together with the BSI (e.g. Anti spam Strategies³⁶), Cert-NDS the Niedersächsische Ministerium für Inneres und Sport³⁷ (building a Länder owned computer

³⁵ See: <http://www.dfn-cert.de/veranstaltungen.html>

³⁶ See: https://www.bsi.bund.de/cae/servlet/contentblob/487422/publicationFile/31009/antispam_pdf.pdf

³⁷ See: http://www.iznnet-kom.niedersachsen.de/IT-Sicherheit/downloads/CERT-NDS_Abschlussbericht_2006-06-30_Druck.pdf

emergency-response teams), and also with the European Union (project eCSIRT³⁸ and project NoHA³⁹).

The German Federal Computer Emergency Response Team - *Computer Emergency Response Team für Bundesbehörden* (CERT-Bund) is part of Division 12 of BSI⁴⁰ and acts as a central contact point for solving computer and network security problems for federal institutions and is running various kinds of information exchanges: bidirectional with other CERTs (national / international) and authorities and unidirectional (advisories).

In "special IT security situations" the CERT-Bund provides a team of specialists that informs users immediately of threats and the counteractions to be taken. The secure platform activities of the BSI are also co-ordinated by Division 12 of BSI. To address these issues a project team "Secure Platforms" was established, that performs analyses and interacts with the industry in order to contribute to the security enhancements when utilising these new technologies.

Such solutions as they are specified by the industry consortium "Trusted Computing Group (TCG)" are in the centre of attention here.

CERT Verbund promotes cooperation among other CERTs in Germany (DFN CERT & CERT Bund).

Fostering a proactive NIS community

International co-operation facilitated via the Franco-German Council of Ministers

The 12th Franco-German Council of Ministers, held in February 2010 under the chairmanship of both President Nicolas Sarkozy and Chancellor Angela Merkel, defined the roadmap of the bilateral cooperation between Germany and France for the coming years.

Amongst the 80 measures accepted, France and Germany agreed to work together on strengthening the protective measures against cyber attacks and especially in the appropriate international forums⁴¹.

The German and French authorities in charge of information systems security, namely the Bundesamt für Sicherheit in der Informationstechnik (BSI) and the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) are long used to work together, yet the development of new threats requires the partnership to be further reinforced.

International co-operation via the European Government CERTs (EGC) group

The German Federal Computer Emergency Response Team (CERT-Bund) is amongst the active members⁴² of the European Government CERTs (EGC) group. EGC is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.

³⁸ See: <http://www.ecsirt.org/>

³⁹ See: <https://www.dfn-cert.de/kooperationen/noah.html>

⁴⁰ See an overview at:

https://www.bsi.bund.de/cln_183/ContentBSI/EN/TheBSI/Functions/Department1/department1.html

⁴¹ Source: BSI, see https://www.bsi.bund.de/cln_174/ContentBSI/EN/Press/pressreleases/BSI-ANSSI_050210.html

⁴² The members of the European Government CERTs group include: Austria - GovCERT.AT, Finland - CERT-FI, France - CERTA, Germany - CERT-Bund, Hungary - CERT-Hungary, Netherlands - GOVCERT.NL, Norway - NorCERT, Spain - CCN-CERT, Sweden - CERT-SE, Swiss - GovCERT.ch, United Kingdom - CSIRTUK, United Kingdom - GovCertUK; See more details at: <http://www.egc-group.org/>

To achieve this goal, the EGC group members:

- Jointly develop measures to deal with large-scale or regional network security incidents
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities
- Identify areas of specialist knowledge and expertise that could be shared within the group
- Identify areas of collaborative research and development on subjects of mutual interest
- Encourage formation of government CSIRTs in European countries
- Communicate common views with other initiatives and organizations.

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

Security incident management and reporting via BSI

At national level, BSI is the central reporting office for co-operation amongst German federal authorities in matters related to the security of information technology – this is clearly stated by the 2009 “Act to Strengthen the Security of Federal Information Technology”.

As part of its responsibilities to perform this task, BSI gathers and evaluates all information necessary to prevent threats to IT security, especially information concerning security vulnerabilities, malicious software, successful or attempted attacks on IT security and the means used to carry out such attacks. It also informs the German federal authorities about such information concerning them and of the facts of the matter ascertained.

In the case other German federal authorities become aware of information concerning security vulnerabilities, malicious software, successful or attempted attacks on IT security, which is significant for carrying out their tasks or for the IT security of other authorities, as of 1 January 2010 these federal authorities shall inform BSI of this information.

The relevant exception to this reporting requirement applies to information which may not be disclosed due to confidentiality regulations or agreements with third parties, and for information whose disclosure would conflict with the constitutional status of a member of the German Bundestag or of a constitutional body, or with the legally mandated independency of individual bodies.

BSI produces two kinds of reports: a restricted version with detailed information, and a public version with high level information and recommendations. Since 2009, there was no updated issue of the “Status report on IT security in Germany” – this report is published every two years.

Emerging NIS risks

BMI has issued a risk and crisis management guide⁴³ for companies and government authorities in order to help them identify risks, implement preventive measures and deal with crises effectively and efficiently. Critical infrastructures are understood in this BMI guide as the ones of central importance for Germany and its people whose failure or functional impairment would lead to severe supply bottlenecks, significant disruption of public security or other dramatic consequences.

The strategy for risk and crisis management presented in this guide consists of five phases:

- planning to set up a system of risk and crisis management,
- describing the basic aspects of risk analysis,
- implementing preventive measures,
- portraying aspects of robust crisis management and evaluating the system of risk and crisis management in an organization.

⁴³ See the BMI guide available at:

http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile

Resilience aspects

The key resilience aspects are addressed by the National Plan for Information Infrastructure Protection - *Nationaler Plan zum Schutz der Informationsinfrastrukturen* (NPSI) that is the German umbrella strategy for the protection of information infrastructures. The following strategic objectives are set out in the NPSI:

- Prevention: Protecting information infrastructures adequately.
- Preparedness: Responding effectively to IT security incidents.
- Sustainability: Enhancing German competence in IT security – setting international standards.

In line with this, key German stakeholders have developed several initiatives aimed at improving the overall national resilience of the information infrastructures. For example, **BSI** issued the Standard 100-4 – Business Continuity Management, a methodology for establishing and maintaining an agency-wide or company-wide internal business continuity management system. The methodology in this standard builds on the IT-Grundschutz methodology described in BSI Standard 100-2.

This standard⁴⁴ is aimed at emergency or business continuity managers, crisis team members, the people responsible for security, security officers, security experts, and security consultants who are familiar with managing emergencies and crises of technical and non-technical origin.

Another example of initiative aimed at improving the overall resilience level is represented by the guidance issued by **BITKOM** for datacenters. This guide⁴⁵ offers support for the planning and implementation of a data center, thus supplementing the existing standards and regulations which one can turn to for support.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented into the German law under the the German Federal Data Protection Act (the Bundesdatenschutzgesetz or “BDSG” or “DPA”).

In August 2010, the German government approved a draft law concerning special rules for employee data protection, originally proposed by BMI. The draft law would amend the German DPA by adding provisions that specifically address data protection in the employment context. The draft law covers nine key subject areas:

Employer Internet Searches	<ul style="list-style-type: none"> • Employers may use public information found through web searches, but may only use information from social networks if the networking platform is intended to present professional qualifications.
Medical Exams	<ul style="list-style-type: none"> • Medical assessments are permitted only as necessary to determine whether an employee can fulfil job requirements.
Automated Data Scanning	<ul style="list-style-type: none"> • Allowed in anonymised or pseudonymised form to detect criminal activity or other serious violations. If unauthorized activity is suspected, data may be

⁴⁴ See the BSI Standard 100-4 – Business Continuity Management document available at: https://www.bsi.bund.de/cae/servlet/contentblob/748954/publicationFile/41759/standard_100-4_e_pdf.pdf

⁴⁵ See: http://www.bitkom.org/files/documents/Reliable_Data_Centers_guideline.pdf

	associated with specific individuals. Employers must document the circumstances of the screening, and inform the relevant employee after the screening.
CCTV	<ul style="list-style-type: none"> Covert monitoring is prohibited. CCTV may be used only if employees receive proper notice, and only in particular areas or for certain reasons (e.g. quality control, security of facilities or entrance). No monitoring of locker rooms or similar locations is permitted.
Tracking	<ul style="list-style-type: none"> Collection of employee data via tracking systems (e.g. GPS) is only allowed during working hours, and only if the tracking serves to ensure employee safety or is used to coordinate the work force (e.g. transport companies). Covert tracking of employees is prohibited.
Biometric Data	<ul style="list-style-type: none"> Such data may be collected, processed or used only for authorization and authentication purposes when there are no prevailing employee protection considerations. Photographs of employees may be used for other purposes if the employee has provided consent.
Telephone, Internet and Email Monitoring	<ul style="list-style-type: none"> If a company allows employees to use telecommunications services for business purposes only, the draft law distinguishes between employer monitoring of phone calls versus monitoring email and Internet use. The draft law allows traffic and content data from email and Internet use to be collected, processed, and used, where necessary to: <ol style="list-style-type: none"> ensure the orderly functioning of the telecommunications network and services, promote data security, facilitate billing, and occasionally monitor performance and behaviour, but only if there is no overriding employee privacy interest.
Works Council Agreements	<ul style="list-style-type: none"> Companies still may enter into works council agreements, but such agreements must not compromise the level of protection provided by law.
Security Breach Notification	<ul style="list-style-type: none"> Employers must notify affected employees if it is determined that employee data has been unlawfully disclosed to a third party. In the event of a serious threat to the rights or protected interests of an employee, the employer must also notify the competent data protection authority.

There are 20 different German federal and regional supervisory authorities responsible for monitoring the implementation of data protection. The names, addresses and websites of these supervisory authorities are available at www.bundesdatenschutz.de (see "Aufsichtsbehörden für den nicht-öffentlichen Bereich").

Information security aspects in the German implementation of the Data Protection Directive

Public and private bodies processing personal data, either on their own behalf or on behalf of others (data processors), are obliged to take measures to ensure compliance with the provisions of the German DPA. The minimum requirements the data controller and the data processor must adhere to relate to: access control, transmission control, input control, availability control and the separation of data.

The German DPA does not currently contain an obligation to inform the competent authority or data subjects of a security breach – the amendments proposed in 2010 cover this topic (see prior paragraphs).

NIS awareness at the country level

Training and awareness programmes and initiatives under the CIP Implementation Plan of the National Plan for Information Infrastructure Protection

In order to increase awareness with respect to the importance of IT security, German operators of critical infrastructures have embarked on cross-sector cooperation with organisations of the public administrations, such as BSI, the Federal Criminal Police Office, the Federal Network Agency and the specialist ministries in charge. Joint exercises are held, such as the crisis management exercise across federal states, Länderübergreifende Krisenmanagement Exercise (LÜKEX).

Awareness actions on emerging topics – cloud computing security requirements

In September 2010, the German Federal Office for Information Security - Bundesamt für Sicherheit in der Informationstechnik (BSI) released a draft framework paper on information security issues related to cloud computing. The draft paper defines minimum security requirements for cloud solution service providers, and provides a basis for discussions between service providers and users. The paper addresses the following issues:

- The definition of cloud computing
- Service provider security management requirements
- ID and rights management
- Monitoring and security incident response
- Emergency management
- Security checks and verification
- Requirements for personnel
- Transparency
- Organizational requirements
- User control
- Portability of data and applications
- Interoperability
- Data protection and compliance
- Cloud certification
- Additional requirements for public cloud service providers that support cloud solutions for the German Federal Administration.

The BSI's goal is to work with stakeholders to develop appropriate security requirements that should be considered with respect to the provision of cloud services. A consultation was open on the above with service providers and users have, to review the paper and provide comments. The final version is expected for 2011.

Awareness actions targeting the consumers/citizens

The BSI für Bürger (BSI for the public) provides in cooperation with the BKA information about relevant NIS topics of interest for the citizens, such as how to prevent illegal traffic on website, general rules and laws around the Internet⁴⁶.

Also, on the Bürger-CERT platform, members of the public and responsible staff in small companies can receive information regarding viruses, worms, and other computer security risks.

⁴⁶ See: https://www.bsi-fuer-buerger.de/cln_030/ContentBSIFB/SicherheitImNetz/RechtImInternet/recht.html

Awareness actions towards spam and/or malware

As in the past years, Germany organised in 2010 the Anti Spam Summit⁴⁷, with the generic theme "National Anti Botnet Initiatives Worldwide". This 8th edition of the German Anti Spam Summit focused on a wide range and number of topics related to spam and botnets. A large number of international experts presented the latest development and share their experience on fighting spam and/or botnets. ENISA was also actively involved⁴⁸ in this German anti spam event.

The "Internet security for SMEs" initiative

To promote Internet security for small and medium-sized businesses (i.e. SMEs), BMWi and BMI have launched the initiative "Internet security for SMEs" (German: Mittelstand sicher im Internet). This initiative⁴⁹ links the issues of Internet security and SME support, because the secure use of information technology and the Internet can improve the competitiveness of all small and medium-sized companies.

Here, small and medium-sized companies can find easy-to-understand information on simple ways to protect themselves against electronic viruses, worms and external attacks without the need for specialist technical knowledge. Targeted information addresses the problems of specific business sectors and offers corresponding solutions: after all, the security needs of automobile supply companies are different from those of retailers.

The initiative also offers practical solutions to address anticipated future needs, according to sector, the number of computers in use and the area of application. Companies can download informational brochures on priority issues that enable them to take the necessary steps with their IT staff. Detailed company examples illustrate what the benefits of IT security are, how it can be implemented in practice, and what business opportunities it can open up.

The initiative works in close collaboration with industry associations and also enjoys the support of key sponsors. In addition, BSI provides the initiative with expert advice.

Others

No International Conference on IT Security Incident Management & IT Forensics was organised in 2010 in Germany (the 5th one took place in 2009). The 6th edition is planned for March 2011.

⁴⁷ See the detailed agenda at: http://www.eco.de/dokumente/eco-AntiSpam_Agenda_web.pdf

⁴⁸ See more details on ENISA involvement in the 8th German Anti Spam Summit at: <http://www.enisa.europa.eu/events/ee/eco10>

⁴⁹ The website www.mittelstand-sicher-im-internet.de is the initiative's central information platform.

Country-specific activities for identifying and promoting economically efficient approaches to information security

On its web site, BMI indicates its focus on assessing the impact of regulation as a crucial action for better legislation. BMI acknowledges that an informative assessment of the impact of regulation is increasingly important and that is key for specialists and stakeholders to be involved from an early stage in examining alternatives and their consequences in a process of consultation.

The aim is to improve the quality and reduce the quantity of government regulation by using a process of consultation in which specialists and stakeholders examine regulatory alternatives. This process both increases the democratic participation of citizens and gives lawmakers a firmer foundation for their decisions. For this, BMI also published or helped produce the following tools:

- Guidelines for Regulatory Impact Assessment;
- Manual of Regulatory Impact Assessment, Baden-Baden: Böhret/Konzendorf (commissioned by the Federal Ministry of the Interior and the Interior Ministry of the state of Baden-Württemberg)
- Regulatory Impact Assessment: Testing in Practice
- Regulatory Impact Assessment: Help for Practitioners

Since December 2008, the Federal Academy of Public Administration (BAköV) has also offered a seminar on regulatory impact assessment. The aim is to establish regulatory impact assessment as an integral part of the legislative process and to continually improve its quality. However, no specific impact assessment results are available on the web site of BMI with respect to NIS-related initiatives.

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

Critical infrastructure protection in Germany

In Germany, within the area of critical infrastructure protection⁵⁰, BSI focuses particularly on IT threats, that is on Critical Information Infrastructure Protection (CIIP). The BSI applies the term "information infrastructure" both to the ICT sector per se (the large IT and telecommunications networks including their components and operators) and to the ICT-based infrastructures of other sectors.

With the National Plan for Information Infrastructure Protection – *Nationaler Plan zum Schutz der Informationsinfrastrukturen* (NPSI), the Federal Cabinet adopted, in 2005, the German umbrella strategy for the protection of information infrastructures. Three strategic objectives are set out in the NPSI:

- Prevention: Protecting information infrastructures adequately.
- Preparedness: Responding effectively to IT security incidents.
- Sustainability: Enhancing German competence in IT security – setting international standards.

In order to further substantiate the umbrella strategy, implementation plans have been drawn up and adopted thereafter.

⁵⁰ Source BSI: https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html

CIP Implementation Plan of the National Plan for Information Infrastructure

Protection⁵¹: about 30 critical infrastructure operators or related business associations joined forces with public authority representatives, most notably from the BMI and BSI, and developed the CIP Implementation Plan - *Umsetzungsplan KRITIS* (UP KRITIS) which was adopted already since 2007 together with the Implementation Plan for the German Federal Administration.

Experts from private and public sector critical infrastructures were invited to have an input in the development of the CIP Implementation Plan. Jointly devised over a series of workshops and additional working group meetings, the CIP Implementation Plan recommends a series of measures intended to further improve the protection of information infrastructures in the German CIP sectors.

The CIP Implementation Plan is the foundation for a long-term partnership between the German public and private sectors. The companies involved have voluntarily adopted the security measures outlined in the CIP Implementation Plan as their own standard, and are now working collaboratively on overarching measures. Four working groups with chairpersons from the private sector are supporting the adoption of the recommendations given in the CIP Implementation Plan:

- WG 1 "Emergency and crisis exercises"
- WG 2 "Crisis response and management"
- WG 3 "Maintaining critical infrastructure services"
- WG 4 "National and international cooperation".

Particular emphasis is on intensifying cross-sector communication. It is regarded by those involved in the CIP Implementation Plan as a key component in improving IT security in critical infrastructures. The required levels of availability will be guaranteed, even during IT crises, with the development and extension of a network of single points of contact as central communication nodes. The IT situation centre at the BIS is part of this communication network and – operated by the Federal Computer Emergency Response Team (CERT-Bund) – regularly issues a national IT situation picture in its capacity as the central analysis point for the evaluation of information on IT incidents.

Also adopted in 2007, the **Implementation Plan for the Federal Administration** – *Umsetzungsplan Bund* (UP Bund) sets out clear guidelines for the implementation of the NPSI in the German Federal Administration. Each ministry is responsible for the implementation in its respective realm.

⁵¹ Full document available at:

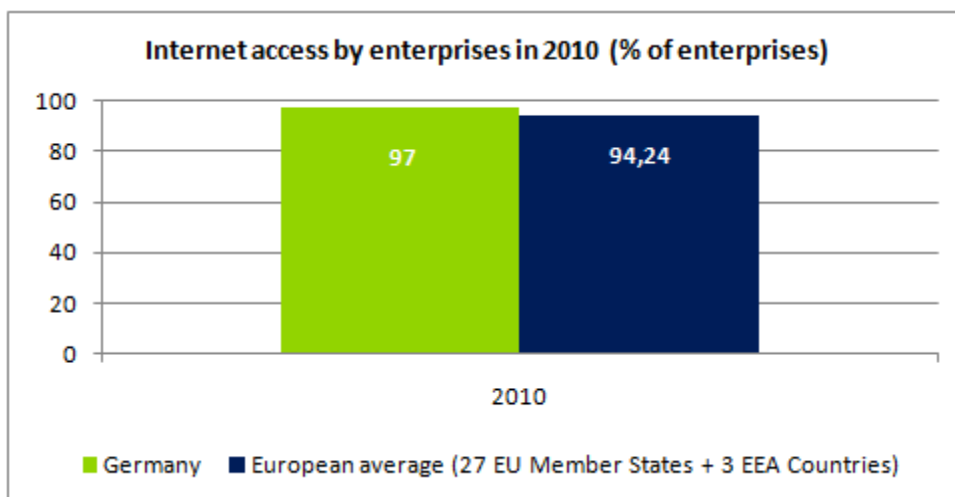
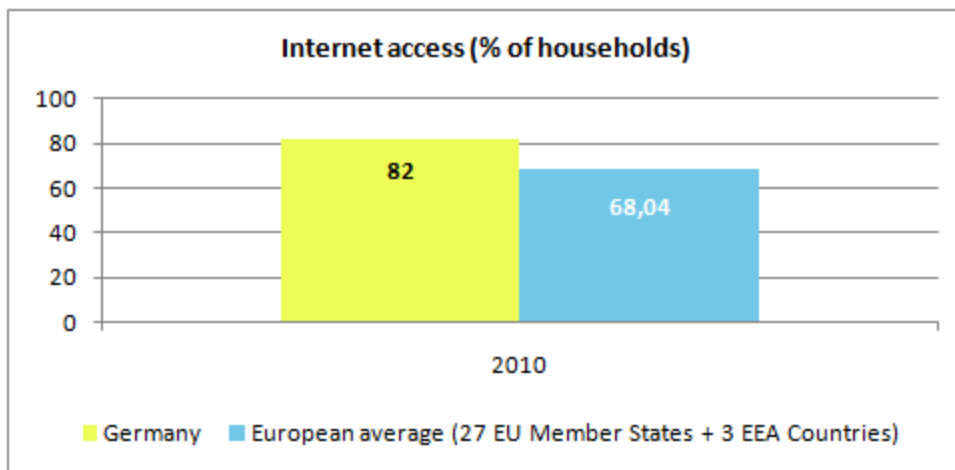
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/UP_KRITIS_en_final.pdf?__blob=publicationFile

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Germany, a series of relevant statistics are included in this section. Some of them indicate that the information society in Germany is at a relatively advanced stage of development in comparison with the European average, while others show interesting trends.

Internet access of population and enterprises

The following graphs, based on Eurostat information, provide an overview of the situation⁵² of Internet access in German for enterprises and respectively households, relative to the European average.

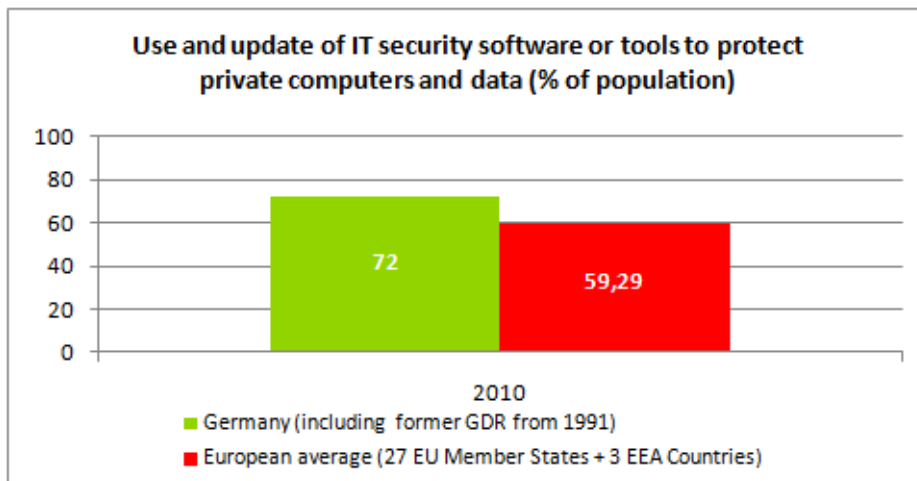
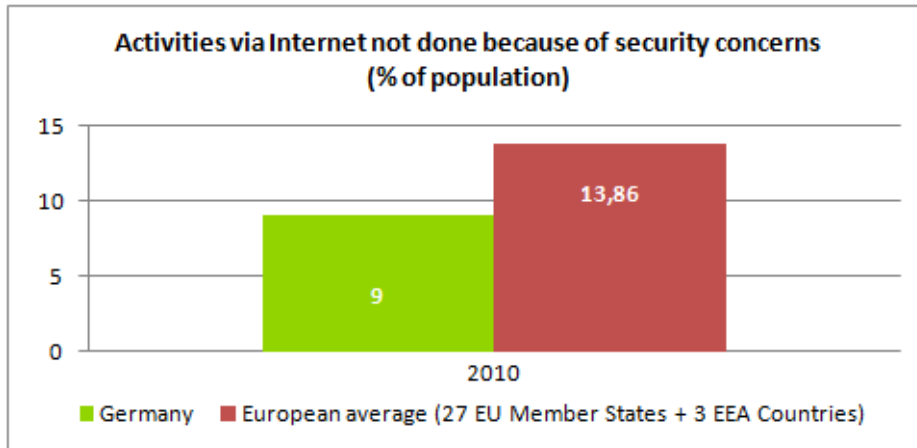


Based on 2010 data, the statistics indicate that the enterprises in Germany have about the same level of Internet access as the European average, while for the households, the Internet access percentage is above the European average.

⁵² Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

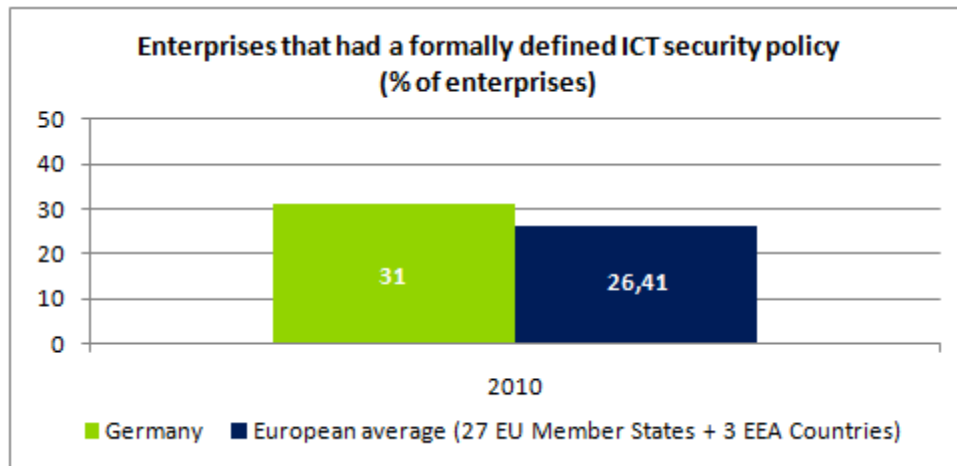
The percentage of population in Germany that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is lower than the European average:



Meanwhile, it appears that the use of security software or tools to protect private computers and data is above the European average, indicating a higher level of overall awareness on the need of using such security measures.

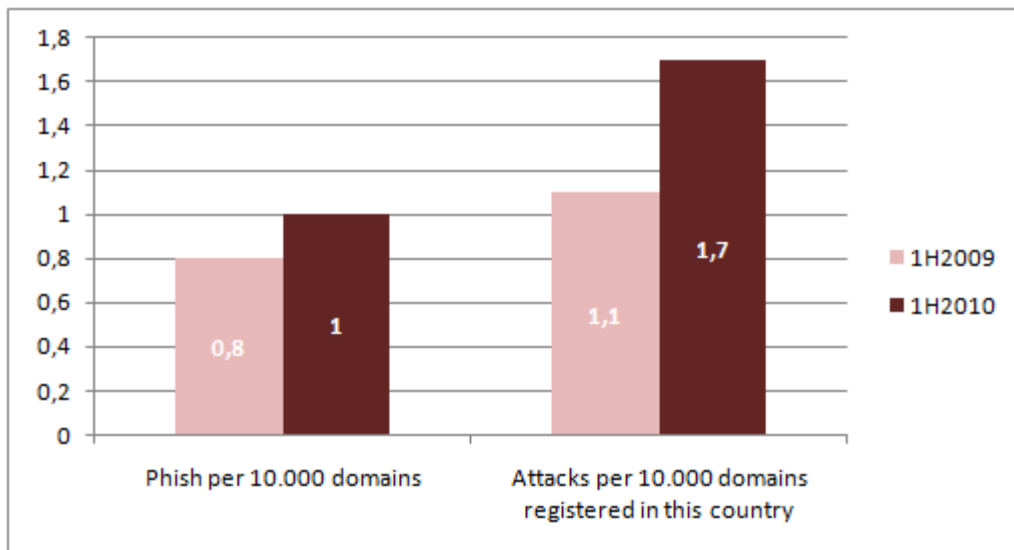
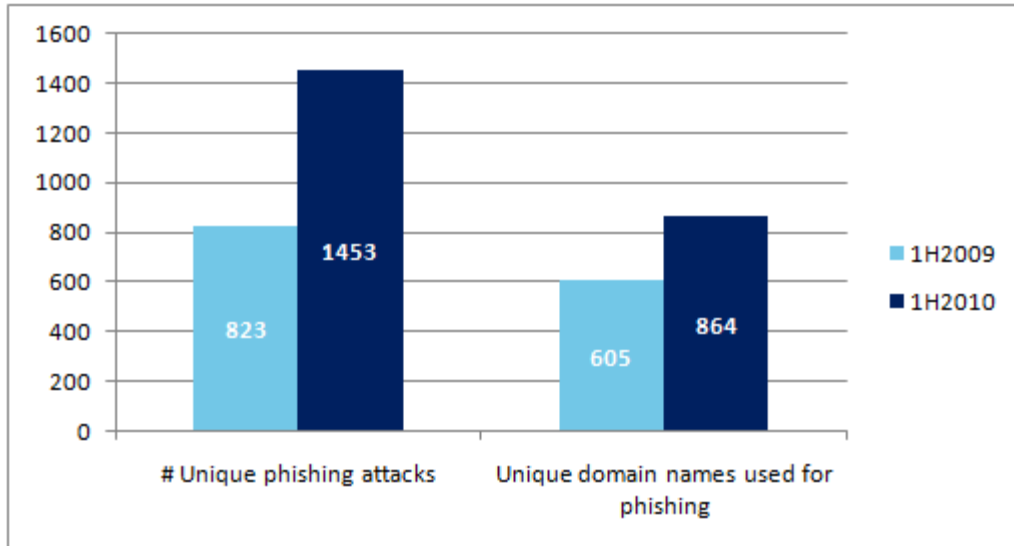
Statistics on use of Internet by enterprises and related security aspects

Enterprises in Germany have a formally defined ICT security policy, at a percentage level that is higher than their European peers. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Germany was mentioned in the global report⁵³ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



The KES (Zeitschrift für Informations-Sicherheit – German newspaper for information and security), Microsoft, the BSI and several other sponsors perform since 2004 every two years IT related security studies. The KES study⁵⁴ of October 2010 included e.g. structural changes in the IT environment, number of CSO/CISO commissaries, IT budgeted evaluation, Malware studies, data-leakage/loss prevention (DLP), criminal statistics, study about security awareness.

⁵³ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

⁵⁴ See: <http://www.kes.info/archiv/material/studie2010/index.html>

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Federal Ministry of the Interior - Bundesministerium des Inneren (BMI)	<p>Its most important responsibility is guaranteeing Germany's internal security. The Ministry is also responsible for the comprehensive use of information technology to modernize the public administration, and the security of information technology:</p> <ul style="list-style-type: none"> • Information security policy. • Protection of critical information infrastructures. • E-government. • Travel documents and biometrics. 	www.bmi.bund.de
2. Federal Ministry of Economics and Technology- Bundesministerium für Wirtschaft und Technologie (BMWi)	<p>The Ministry is responsible for developing economic policy.</p> <ul style="list-style-type: none"> • Economic policy including ICT policy. • Telecommunications security policy. • Contingency planning policy for telecommunications networks and services. 	www.bmwi.bund.de
3. Federal Office for Information Security - Bundesamt für Sicherheit in der Informations technik (BSI)	<p>BSI is the central IT security service provider for the German federal government. Furthermore it advises manufacturers, distributors and users of information technology.</p> <p>BSI provides services for instance in the fields of:</p> <ul style="list-style-type: none"> • IT security management • Internet security • Security in mobile devices • Network security • Certification of products. • Prevent threats to the security of federal information technology <p>Other tasks / capacities assigned to the BSI are:</p> <ul style="list-style-type: none"> • Protection of federal communication systems; • publishing of binding minimum standards for information assurance; • issuance of vulnerability warnings to relevant parties; • central IT incident reporting office for the federal administration; • central evaluation, certification and accreditation office. 	www.bsi.bund.de www.bsi-fuer-buerger.de
4. BIT (Federal Office for Information Technology)	<p>Federal administration for central IT services provides Central IT services to the federal administration.</p>	www.bit.bund.de
5. Federal Commissioner for Data Protection and Freedom of Information - Der Bundesbeauftragte für den Datenschutz und die	<p>The Federal Commissioner for Data Protection and Freedom of Information is the Supervisory authority on data protection, for instance concerning:</p> <ul style="list-style-type: none"> • Communication services • Technological data protection • Protection for telecommunication and postal 	www.bfdi.bund.de

National authorities	Role and responsibilities	Website
Informationsfreiheit	services providers <ul style="list-style-type: none"> Health and social security. 	
6. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen – Federal Network Agency for Gas, Telecommunications, Post, and Railway.	The Federal Network Agency is an authority within the scope of business of the Federal Ministry of Economics and Technology. Its task is to provide, by liberalisation and deregulation, for the further development of the electricity, gas, telecommunications, postal and railway markets.	www.bundesnetzagentur.de
7. Federal Criminal Police Office - Bundeskriminalamt (BKA)	The Federal Criminal Police Office (. BK) is assigned the nationwide fight against criminal acts, amongst which NIS crime.	www.bka.de

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
8. CERT-BUND	<p>CERT-BUND is the federal government institution and governmental network backbone.</p> <p>The CERT-Bund is the central advice institution for preventive and reactive measures regarding security and availability incidents of computer systems. CERT-Bund services are in the first instance for IT management of federal authorities.</p> <p>This is done by Computer Security Incident Prevention and Computer Security Incident Response including among other:</p> <ul style="list-style-type: none"> Analysis of incident reports Management of a warn and information service Recommend reactive measurements for damage limitation or correction Documentation and statistics Development of research methods and tools Publishing i.e. WID warn and information service (www.cert-bund.de) <p><i>FIRST member, TI listed</i></p>	www.bsi.bund.de/cln_174/DE/Themen/CERTBund/certbund_node.html
9. CERTBw	<p>CERTBw is the CERT of the Ministry of Defence.</p> <p><i>FIRST member, TI listed</i></p>	www.bundeswehr.de
10. CERT Verbund – CERT Network	The German national CERT-Verbund is an alliance of German security and emergency response teams. The CERT-Verbund provides the German teams with a framework for co-operation and information sharing. Besides this, all the single teams stay autonomous in their responsibility for	www.cert-verbund.de

⁵⁵ <http://www.first.org/members/teams/>

⁵⁶ <http://www.trusted-introducer.nl/>

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST⁵⁵ member • TI⁵⁶ listed <p>their respective constituency.</p> <p>CERT-Verbund has the following overall goals:</p> <ul style="list-style-type: none"> • Protection of the national IT-networks • Immediate joint reaction to security incidents <p>CERT-Verbund looks after the following projects:</p> <ul style="list-style-type: none"> • DAF - Deutsches Advisory Format (German advisory format) • SIRIOS – System for Incident Response in Operational Security 	
11. ESACERT	<p>The goal of the ESACERT is to provide Information Systems Security Solutions for the European Space Agency. As such, the mission of the ESACERT is to become ESA's co-ordination, service and competence center for all Information Systems Security related matters.</p> <p>The ESACERT:</p> <ul style="list-style-type: none"> • collaborates with ESA's partner organizations and other CERT/CSIRT entities to support these activities. • supports the development of ESA's Information Systems Security policies. • works out and maintain several Information Systems Security procedures for the ESA Information Systems user community. • provides several value-added Information Systems Security services. Examples of these services can be, but are not limited to: <ul style="list-style-type: none"> • Intrusion Detection • Incident handling • Alerts and Announcements • Collaboration and Coordination • Vulnerability and Artifact Analysis and Response • System Scanning and Certification • Training and Awareness • Consulting and Risk Analysis, etc. <p>The ESACERT intends to implement all these Procedures and Services over time as resources become available. <i>FIRST member, TI listed.</i></p>	www.esacert.esa.int
12. RUS-CERT	<p>The RUS-CERT offers various services to members of the University on the topic of security:</p> <ul style="list-style-type: none"> • Services of the RUS-CERT • Perimeter Filter (University of firewall) • Service attack (scan service) • Security of network connected computers • Forgot your service • Checking for weak passwords • Software Projects • various projects within the work of the RUS-CERT have arisen • Archive (mailing lists) • Archives of various mailing lists around the 	http://cert.uni-stuttgart.de

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST⁵⁵ member • TI⁵⁶ listed <p>work of the RUS-CERT</p> <ul style="list-style-type: none"> • The 5 recent news • Integration of the 5 latest news in your website • The RUS-CERT Sidebar • RUS-CERT reports in the Mozilla sidebar • Mailing Lists • List of all the mailing lists of the RUS-CERT • Statistics <p>The RUS-CERT offers services for members of the University of Stuttgart. <i>FIRST member, TI listed</i></p>	
13. DFN-CERT	The DFN-CERT is the CSIRT for the German Research Network 'Deutsches Forschungsnetz' (DFN). Its constituency comprises all member institutions of the DFN. <i>FIRST member, TI listed</i>	www.dfn-cert.de
14. KIT-CERT	KIT-CERT is the Computer Emergency Response Team of the Karlsruhe Institute of Technology. The clientele of the KIT-CERT are all students and staff of the KIT. The team can be reached via the contact details published on the site. <i>FIRST member, TI listed</i>	www.cert.kit.edu
15. CERTCOM	<p>The CERTCOM AG is the leading manufacturer of products and services in the area of Active Business IT security. It operates the first commercial CERT, which is open to any company that manufacturers. The CERTCOM AG employees transfer the success parameters of global CERT structures in standardized and above all affordable Active Business IT security products.</p> <p>They provide companies with standardized IT security structures of globally active corporations. The services and products help to realize active safety at all levels and to achieve the best possible result. <i>TI listed</i></p>	www.certcom.de
16. ComCERT	The CERT of the Commerzbank. <i>FIRST member, TI listed</i>	www.commerzbank.com
17. CERT-VW	The CERT of the Volkswagen. <i>FIRST member, TI listed</i>	www.volkswagen.de
18. SAP CERT	The CERT of SAP. <i>FIRST member, TI listed</i>	www.sap.com
19. Siemens CERT	<p>The Siemens Computer Emergency Response Team (CERT) has been protecting internal IT infrastructure and supporting secure product development since 1998. It is established as an independent auditor and trustworthy partner to respond to security incidents, develop preventive measures and assess information security.</p> <p>With these activities, Siemens CERT helps its customers worldwide to achieve the necessary security level for effective protection against hacker attacks. With its research activities, Siemens CERT proactively investigates future technological challenges and develops practical solutions for its customers. <i>FIRST member, TI</i></p>	https://w1.siemens.com/innovation/en/about_fande/corp_technology/research_technologies/technology_divisions/info_comm/cert.htm

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST⁵⁵ member TI⁵⁶ listed 	
	<i>listed</i>	
20. SunCERT	The CERT of Sun Microsystems FIRST member, TI listed	www.sun.com
21. Telekom-CERT	The CERT of Telekom. FIRST member, TI listed	www.telekom.de
22. dCERT	T-Systems offers its established service "dCERT". The aim of dCERT is to provide its customers with up-to-date high quality security information. Experienced IT-security experts compose daily information for security of computers and networks. The analyzed information and countermeasures are distributed electronically per e-mail. Monthly digests provide an overview. The moderated forum allows the discussion and the exchange of practices among the dCERT-partners, dCERT-members and the experts of T-Systems. dCERT also organizes analyst days and Security seminars. <i>FIRST member, TI listed</i>	www.dcert.de
23. PRE-CERT	PRESECURE is a member of FIRST, and TI accredited Level 2 team. Given the increasing threats on the Internet grows, the importance of incident response. Only through the creation of an optimal security architecture, a company can protect against attacks. Technical solutions are only one aspect. As a good computer emergency response team, PRESECURE can effectively handle attacks. <i>FIRST member, TI listed</i>	www.pre-secure.de
24. S-CERT	In collaboration with its member institutes, S-CERT has declared the following as its ongoing mission: <ul style="list-style-type: none"> Damage Prevention Consistent reduction of IT security risk through comprehensive threat recognition Facilitation of an efficient, economical and professional computer emergency response team Reaction and Emergency Aid Competent and easily comprehensible handling of security issues Reliable handling and confinement of security incidents Future-proofing: preserving appropriate security levels Continual assessment and restatement of the quality level of security measures Development of IT security skills The cultivation of a strong awareness of IT security issues. <i>FIRST member, TI listed</i>	www.s-cert.de
25. secu-CERT	IT security and its innovative application is the core competency of secunet Security Networks AG. Outstanding technological know-how is reflected in their consulting services and adapted products. They guarantee customer orientation and an understanding of the industry with our four business areas Automotive, Business Security, Government and High Security.	www.secunet.com

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST⁵⁵ member • TI⁵⁶ listed 	
	<i>FIRST member, TI listed</i>	
26. BFK	<p>BFK edv-consulting GmbH originates from the MicroBIT Virus Center of the computer center at the University of Karlsruhe, whose outstanding research and publications about computer viruses and sabotage led to an intensive demand in industry and public institutions.</p> <p>The increasing need of consultancy services quickly exceeded the capacities of the scholastic structured MicroBIT Virus Center. At the end of 1989 BFK was founded and turned into an equivalent of an LLC in April 1990.</p> <p>BFK edv-consulting GmbH developed its businesses from pure anti-virus-consulting to comprehensive IT-security consulting, due to the growing complexity of the topics. Their main competences are:</p> <ul style="list-style-type: none"> • preventive security consulting (security concepts, penetration tests, support in development) • emergency support (incident response, digital forensics) • open source monitoring <p><i>FIRST member</i></p>	<p>www.bfk.de</p>
27. FSC-CERT	<p>Fujitsu provides a range of infrastructure services that allow companies to deliver quickly and effectively while still optimizing the overall IT spend, reducing overall costs, improving ROI and still delivering outstanding service quality to your users. <i>FIRST member</i></p>	<p>http://ts.fujitsu.com</p>

Industry organisations active in network and information security

Academic Organisations	Role and responsibilities	Website
28. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) – German Association for Information Technology, Telecommunications, and New Media	<p>Bitkom is the voice of the IT, telecommunications and new media industry in Germany. The organisation represents more than 1200 companies, 900 of which are members.</p> <p>Bitkom has a seat on the executive board of EICTA (European Information, Communications and Consumer Electronics Technology Industry Associations).</p> <ul style="list-style-type: none"> • Education and the training of IT and telecommunications specialists, • green ICT, e-government, • e-health, • economic policy, copyright and patent law, • security and privacy issues, • software technologies, • consumer electronics, • climate protection, • sustainability <p>It provides a new legal framework for telecommunications and the media.</p>	www.bitkom.org
29. eco (Verband der deutschen Internetwirtschaft e.V.)	<p>eco – the German Internet Business Association represents and supports all enterprises that make commercial use of the Internet. It represents companies in the political process, encourages communication among market participants and supports the marketing of their products.</p> <p>eco's main activities are clustered around topics such as: infrastructure and technology, content, applications, as well as legal and regulatory matters, each of which is assigned to an individual member of the board.</p>	www.eco.de
30. VATM (Association of Telecommunications and Value-Added Service Providers)	<p>The Association of Telecommunications and Value-Added Service Providers (VATM) represents more than 70 telecommunications and multimedia companies active in the German market. The majority of VATM members are subsidiaries of, or affiliated with European and overseas service providers.</p> <p>VATM supports a working group on safety and data protection.</p>	www.vatm.de
31. VDE (Verband der Elektrotechnik, Elektronik und Informations-technik e.V.)	<p>The Association for Electrical, Electronic and Information Technologies (VDE) represents over 33 000 individual members, including a broad spectrum of engineers, scientists, technicians and some 5 000 students. In addition, 1 250 corporate and institutional members represent major German enterprises of the electrical, electronic and information technology industry, electrical utilities, federal authorities and institutions.</p> <p>Their goal is to ensure the ongoing development of various technologies and encourage their</p>	www.vde.com

Academic Organisations	Role and responsibilities	Website
	<p>applications in a wide variety of industries. They do this by promoting the national and international transfer of technical know-how; by supporting the education and training of new generations of talents; by participating in political decision-making on education and research; and by backing educational and career development with a broad program of conferences, symposia and seminars.</p>	
<p>32. ZVEI (Zentralverband Elektrotechnik- und Elektronik-industrie e.V.)</p>	<p>ZVEI represents 1 600 enterprises of the German electrical and electronics industry. Membership includes enterprises manufacturing electrical engineering products, producing software, operating electrical and electronics systems and networks or providing electronic information services. ZVEI is a member of EICTA (European Information, Communications and Consumer Electronics Technology Industry Associations). One of ZVEI's main objectives is to secure the competitive and innovative ability of the electrical engineering industry in Germany.</p>	<p>www.zvei.de</p>
<p>33. IT Security Made in Germany (ITSMIG)</p>	<p>ITSMIG is an association of German IT security companies that aims to foster cooperation between German IT security solutions suppliers and partners in foreign countries. It is a network of manufacturers, systems integrators, service providers, research institutes, and public services. Organization and management lies with the Fraunhofer Institute for Secure Information Technology (SIT).</p> <p>This international partner network enables German IT security companies to use instruments of external trade promotion and consolidates the export control of the federal government.</p> <p>The association links this network of German companies to the federal authorities, improving the use of existing public services in developing markets in target regions, i.e., the Arab states, Southeast Asia, and Eastern Europe. The network encompasses a considerable number of German enterprises in crypto-economy, trusted services (PKI), secure service provision, biometry, and systems integration.</p> <p>The tasks of the association comprise specifically:</p> <ul style="list-style-type: none"> • The advancement of the members' export activities, prioritized by target regions and groups • The advancement of the members' cooperation when submitting tenders in the target regions • The representation of members' interests in the target regions and their respective target groups 	<p>www.itsmig.de</p>

Academic Organisations	Role and responsibilities	Website
	<ul style="list-style-type: none"> The representation of the members' interests towards other associations and also directly towards international organisations, governments and the political system in general <p>The representation of the members towards corporate actors and the public, especially in the target regions.</p>	

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
34. University of Applied Sciences Gelsenkirchen, Faculty of Computer Sciences, Institut für Internet-Sicherheit if(is) – Institute for Internet-Security	<p>The institute conducts research and development in the area of Internet research, Internet EarlyWarning Systems, NIS research, e-mail security, Identity Management, Trusted Computing., and is also a creative service provider with a focus on internet security.</p> <p>The Institute for Internet-Security is an independent, scientific facility of the Gelsenkirchen University of Applied Sciences. Besides research and development, the institute is a service provider with a focus on Internet Security. One of the overall tasks is to enhance research and development in terms of Internet Security and to improve the statutory framework of Internet Security.</p>	www.internet-sicherheit.de
35. University of Bamberg, Faculty of Information Systems and Applied Computer Sciences	<p>Area of responsibility: Geo-information systems and services, digital libraries and archives, mobile assistance systems, computer-mediated communication; communication services, telecommunication systems, computer networks; SOA, middleware-integration, robust distributed and mobile systems, visual design and programming languages, visualisation of complex software systems.</p>	www.uni-bamberg.de www.uni-bamberg.de/gdi/leistungen/lehre/uebersicht/informationssicherheit/
36. University of Bonn, Institute of Computer Science IV, Communication and Distributed Systems	<p>The Institute of Computer Science IV addresses a wide range of topics. With long-term cooperation contracts linking the department to the Fraunhofer Institute IAIS and to the FGAN Institute FKIE, it reaches out to application-oriented research institutes in the region. Numerous joint research activities with these institutes and project-based cooperative research with key industry players such as Siemens, Nokia, T-Com and T-Mobile, allow both staff and students, to work on next generation prototype systems. In addition, the institute is active in basic research efforts funded by the DFG (the German Research Foundation), by the EU and others.</p>	http://iv.cs.uni-bonn.de
37. International School	The university is very active in organizing security	www.is-its.org

Academic Organisations	Role and responsibilities	Website
of IT Security (ISITS)	awareness sessions, facilitating the efforts of experts in obtaining the Master of Science in Applied IT Security.	
38. Technical University (TU) of Dresden, Faculty of Computer Science - Institute of Systems, Architecture - Chair of Operating Systems	Secure operating systems, Microcentres /L4, Trusted Computing, TPMs, Systems with extremely small trusted computing base, Secure start-up, IPSec, Real-time system, Trusted GUI.	www.inf.tu-dresden.de
39. University of Hildesheim, Institute of Computer Science	Intelligent Information Systems (IIS), Software Systems Engineering (SSE), Information Systems and Machine Learning Lab (ISMML).	www.uni-hildesheim.de www.sse.uni-hildesheim.de www.ismml.uni-hildesheim.de
40. Leibniz University Hanover, Faculty of Law, Institute for Legal Informatics (IRI)	IRI research focuses on data protection law, data security law, medico-legal aspects of information technology, intellectual property law (in particular copyright law), telecommunications law as well as the law of electronic business transactions. Work has also recently included aspects of legal theory and biotechnology law.	www.iri.uni-hannover.de
41. Leibniz University Hanover Research Initiative Safety & Security	The thematic complex 'safety and security' are currently burning issues in a worldwide context. Due to the broad heading of the subject, an interdisciplinary approach is indispensable. Leibniz University Hanover has installed the "research initiative safety & security", in which 25 institutions of all 9 faculties are co-operating to formulate and investigate problems and find solutions; researchers have technical, humanistic and socio-scientific origins. The research initiative's efforts are coordinated by a coordination team of researchers with a historical/ socio-scientific and mechanical engineering background.	www.uni-hannover.de
42. TU Braunschweig - Institut für Betriebssysteme und Rechnerverbund	The Institut für Betriebssysteme und Rechnerverbund is providing research and education in information technology law, covering the full spectrum of this still emerging discipline from data protection law and legal aspects of electronic commerce to all questions of intellectual property (copyright, trademark, patent law). A further focus is on legal theoretical issues raised by information technology. These topics can not be dealt with from a purely national perspective. They are international by their very nature. Therefore, IRI is taking part in a network of research institutions from all over the European Union. This network enables students to attend classes in Hannover and abroad to earn a European Master of Laws degree (LL.M.) in information technology law. IRI is also cooperating on a research level with European universities.	www.iri.uni-hannover.de

Academic Organisations	Role and responsibilities	Website
43. b-it (Bonn-Aachen International Center for Information Technology)	B-IT offers highly selective International Master Programmes in Applied IT as well as summer/winter schools for qualified computer science students.	www.b-it-center.de
44. Universität Mannheim Lehrstuhl für Praktische Informatik 1	"Praktische Informatik 1" is the Laboratory for Dependable Distributed Systems at the Department for Computer Science of the University of Mannheim, Germany.	http://pi1.informatik.uni-mannheim.de
45. Universität Karlsruhe, Fakultät für Informatik, Institut für Kryptographie und Sicherheit (IKS)/ Europäische Institut für Systemsicherheit (EISS)		http://iaks-www.ira.uka.de
46. LMU München Institut für Informatik	The Institute for Mobile and Distributed Systems (Prof. Dr. Claudia Linnhoff-Popien) provides teaching and research in: Location-based services (location-based services), Ubiquitous Computing , Mobile Platforms and Applications, Context-sensitive services, Mobile multimedia services, Car-to-Car Communication.	www.ifi.lmu.de
47. Fraunhofer Institute for Secure Information Technology (SIT)	The Fraunhofer Institute for Secure Information Technology SIT develops tailored, directly applicable solutions for all branches, including health, transport, traffic and production, as well as for commerce and financial services. In addition to client-oriented contract research, SIT offers consultation on the development of security concepts, and conducts studies for both the private sector and government.	www.sit.fraunhofer.de
48. Lehrstuhl Management der Informationssicherheit – Chair for IT-security Management of the University of Regensburg	Chair for IT-security Management of the University of Regensburg conducts research into testlab IT security; secure business processes; secure communications infrastructures; network and Internet security; mobile security and distributed systems; data protection, privacy and multilateral security; identity management and public key infrastructures (PKI); and digital rights management (DRM).	www-sec.uni-regensburg.de
49. University of Wuppertal, Faculty D - Safety Engineering	The first independent Faculty of Safety Engineering in Germany was founded at the Bergische Universität Wuppertal (Wuppertal University) in 1975. Today, every year about 500 students are trained in order to attain Bachelors of Science Safety Engineering as well as Masters of Science Safety Engineering, M.Sc. Fire Safety Engineering and M.Sc. Quality Management. Outstanding engineers and scholars in general can receive a Doctors degree as Dr.-Ing. (doctor of engineering) as well as Dr. rer. sec. (rerum	www.uni-wuppertal.de

Academic Organisations	Role and responsibilities	Website
50. University of Freiburg, IMTEK - Institute for Microsystem Technology, Laboratory for Electrical Instrumentation	<p>The core business of our research in safety and security includes:</p> <ul style="list-style-type: none"> • embedded wireless energy autonomous microsystems; • energy harvesting strategies for autonomous microsystems; • measuring and sensing and strategies; • design of antennae and communication protocols; • signal processing and sensor-actuator interfaces; • redundancy of microsystems and on-chip systems; • wireless passive and active sensor devices and radio frequency identification tags; • surface and bulk acoustic wave devices for sensor, radio frequency identification and frequency control applications; • research on materials of suitability of surface and bulk acoustic wave components. 	<p>www.imtek.de http://cst.mi.fu-berlin.de</p>
51. Ruhr-University Bochum, Horst Grötz Institute for IT-Security (HGI) Institut für Sicherheit im E-Business (ISEB) – Institute for eBusiness Security	<p>The Institute for IT-Security is one of Europe's largest university-based institutions for interdisciplinary research in the field of IT security. The HGI actively participates in international research in theoretical and applied cryptography; embedded security; mobile and fixed network security; trusted computing; secure operating systems and platforms; and legal and economic aspects of security.</p> <p>The Institute for eBusiness Security researches the business and economic implications of security in eBusiness, as well as information security in companies and public institutions. The main focus is economical analyses and organizational design tasks in the context of information security. Examples include information risk and security management, or questions of information security and confidence in online trading.</p>	<p>www.hgi.rub.de www.iseb.ruhr-uni-bochum.de</p>
52. Passau University, Institut für IT-Sicherheit und Sicherheitsrecht (ISL) – Institute of IT-Security and Security Law	<p>The Institute of IT-Security and Security Law (ISL) is characterized by its interdisciplinary focus on computer science, law and economics. The technical and economical aspects of IT security are extended to the dimension of law. With this interdisciplinary focus on IT security, the institute has a broad research field and can serve a broad market. Synergy between theory and practice as well as research and industry are in ISL's focus.</p>	<p>www.isl.uni-passau.de</p>
53. Technical University (TU) of Dortmund, Faculty of Computer	<p>Research and teaching in fields of information systems and security.</p>	<p>http://is6-www.informatik.uni-dortmund.de</p>

Academic Organisations	Role and responsibilities	Website
Science, Information Systems and Security (ISSI)		
54. Technical University Hamburg-Harburg Information and Communication Systems "CIT - Communication and Information Technologies"	Modern Methods for Modeling of Communication Networks, Software Security, Web Engineering, Electronic Commerce.	www.tu-harburg.de/cit
55. University of Applied Science Ludwigshafen/Rhein Chair Information Management and Consulting "	University of Applied Sciences in Ludwigshafen offers study paths for business information systems, information management and consulting in different variations leading to the degrees "Bachelor of Science" and "Master of Science" respectively. Information security is part of the curriculum. Much basic work and research has been done in cooperation with external companies as well as in the context of seminars and thesis.	http://web.fh-ludwigshafen.de
56. University of Applied Science Brandenburg Department of Business and Management	<p>Master of Science Security Management: The University of Applied Sciences Brandenburg offers the fully accredited master study course "Security Management" in cooperation with companies like SAP, Commerzbank, T-System and Lampertz.</p> <p>During three semesters, which can be fulfilled extra-occupational, students receive an overall view of security in companies and organizations, based on a practically oriented basic education. Each student can place individual focus on a special topic, e.g. information security, forensics, security of buildings and persons as well as business continuity or crisis management.</p>	www.fh-brandenburg.de
57. Free University of Berlin - Institute of Computer Science Computer Systems and Telematics	Focus of research at CST (Computer Systems & Telematics) group at Freie Universität Berlin (FU Berlin) is on mobile and wireless communications, communication architectures and operating systems for embedded devices, and quality of service aspects in communication systems. Within these topics CST develops software and hardware solutions for research prototypes, cooperates in international research projects, and integrates components in industrial solutions. Main emphasis is always on robustness, reliability, and security of all solutions.	www.fu-berlin.de
58. Technische Universität Berlin Fakultät IV für Elektrotechnik und Informatik	<p>The Technische Universität Berlin carries out research and teaching on technology for new generation of services and distributed systems, Smart Services and Smart Systems. These Smart Services and Smart Systems have a number of new properties that make them an autonomous, intelligent behavior.</p> <p>Basic research takes place in six centers of</p>	www.dai-labor.de

Academic Organisations	Role and responsibilities	Website
	excellence in various fields. The building will be in different application areas, the technologies developed for the realization of Smart Services and evaluated. This practice is intended to validate and test for demonstration purposes. An intensive cooperation with industrial companies guarantees a practical and solution-oriented approach. In this way, the DAI-Labor is able to develop in a university environment, technologies that meet high industrial standards.	
59. Fraunhofer Institute for Secure Information Technology (SIT)	The Fraunhofer Institute for Secure Information Technology SIT is the leading expert for IT Security and develops solutions for immediate use, tailored to the customer's needs.	www.sit.fraunhofer.de/EN/
60. Arbeitsgruppe Advanced Multimedia and Security, Fakultät für Informatik, Institut für Technische und Betriebliche Informationssysteme	Department of Computer Science, Research Group Multimedia and Security. Institute of Technical and Business Information Systems linked to the Otto-von-Guericke-University of Magdeburg.	http://omen.cs.uni-magdeburg.de/itiamsl

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
61. Initiative D21	D21 is Germany's largest public private partnership and its goal is to improve the general conditions necessary to move on successfully into the information and knowledge society.	www.initiated21.de
62. TeleTrust	Non-profit organisation for the promotion of trustworthiness of information and communication technology.	www.teletrust.de
63. Klicksafe.de	The German awareness node 'klicksafe.de' is part of the European Internet safety network 'Insafe' under the 'Safer Internet' programme which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user, as part of a coherent approach by the European Union.	www.klicksafe.de
64. Gesellschaft für Informatik (GI) – Network for IT	GI is a non-profit organization with approximately 25,000 worldwide, most of whom teach, research, or otherwise work in the field of informatics, while others are involved in related business and political areas. The main purpose of this network of professionals is to promote the impact informatics has had on the economy, business, and society.	www.gi-ev.de
65. CAST	GI is a non-profit organization with approximately	www.cast-forum.de

	25,000 worldwide, most of whom teach, research, or otherwise work in the field of informatics, while others are involved in related business and political areas. The main purpose of this network of professionals is to promote the impact informatics has had on the economy, business, and society.	
66. ISACA Germany	ISACA Germany is the German chapter of ISACA International. The association builds knowledge and facilitates the CISA and CISM exams and certifications for IT security professionals.	www.isaca.de
67. OWASP Germany	<p>The Open Web Application Security Project (OWASP) is an open-source application security project with local chapters. The OWASP community includes corporations, educational organizations, and individuals from around the world.</p> <p>This community works to create freely-available articles, methodologies, documentation, tools, and technologies. OWASP advocates approaching application security by considering the people, process, and technology dimensions.</p>	www.owasp.org/index.php/Germany
68. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)	<p>The Independent Center for Privacy Protection Schleswig-Holstein is a service that is there for the citizens. They investigate data security breaches and produce a written evaluation. They investigate data processing the authorities in Schleswig-Holstein. Breaches of the data protection law reported and remedial measures are presented.</p> <p>They advise authorities, businesses and citizens on all aspects of data protection, e.g. when setting up new computer systems, issues of interpretation of the data protection law or legislation. Every year they report on their activities in an annual report.</p>	www.datenschutzzentrum.de
69. vzbz (Verbraucherzentrale Bundesverband e.V.)	The Federation of German Consumer Organisations (vzbv) is a nongovernmental organisation acting as an umbrella for 41 German consumer associations. It represents the interests of consumers in public and vis-à-vis legislators, the private sector and civil society.	www.vzbv.de
70. Stiftung Warentest	Foundation for comparative testing of products and services.	www.stiftung-warentest.de
71. Deutschland sicher imNetz e.V. (DsiN)	DsiN is an association under the patronage of the German Federal Minister of the Interior. Members are companies, associations and inter-trade organisations from the field of IT-security. Main goal of DsiN is to raise awareness among consumers and companies towards a safer use of internet and IT in general.	www.sicher-im-netz.de

References

- Critical Infrastructure Protection (CIP Strategy) available at:
http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf
- Datenschutz im Internet – Gesetzentwurf des BMI zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht document available at: www.bmi.bund.de
- Study on eID Interoperability for PEGS: Update of Country Profiles - document available at:
<http://ec.europa.eu/idabc/servlets/Docb482.pdf?id=32522>
- BSI Standard 100-4 – Business Continuity Management available at:
https://www.bsi.bund.de/cae/servlet/contentblob/748954/publicationFile/41759/standard_100-4_e_pdf.pdf
- The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010
- ENISA CERT Inventory available at: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>
- IuK report issued by BKA at: http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf
- For more details on 1st IT Grundschutz Tag 2010 see:
https://www.bsi.bund.de/cln_156/ContentBSI/Presse/Pressemitteilungen/Erster_IT_GrundschutzTag_180310.html
- For more details on 1st IT Grundschutz Tag 2011 see:
https://www.bsi.bund.de/cln_156/ContentBSI/Aktuelles/Veranstaltungen/gstag/gstag_300311.html
- BMI guide available at:
http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile
- Global Phishing Survey: Trends and Domain Name Use 1H2010, available at:
http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu