Federal Ministry
of the Interior

National Plan for Information Infrastructure Protection

www.bmi.bund.de

Contents

1 Introduction

1.1 Germany's information infrastructures

Germany is already far advanced on the way to the information society. State institutions, businesses and society in general make intensive use of information technology. Today, like roads, water and power supply facilities, the information infrastructures are part of the national infrastructure, without which private households and public life would come to a standstill.

Information infrastructures are the nervous system of our country

Because our society depends largely on information technology, it faces new kinds of threats unknown in the past. Due to the global character of IT networks, IT security incidents may cause disruptions or total failure of the German information infrastructure, even if such incidents do not originate in our country. Criminals and terrorists increasingly try to damage complex technical systems with targeted attacks, and it cannot be ruled out that vital information infrastructures in Germany may become the target of such attacks.

Today our internal security is therefore inseparable from secure information infrastructures; their protection is a key priority for our national security policy. For this reason, the present National Plan has been drawn up under the aegis of the Federal Ministry of the Interior. Implementing this plan will help strengthen the defence of Germany's information infrastructures against global threats.

1.2 Threats and risks to our information infrastructures

Technical defects, human error or deliberate acts of damage or destruction are a frequent cause of system disruptions or break-downs which, in turn, may directly affect other sectors because of the network architecture of information infrastructures. This may have a snow ball effect on the economy and society as a whole.

New threats

Whether used in private or business environments, IT systems are always vulnerable to hacking attacks or threats posed by computer viruses and worms. A growing number of malicious software programmes and targeted attacks can be attributed to organized crime and terrorist groups. Their main motive, in contrast to that of 'script kids', is not to get attention but to profit financially from such attacks or harm the national economy.

Primary targets of such attacks are large companies, banks or public institutions, in addition to private household computers which criminals try to penetrate to steal online banking details or spread computer viruses and spam.

The attackers use a whole range of different methods, some of which have been included, by way of example, in the following list:

- denial of service attacks using privately owned hacked computers
- use of spyware
- interception or manipulation of data transfers
- taking advantage of weaknesses, or using malware, such as computer viruses and worms.

The fact that the majority of PCs use standard software, from internet applications to complex administration systems, makes it easy for attackers to find vulnerabilities. Automated attacks that make use of security gaps in these programmes cause enormous damage in many systems at exactly the same time, before a response is possible or vulnerabilities could be patched.

In the meantime, organized criminals have shifted their attention away from single PCs towards routers, firewalls and other security applications intended to protect the IT systems of businesses and public administrations. This new type of attack affects not only individual PCs, but possibly thousands of PCs in the attached network. In the worst-case scenario, manipulation of central IT systems may cause the entire information infrastructure to collapse, resulting in significant economic damage.

1.3 Strategic objectives

To ensure full protection of information infrastructures in Germany, the Federal Government has set out three strategic objectives in the National Plan for Information Infrastructure Protection:

- **Prevention: Protecting information infrastructures adequately**
- **Preparedness: Responding effectively to IT security incidents**
- **Sustainability: Enhancing German competence in IT security/ Setting international standards**

These objectives are a supplement to the Federal Government's IT strategy. Implementation plans for the federal administration and for critical infrastructures will be drawn up to ensure that these objectives are achieved, and additional plans may follow, if necessary.

To protect information infrastructures in Germany on a sustained basis, the Federal Government will regularly review this National Plan and make necessary adjustments in accordance with actual needs.

1.4 Shared jurisdiction for protecting information infrastructures

The growing importance of information infrastructures for our country requires joint action by the state, economy and society. With the present National Plan, the Federal Government ensures that these tasks are fulfilled.

IT security in the federal administration

The federal administration itself operates parts of the national information infrastructure. The present National Plan serves to guarantee medium- and long-term IT security on a high level. Therefore, the Federal Government will set out precise guidelines for the protection of the federal administration information infrastructures in an implementation plan for the federal administration (Umsetzungsplan Bund).

This plan should lay down jointly prepared technical, organizational and procedural standards for the federal administration, which the ministries should apply in a flexible manner under their own responsibility.

With this plan, the Federal Government sends a clear signal: protecting the administration's own infrastructure is the basis for the protection and reliable operation of national infrastructures in Germany. Thus, implementing this National Plan will also add to the attractiveness of Germany as a place to do business.

As the national authority in charge of IT security and as the Federal Government's main IT security service provider, the Federal Office for Information Security (BSI) is responsible for coordinating the implementation of this National Plan. To enable the BSI to fulfil this task, the number of its staff has been and to some extent still will be increased and priorities will be redefined; overall, the BSI will be assigned a more active role as IT security advising institution.

Cooperation between the federal government and the private sector

In Germany, the majority of information infrastructures are run by private companies. Hence, protecting these infrastructures is primarily the task of private operators and service providers. However, given the dramatic consequences damage to those infrastructures might have for the state, the economy and large parts of the population, sole responsibility of individual operators is neither sufficient nor appropriate. This holds true also for critical infrastructures in Germany.

Although the Federal Government defines the necessary requirements for the protection of information infrastructures, it is not capable of implementing them all by itself. For this reason, it will enter into precise agreements with private operators on how to fulfil the necessary tasks and respond effectively and in a concerted manner to IT security incidents.

Therefore, the Federal Government calls upon its partners in the private sector to take an active part in implementing the National Plan, especially where it refers to critical infrastructures. The goal must be to ensure that protective measures are taken not only to safeguard one's own business operations, but to promote Germany as a place to do business and to ensure its international competitiveness.

To this effect, the Federal Government, together with operators of critical infrastructures, is preparing the CIP Implementation Plan (Umsetzungsplan KRITIS). It will lay down measures to raise the level of IT security considerably. The Federal Office for Information Security (BSI) as well as other competent public authorities will offer their expertise to assist the operators of critical infrastructures in carrying out the measures set out in the CIP Implementation Plan.

Citizens and society as a whole

Comprehensive protection of information infrastructures in Germany is not only the business of IT specialists. It needs the commitment of everyone – of manufacturers of IT products, service providers, employees, people in charge of IT matters in public authorities and private businesses, and of those who use these structures.

As consumers, citizens increasingly use information infrastructures. In so doing, well-informed consumers are very aware of the security issues involved and therefore prefer trustworthy products and procedures. Hence, compliance with high security standards is also a positive economic factor for IT manufacturers and distributors and IT service providers; it is the basis of a functioning market and innovation schemes.

The aim of the Federal Government is to encourage people to make more intensive use of existing information and information provided in this National Plan. By following the government's recommendations citizens actively contribute to IT security in Germany, and at the same time manufacturers and distributors of IT products and services are encouraged to give utmost priority to the security of their products already during development and adequately inform their customers of IT risks and possible protective measures.

International cooperation in protecting information infrastructures

In addition to cooperation with private businesses, another main pillar of the National Plan is actively advocating German interests in order to shape policy at the international level.

Binding standards for checking and evaluating security features of IT products are a prerequisite for secure information infrastructures. Therefore, the Federal Government advocates the creation of appropriate international norms and standards.

2 Prevention: Protecting information infrastructures adequately

Security risks can be reduced by spreading knowledge about threats and possibilities for protection, by clearly assigning responsibilities for security matters, by implementing security measures and by using reliable products and processes.

Goal 1: Raise awareness of risks related to IT use

The Federal Government continues to trust in raising the awareness of and informing the general public and the business sector about the risks to IT use. To this effect, initiatives are being launched that are directed to people at all levels, from corporate management and high-level public administration to ordinary employees and private individuals as PC users.

Goal 2: Use of safe IT products and secure IT systems

The Federal Government supports the use of reliable IT products and systems and trusted IT security applications in Germany, above all within the federal administration. The Federal Office for Information Security (BSI) will extend and improve its capacity to examine and evaluate IT products and systems under security aspects

and issue relevant certificates. The BSI publishes product recommendations, issues technical guidelines for the use of these products and lists products that were issued a German IT security evaluation certificate.

Goal 3: Respect confidentiality

Unprotected digital communications are extremely vulnerable, easy to intercept and manipulate. Therefore, the security of the German information society and Germany as a place to do business depend on the availability of reliable, innovative and trusted encryption products that guarantee confidential communication. The Federal Government is promoting the development and the German manufacturers of adequate products, in accordance with the 1999 decision concerning encryption; in addition, it will use encryption and security applications for its own communications.

When awarding IT and IT security contracts at federal level, public authorities will pay greater heed to national security interests on the one hand and the reliability and trustworthiness of bidders on the other.

The business sector is made particularly aware of the risks associated with information theft (e.g. caused by economic espionage) and the possibilities and benefits of preventing such theft by using reliable German encryption products.

Goal 4: Putting safeguards in place

It is necessary to put coordinated technical, physical, organizational, and structural safeguards in place. Responsibilities, duties and roles for all tasks related to IT protection must be clearly defined. Adequate IT security measures are being implemented in all public authorities at federal level. The federal ministries in charge will ensure that IT security strategies for federal authorities are kept up to date and are implemented effectively. The Federal Government is improving IT security management coordination within the federal administration to ensure uniform and generally comparable, efficient, and transparent processes and work-flows from the highest ministerial level down to every single authority within the remit of each ministry. All businesses and organizations are firmly called upon to make adequate arrangements for protecting their IT systems.

Goal 5: Creating framework conditions and guidelines

The Federal Government undertakes to create adequate framework conditions and guidelines, taking account of international norms and standards, in order to ensure full protection in all security-relevant areas.

Each federal ministry will make sure that standards and guidelines are implemented in accordance with the Umsetzungsplan Bund by its own ministry and all authorities within its remit, for example by putting the necessary structures in place (e.g. commissioner for IT security issues; reporting; role and responsibilities of the management, etc.).

Appropriate guidance will be given to those branches of the economy where special requirements apply to IT security. All other areas of society will be provided with recommendations and guidelines on IT security.

Goal 6: Coordinated security strategies

Since security systems are only as robust as the weakest link in the chain, it is crucial to harmonize security-relevant processes and mechanisms. Therefore, the Federal Government advocates defining joint standards and coordinated application concepts, among other things, in order to optimize systems with regard to their security, technical, economic, and data protection properties.

Goal 7: Shaping policy at national and international level

The Federal Government will intensify its efforts to actively shape policy with regard to existing and new forms of cooperation for protecting information infrastructures. In addition, it will strengthen national and international cooperation in order to bring German security interests to bear when formulating guidelines, directives and other legal instruments. To be able to respond comprehensively to threats, given the global character of networks, the federal ministries and other federal authorities will increase their cooperation with their counterparts abroad. Together with its partners, for example in the EU (especially ENISA), NATO, OECD, UN, G8 and at international level in general, the Federal Government will raise the awareness of the vulnerability of information infrastructures and support the provision of technical solutions.

3 Preparedness: Responding effectively to IT security incidents

Information infrastructure disruptions require fast and effective responses. In addition to collecting and analysing information, this includes alerting those affected and taking action to reduce the damage. To this effect, the Federal Government is developing a national IT crisis response centre.

Goal 8: Identifying, registering and evaluating incidents

The IT crisis response centre at the Federal Office for Information Security (BSI), which is currently being put in place, will play the role of a national command, control and analysis centre that will be able to provide a reliable assessment of the current IT security situation in Germany at any time and that will cooperate with existing control and crisis centres in a given incident. To enable the BSI to fulfil this function, a network of sensors will be put in place to detect IT security incidents. Additional sources supplying information on IT incidents will be made available to the BSI by extending the international watch and warning network, of which the Federal Government was a founding member. All these measures will ensure that those in charge in the public and the private business sectors have the information necessary to quickly decide what action must and can be taken.

Goal 9: Informing, alerting and warning

The competent federal authorities will provide information on current threats and risks tailored to certain target groups. All those in charge of IT systems and information infrastructures, from the ordinary private user to the IT administrator in companies, public authorities and other organizations, will get access to appropriate information.

As part of the national IT crisis management concept of the Federal Government, an alert and warning system will be established to inform all those potentially affected in a rapid and comprehensive manner of imminent attacks against or severe disruptions of information infrastructures. This will help respond in time and prevent large-scale damage.

Goal 10: Responding to IT security incidents

The federal IT crisis response centre will enable all competent bodies to respond rapidly to serious incidents. It provides incident analyses and assessments to all relevant bodies and coordinates the cooperation with local and sector-internal crisis management organizations. If in the case of incidents affecting larger parts of the federal administration it is necessary to take measures that require greater powers than those assigned to local authorities, a coordinating body of the federal ministries will agree on the necessary measures and commission the IT crisis response centre to enforce their implementation.

A prerequisite for being able to respond effectively to IT security incidents are well-prepared emergency plans and clearly defined procedures.

The Federal Government requires such emergency plans to provide also for coordination and cooperation with national crisis management, in addition to regulations concerning crisis management in companies and public authorities at local level.

4 Sustainability: Enhancing German competence in IT security/ Setting international standards

For the long-term protection of national information infrastructures Germany needs highly-qualified experts and trusted IT services and security products, in addition to the political commitment of all those in charge to improve IT security.

Goal 11: Promoting trusted and reliable information technologies

The Federal Government promotes the development of trusted German IT products and services, and of trusted information technologies in Germany, particularly the encryption industry. The aim is to increase the market penetration and encourage a wider community to use trusted IT products.

Goal 12: Enhancing national competence in IT security

The Federal Government will use the expertise of German IT security service providers, contribute to its further development and thus to national competence in IT security. In the course of implementing this National Plan, already existing competences and functions of the BSI will be expanded considerably and supplemented by the expertise in other ministries. As the key national IT security agency the BSI will work together with other important supervisory bodies such as the Regulatory Authority for Telecommunications and Posts (RegTP) and play an active part in shaping policies concerning IT security in the federal administration, large-scale projects of the Federal Government and critical infrastructures.

Goal 13: IT security competence in school education and professional training

The Federal Government uses its expertise in the field of IT security to raise the priority of IT security in school education and professional training on a broader scale and to make sure that IT security is given due heed in developing new professions and training and study subjects. Furthermore, information services for citizens, schools, universities, the business sector and public administration will

be expanded and improved, increasing awareness of IT security issues within society as a whole.

Goal 14: Promoting research and development

The Federal Government supports basic scientific research in Germany, advocates the engagement of German businesses in international research and technology programmes, particularly in the 7th European Research Framework Programme. Developing innovative products guarantees the long-term reliability of German information infrastructures. The cooperation between industry and R&D at universities will be intensified.

Goal 15: Expanding international cooperation and setting standards

The Federal Government will advocate German security interests in international standard setting bodies when developing international standards for the protection of information infrastructures. To this end, inter-ministerial and inter-disciplinary cooperation in drafting relevant norms, standards and laws will be strengthened at national level.

Together with European partners, the Federal Government will develop reliable IT security solutions. German IT security products and solutions will receive due consideration.

Abbreviations

BMI	Federal Ministry of the Interior
BSI	Federal Office for Information Security
ENISA	European Network and Information Security Agency
EU	European Union
IT	Information technology
ITSEC	Information Technology Security Evaluation Criteria
KRITIS	Critical infrastructures
NPSI	National Plan for Information Infrastructure Protection
PC	Personal computer
PGP	Pretty Good Privacy
RegTP	Regulatory Authority for Telecommunications and Posts
S/MIME	Secure Multipurpose Internet Mail Extension

Glossary

(Definition of key terms used in the National Plan for Information Infrastructure Protection / in the present document)

Information infrastructure

The entirety of IT elements that are part of a given infrastructure.

Interdependency

The total or partial mutual dependency of several goods or services.

IT security

Ensures the availability, integrity, verifiability and confidentiality of information in the use of information technology.

For this purpose,

- 'availability' means the situation in which the necessary usability of information as well as IT systems and components is ensured;
- 'integrity' refers to the exclusion of unauthorized and prohibited modifications of information as well as of IT systems and components;
- 'verifiability' means the situation in which required or promised properties or features of information or transfer facilities can be verified by the user and vis-á-vis third parties;
- 'confidentiality' refers to the exclusion of unauthorized obtaining or procuring of information.

IT security products

Products used to ensure compliance with IT security requirements, including virus scanners, firewalls, public key infrastructures (PKI), intrusion detection systems (IDS), and plug-ins for data encryption in e-mail clients, e.g. for PGP or S/MIME. IT security products help ensure protect software applications, processes, systems and/or data to a greater extent than would be possible without such products.

Critical infrastructures

Organizations and facilities of great significance for the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions of public order or other dramatic consequences.

In Germany, the following infrastructure areas are deemed as critical: (see also http://www.bsi.bund.de/fachthem/kritis/index.htm):

- transport
- energy (electricity, oil and gas)
- hazardous substances (chemical and biological agents, transport of hazardous material, arms industry)
- information technology and telecommunications
- the financial, monetary and insurance system
- supply of vital goods and services (public health service, emergency and rescue services, civil protection, food and drinking water supply, waste disposal)
- public authorities, the administration, the judiciary (including police, customs and federal armed forces)
- other (the media, large research institutions, architectural buildings of outstanding or symbolic value, cultural heritage)

Safe IT products

In contrast to IT security products, the main characteristic of safe IT products is that they themselves are safe. Whether a product is safe or not can be established by evaluating it under certain security standards, such as ITSEC or Common Criteria, and can be documented in an IT security evaluation certificate. Special strategies, which strive to minimize the chance that vulnerabilities occur at all or, if they occur, to ensure that they are less complex, are used to develop safe IT products.

Secure IT systems

IT systems comprise several IT products and components and are used in specific environments and under given framework conditions as regards organizational structures and human resources. Secure IT systems are characterized by having in place a security management and by having implemented the necessary infrastructural, organizational, personnel and technical security measures that were evaluated by an independent body and issued a system security evaluation certificate.

Reliability

Systems, applications or services are deemed reliable if they comply with relevant requirements (e.g. quality of service requirements) and if they function in a way that does not differ to an unacceptable degree from users' expectations. In this context, the term ‘reliability’ is used as an umbrella term, including (at least) the following concepts:

- availability (i.e. permanent usability)
- robustness (i.e. functional stability)
- safety (i.e. possibility to operate and apply such systems or products without being harmed or without harming the environment)
- confidentiality (i.e. no unauthorized disclosure of information)
- integrity (i.e. no unauthorized modification or destruction of data)
- maintainability (i.e. possibility to maintain/ restore operation by repair works; possibility to upgrade the system)

Published by:

Bundesministerium des Innern

IT-Stab, Referat IT 3

Alt-Moabit 101D | 10559 Berlin

Editor:

Bundesministerium des Innern

IT-Stab, Referat IT 3

Design & Production:

Zucker.Kommunikation, Berlin

Images:

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Status:

October 2005