



Federal Ministry
of the Interior

National Plan

for Information
Infrastructure Protection
CIP Implementation Plan



Early detection and Mitigation of IT Crises

UP KRITIS
Working Group 2
“Crisis Response and Mitigation”

www.bmi.bund.de

Preface

The vulnerability of modern industrial infrastructures became obvious for the worldwide public no later than with the terrorist attacks in New York, Madrid and London. Of course, there had been attacks on all manner of vital assets in highly developed industrial societies and service economies before 11 September 2001 – we might recall the poison gas attacks in Tokyo in the spring of 1995 – but it was only after New York that non-experts became aware of the importance of functioning transmission links, supply systems, communication channels, etc. – or, more concisely, infrastructure.

In Germany, the course of action taken jointly by government and industry to safeguard infrastructures relevant to the whole of society is one significant effect of this new development. This approach, which is based on the “Public-Private Partnership” model (PPP model), has proven more successful in the long term than separate actions being taken by government and the private sector and is, as a result, a *modus operandi* appreciated both by the public and the private sector and therefore provides resilience in case of crisis situations.

One of the key insights gained by working together has been that the protection of vital infrastructures in our society had been practised in isolation in any given sector. However, it has become apparent that sharing the work involved in critical infrastructure protection (CIP) provides the best chance to serve the society in times of crisis. Needless to say, the PPP approach did not settle overnight like dew on the critical infrastructure field, in contrary a great deal of convincing was required on many fronts before the seed was finally able to bear fruit.

The connecting element of the growing CIP community is the “National Plan for Information Infrastructure Protection (NPSI)” adopted by the Federal Government in June 2005. This Plan acts as a reference framework for information infrastructures, supporting and protecting the various angles in the strategy polygon. As early as August 2005 the Federal Ministry of the Interior (BMI) published as a physical counterpart to the NPSI the Baseline Protection Concept for the “Protection of Critical Infrastructures” as a recommendation for companies, and then started to work at the beginning of 2006 on the CIP Implementation Plan branded as UP KRITIS (this term will be used throughout this document). Following the publication of this plan

in September 2007, work began on fleshing out the theoretical bones of the Implementation Plan. The results of these efforts concerning the early detection and management of IT crises are presented in this document.

Contents

1	Introduction and motivation	5
2	Participating organisations	10
2.1	Companies	10
2.2	Single Point of Contact (SPOC)	12
2.3	BSI IT Situation Centre	14
2.4	Communications platform for informal information exchange	16
2.5	Other communication structures	17
3	Early crisis detection and mitigation processes	18
3.1	Basics	19
3.2	Security situation assessment	23
3.3	Early crisis detection	24
3.4	Alerts and crisis mitigation	26
3.5	Regular exchange of information	27
3.6	Summary in tabular form	28
3.7	Communications technology	29
4	Actual implementation and further procedures	30

Annex	32
Abbreviations	33
Glossary	34
References	38
Participating UP KRITIS partners	39

Figures

Figure 1: Statuses in UP KRITIS communications	20
Figure 2: Lines of communication from companies to the BSI via SPOCs	20
Figure 3: Lines of communication from the BSI to companies via SPOCs	21

Tables

Table 1: Parties, tasks and means of communication involved in the crisis management statuses	28
--	----

1 Introduction and motivation

The significance of critical infrastructures is most evident in the services which are essential for a modern industrialised society. The availability of services is increasingly dependent on the functioning of the information infrastructure. Information technology (IT) is all but indispensable in the modern-day business world and for the control and monitoring of processes. Existing interdependencies across different sectors and industries are reinforced further still by the joint use of the Internet and telecommunications networks.

The Federal Government responded to this development by adopting its “National Plan for Information Infrastructure Protection (NPSI)”¹ as the overarching government IT security strategy. The NPSI emphasises the society-wide responsibility for the protection of information infrastructures, a task requiring a coordinated approach supported of all responsible parties. The document is aimed particularly at the Federal Administration and the operators of critical infrastructures.

The responsibility for the provision and operation of critical infrastructures in Germany falls mainly to the private sector, i.e. on individual enterprises. Accordingly, individual companies and organisations so far have been responsible for covering their own IT security requirements for the most part. This responsibility still exists but has to be supplemented by company-wide and cross-sector elements.

In accord with the NPSI, the private sector and the Federal Government drew up the Implementation Plan of Critical Infrastructures, furtheron referred to as UP KRITIS¹, which was approved by the Federal Cabinet on 5 September 2007. The CIP Implementation Plan concludes with recommendations for crisis prevention and response to crises, which are largely contingent upon failure or limitation on IT systems. These are referred to below as IT crises.

¹ German title for “Implementation Plan of Critical Infrastructures”(CIP Implementation Plan):
Umsetzungsplan für Kritische Infrastrukturen, also referred to as Umsetzungsplan KRITIS or UP KRITIS.

It is quite possible for an IT crisis to have its origins outside of IT, arising as a result of a natural event, for example, or a failure of supply capacities. Incidents outside or within IT which affect IT can, in turn, spark further incidents which take on crisis proportions in terms of their impact on the IT infrastructure. If crises are to be detected at an early stage, it is essential to observe and report all events which can have repercussions on IT and not to restrict the observation to events within the information technology.

Crisis are often unpredictable and their impact on individual companies or sectors of industry cannot be reliably predicted. Under certain circumstances, it can be entirely impossible to recognise them and to mitigate them at an early stage because of highly dependent relationships between involved individuals which are not always immediately obvious. Not until information has been exchanged with the right contacts is the required transparency established, allowing efficient action to be taken in the event of a crisis. Damaging effects cannot arise solely as a direct result of a triggering event, but primarily due to delayed action and inadequate communications before and during crisis mitigation.

The NPSI and the UP KRITIS therefore regard the early detection and mitigation of crises primarily as a challenge for the communication flow between the companies and organisations of different sectors and industries, but also between organisations and government bodies.

Aims of the document

Communication links are therefore the most important prerequisite for both early detection of and response to a crisis. Consequently, experts from industry and the Federal Administration cooperate to draw up a concept for the establishment of appropriate communication structures in the context of the CIP Implementation Plan. Since April 2007 selected experts have been concentrating on the principles fundamental to an effective cross-sector early detection and mitigation of crises ranging from constrained ones up to those of national proportions. This document is the result of their work.

Deliberations are focused on the cross-sector communication structures and processes, ranging from the basic exchange of information, analysis of

the IT situation, warning and alerting up to the coordinated mitigation of the crisis.

The document identifies requirements for the organisations involved in the communications structure in terms of capabilities, interfaces and the means of communication used. Single Points of Contact (SPOCs) are central to the communications structure in order to minimise the communication effort required by each individual involved and to structure the lines of communication. This concept defines the processes required for an efficient exchange of information and links all the parties involved in communications.

The communications structure developed will supplement the existing facilities and procedures in the companies, sectors and the Federal Administration. It will create the appropriate basis for the combined efforts of the private sector and the national IT Situation Centre at the Federal Office for Information Security (BSI) towards the effective counteraction against future IT crises.

The extraction of reliable information is based on a comprehensive view comprised of many local perspectives. This breadth of perspective can only be achieved with the active and collaborative contribution of those participating in UP KRITIS. Only as the result of concerted action is it possible to generate a realistic and overall picture of the IT security situation, which will benefit the companies and sectors involved because potential damage can be limited by taking directed action at an early stage. A common understanding of the nature of the threat also enables a well-coordinated approach to managing the crisis.

Companies are already informing each other about the security of their IT infrastructures within their sector because damage can be reinforced by technical interdependencies between companies. Moreover, initial communications structures which extend beyond the confines of specific companies in the event of a crisis have already been established. Some sectors already have their own escalation processes and reporting channels which involve the relevant authorities and police forces. Although appropriate crisis response and crisis mitigation structures already exist in companies and organisations and in some sectors, the Federal Government and the operators of critical infrastructures see the necessity for further sector-wide and cross-sector development.

This concept document provides a detailed description of both cross-sector and sector-wide structures and processes.²

Benefits for companies

Using a cross-sector approach to crisis response and mitigation, operators of critical infrastructures and the Federal Government are working on a resilient communications structure which consists of a “network of trust” and in which the BSI plays a central role. As a government institution with no competitive interests, the BSI can guarantee its confidential handling of the information and sensitive data it receives. Companies and the BSI will be both givers and receivers of information in this communications structure. Legal requirements, data protection considerations and the necessary trustworthiness will be taken into consideration when establishing the communications infrastructures and will be essential and fundamental to this cooperation.

It is in the best interest of companies to collaborate on UP KRITIS with a view to strengthening Germany’s economy but also in the interest of shareholders, customers and employees of the companies as their cooperation can help to avert or at least minimise potential damage arising from IT crises. This is an integral part of risk management and is in a company’s economic interest.

As a result of this cross-sector communication, the companies can have early access to information which gives them additional time to react to incidents and take effective countermeasures. Necessary, and possibly cost-intensive, measures can be taken in advance of an IT crisis or during the crisis management process on the basis of broad and well-founded knowledge of the IT security situation.

All companies are treated equally in the scope of cooperation on UP KRITIS as this facilitates a joint and early response to an IT crisis. Trusted contact persons should also be available who have the necessary cross-sector expertise to pinpoint solutions for mitigation of an IT crisis. Common terminology facilitates coordination of response to a crisis across sectors. Moreover, the costs in terms of developing solutions for early crisis detec-

² The body of the text only differentiates between these structures where there are essential differences. Otherwise, it uses the term industry-wide communication.

tion and mitigation processes can also be reduced if know-how is shared across different sub-sectors. Joint exercises also improve a company's own ability to respond to a crisis.

Assignment of tasks

The assignment of tasks can be described as a system in which the companies take measures serving the purposes of communication and the dissemination of information. SPOCs are responsible for the cross-company exchange of information with the BSI. Across sectors the information relevant to early crisis detection and mitigation processes, which has been obtained by companies or by the BSI, is disseminated to all the relevant parties via the SPOCs.

With the present document the members of the "Crisis Response and Mitigation" working group have developed a concept for a communications structure appropriate for early crisis detection and crisis mitigation and support its implementation. The communications processes set up on the basis of this document will be tested in the context of the emergency exercise concept devised by the "Emergency and Crisis Exercises" working group.

Consistency and sustainability will be ensured by the fact that under the auspices of the Federal Ministry of the Interior, the concept will be updated and adapted to meet changing framework conditions.

2 Participating organisations

This chapter describes the organisations participating in the communications structure, as defined in UP KRITIS, and their role in the context of information exchange across sectors. Any existing structures and conceptual approaches are included in the process. Examples include the BSI IT Situation Centre and organisations in the companies which are already committed to the fundamental idea behind UP KRITIS. Single Points of Contact (SPOCs) are newly included in their capacity as linking elements. The SPOCs enable companies to communicate with the BSI IT Situation Centre and exchange information on early crisis detection and mitigation. In the following this document specifies the participants and their organisations, including their respective responsibilities and activities, the capabilities and interfaces required, and the necessary means of communication.

2.1 Companies

IT security is essential for the entire economy to maintain the business and production processes. Consequently, companies have already established appropriate structures for early crisis detection and mitigation. Moreover, companies have well-founded knowledge of their sector of industry and of the proven forms of communication. Their capabilities and know-how are therefore indispensable to the effective, efficient and cross-sector implementation of the objectives set out in UP KRITIS.

Capabilities and tasks

Companies have fundamental knowledge of their own IT security situation. They are adept at making an expert analysis and evaluation of any incidents with regard to their criticality for the company. Hence, they are well equipped to make an accurate assessment of their own IT security situation. The companies use this know-how to operate their own internal security situation diagnosis procedures for the detection and reporting of incidents. Those who assess whether the company is faced with an impending crisis can also specifically evaluate external information and its impact on the company.

Taking the known facts of the situation into consideration and acting to the best of their knowledge and belief, the companies should make sure that information on the IT security situation reaches the BSI IT Situation Centre via the SPOC responsible for their sub-sector (see also Section 3.3). Conversely, companies should ensure that information, especially any information regarding developments relevant to IT security, received from the SPOC or the BSI is transmitted to the relevant bodies in the company. These organisational matters have to be integrated into the companies' policy and process documentation. Forwarding an item of information is always voluntary.

Companies have a vital interest in a rapid response capability in the event of a crisis. Consequently, they should take measures to ensure that they can be contacted by the SPOCs, ideally around the clock and every day (24/7), but at the very least during the standard working hours for the particular sub-sector.

Interfaces

Companies operating in the same sub-sector often exchange information on the IT security situation with each other. In the course of implementing this concept, they also set up a communications interface to the SPOC responsible for their sub-sector for the purpose of transmitting any future reports on the IT security situation and, where necessary, raising the alarm.

Companies, large-scale enterprises and international concerns can also communicate directly with the BSI IT Situation Centre, especially in cases where an sub-sector has not set up its own central SPOC or where the availability of the SPOC is still limited.

There are points of contact within the companies where information can be shared outside the crisis mitigation process. In the event of an IT crisis it is possible that the responsibility in the company for communications regarding IT will change depending on the specific situation and the concrete exposure to threats. To maintain communication it is therefore necessary for the relevant corporate units to be aware of and comply with this concept. The companies should inform the relevant communication partners about any change in responsibility for their communications. The companies are responsible for informing the SPOC promptly of any changes to their contact details.

2.2 Single Point of Contact (SPOC)

It is essential for the early detection and mitigation of IT crises that the operators of critical infrastructures and the BSI IT Situation Centre communicate with each other. A bilateral exchange of information between all companies and the BSI IT Situation Centre is not feasible given the large number of companies. Therefore, the SPOC which is set up in the individual sub-sectors is intended to serve as the reporting point and the link between companies and the BSI IT Situation Centre. The SPOC is an established function in the sub-sector and can be located within a company.

A SPOC is required to be in possession of the fundamental technical and organisational capabilities, to have access to as many means of communication as possible, and to be acquainted with the current IT security situation in its sub-sector on the basis of the information supplied by the companies. The companies have a strong and sustainable relationship of trust with the SPOC responsible for their sub-sector.

The central task of the SPOC is to transmit information with speed, integrity and dependability, and to alert the companies in its own sub-sector and the BSI IT Situation Centre.³ The SPOC is therefore marked out by the rate at which it can respond and is effective both in terms of the early detection of a crisis and raising the alert.

Knowledge of the sub-sector and IT security expertise specific to the sector are desirable elements which, for example, enable the SPOC to explain messages received in its sub-sector to persons outside that sub-sector. However, the diagnosis of the IT security situation does not lie within the remit of the SPOC. Therefore, it does not necessarily have any profound technical expertise and know-how with regard to the analysis and evaluation of incidents.

If necessary the SPOC should summarise similar messages from different companies in its sector before forwarding them, thus condensing the flow of information at the sub-sector level.

If requested by the reporting party, the SPOC will filter messages before forwarding them, removing any classified or sensitive items of information. If this is the case, the company issuing the report will have to indicate the rel-

³ However, the present concept does not imply that the SPOC has an obligation to report information.

evant parts. The aim of this sanitisation process is to protect the legitimate interests of those sharing information while maintaining the relevant concepts. Not least for this reason does the efficiency of the SPOC depend on enjoying the trust and confidence of the companies in its sub-sector.

In the context of crisis management the SPOC may also take on the role of a coordinator in communications between the companies in its sub-sector, and participate in cross-company measures in its sub-sector, for example.

The company which takes on the role of the SPOC for a sub-sector should be able to provide additional resources during crisis mitigation. In particular, these resources might take the form of additional expertise or organisational support.

Some SPOCs may not be fully operational in the initial concept implementation phase; therefore it may be advisable to adopt the strategy in stages. Consequently, in the transitional phase there will still be a need for the companies to communicate directly with the BSI IT Situation Centre. A SPOC might initially limit its role to the forwarding of information, whereas it can subsequently add the capability of evaluation and analysis. However, the priority is always to transmit information with speed and integrity.

Since the SPOC also forwards early crisis detection and alert messages, it should be accessible around the clock seven days a week (24/7) and capable of responding immediately. Communication systems might break down in a crisis, preventing the exchange of information, therefore the SPOC ought also to have access to the means of communication listed in Section 3.6 “Summary in tabular form”.

Interfaces

All SPOCs have interfaces to the BSI IT Situation Centre and to contact persons in the companies in their respective sub-sectors who are as accessible as possible. The SPOC is the reporting point for the companies in a sub-sector, receiving the information sent in and relaying it to the companies or to the BSI. The SPOC is the BSI’s primary point of contact for the sub-sector.

The SPOC maintains and updates the contact address list for the companies in its sub-sector. The BSI maintains the address list of all the SPOCs. The

SPOCs are responsible for informing the BSI promptly of any changes to their contact details.

2.3 BSI IT Situation Centre

The BSI IT Situation Centre was established to enable a rapid and competent assessment of the need for action and the possible courses of action in the event of IT security incidents both at government level and in commerce.

Capabilities and tasks

The BSI IT Situation Centre receives information from a number of sources in the areas technology, security agencies, police force and industry, some of which is not available to the business community. The established and approved contacts to other government agencies and to international partners are also used to generate the national IT security situational picture.

The IT security situational picture is a clear summary and evaluation of the current IT security situation in Germany and also offers an analysis of the situation, perhaps with regard to the need for action and possible courses of action. It is addressed to the heads of the agencies or the management with a focus on the IT security management (CISO).

The BSI is characterised by a broad base of expertise and specialist departments in IT security, making its professional resources available to the BSI IT Situation Centre for the preparation, evaluation and target group-appropriate provision of information. Due to the interaction of sources of information and the technical expertise of the BSI, the IT security report allows a far more comprehensive picture of the situation than can be gained through standard CERT reports. The additional content gained through condensing the information is incorporated into the IT security situational pictures.

The BSI IT Situation Centre also has the technical facilities to obtain information on the national IT security situation. These include a network of sensors for the detection of irregularities on the Internet.

The early crisis detection and crisis mitigation concept is a fundamental contribution on the part of the UP KRITIS partners, with a view to their preparing up-to-date IT security reports on the basis of sanitised and

condensed information on the IT security situation from commerce and industry. Having been amplified in this manner, the IT security report is made available to the UP KRITIS partners.

A continual stream of information extending beyond the IT security situational picture is disseminated in crisis management, as are technical appraisals on the current IT situation. The BSI IT Situation Centre issues recommendations regarding actions to take, facilitates communications between the parties involved, and coordinates crisis mitigation.

The BSI IT Situation Centre is the central point of contact in the mitigation of IT crises. Alerts are forwarded to the private sector and government agencies as quickly as possible. The BSI IT Situation Centre is available and ready for action 24/7. It has the resources to provide additional personnel and professional expertise in the event of an IT crisis.

Interfaces

The BSI IT Situation Centre communicates with the companies via the SPOCS set up in the various sub-sectors. It is also the interface between the companies and the government crisis task force.

The national IT security situational picture is made available to the companies via the SPOCs. Conversely, the SPOCs keep the BSI IT Situation Centre informed about the IT security situation in the companies.

The address list of all the SPOCs which have been set up is maintained by the BSI. The SPOC maintains and updates the contact address list for the companies in its sub-sector.

2.4 Communications platform for informal information exchange

The parties involved in UP KRITIS have set up a regular information exchange initiative which functions on an informal basis regardless of crises and including situations which do not involve early crisis detection and mitigation processes. A joint communications platform is also being set up which will provide the facility to share confidential information about developments and trends relevant to the national IT security situation.

Two of the objectives of the communications initiative are to set up a platform to encourage the development of possible solutions and to share examples of best practice with regard to early crisis detection and mitigation.

Those taking part in the communications should be experts on IT security issues in their sub-sector. They should be able to facilitate discussion of problems specific to their sub-sector, possibly in a workshop setting, conveying the issues in an appropriate fashion to their counterparts outside the industry.

Those participating in the communications can be drawn from a wider circle than the parties involved in UP KRITIS. The communications platform can be subdivided into interest groups with a varying cast of professionals depending on the subject matter. Interest groups are free to meet on their own as the need arises. Regular and consistent attendance with minimum turnover of staff is important for building trust among those participating and working together.

In contrast to the SPOCs, the communications platform has no operational role in early crisis detection and mitigation. Given its remit, therefore, the communications platform need only be available by arrangement. The heads of the working groups organise and manage the communications platform.

2.5 Other communication structures

Society as a whole, government institutions, sectors of industry and individual companies can be affected by crises with a variety of causes and effects. The processes and structures which have been put in place to mitigate crises but do not relate to IT systems are not covered in this document and are not substituted by the structures set out in this document, which are only relevant to IT crises.

Due to Germany's federal structure, there will remain various responsibilities for early crisis detection and mitigation on different administrative levels. However, nationwide and interstate exercises which embrace trade and industry (e. g. LÜKEX) will continue to optimise the interaction among those participating.

3 Early crisis detection and mitigation processes

Operators of critical infrastructures need up-to-date and reliable information as well as high-quality analyses and evaluations in order to be able to detect crises at an early stage or to mitigate them, respectively, and yet still satisfy their corporate and business obligations. Informed decisions and effective action have to be based on the overall context of the respective situation already incorporating up-to-date and reliable information from a number of local viewpoints. This concept of early crisis detection and mitigation provides those involved in UP KRITIS well-defined processes for communications and for appropriate decisions about responsibilities and operations.

If all those involved actively implement and follow the processes outlined below, this will guarantee that measures can be taken in good time to avert or to mitigate crises. All those involved are therefore advised to use the processes set out below for early crisis detection and mitigation. The extensive implementation of processes, cross-sector communications and the involvement of the BSI IT Situation Centre can be instrumental to the effective early detection and mitigation of crisis situations for the critical IT infrastructures used in Germany. Training and validation of the processes outlined in this document are targeted by the concept “IT Emergency and Crisis Exercises in Critical Infrastructures”.

The following sections introduce the basic process principles before illustrating the early crisis detection and mitigation processes. The processes are then presented and explained in more detail in further sections.

3.1 Basics

Statuses

The processes described below are based on the following statuses:

- IT security situation assessment (green)
- Early crisis detection (amber)
- Alert/crisis mitigation (red)

These statuses can be allocated to companies, SPOCs and the BSI IT Situation Centre. Each status is assigned a traffic light colour – red, amber or green – reflecting the acuteness of the situation. The IT security situation assessment status (green) signals a normal level of observation outside any crisis, whereas the early crisis detection status (amber) is marked by increased alertness, triggered by incidents extending beyond events normally observed and indicating a potential IT crisis. The alert / crisis mitigation status (red) triggers a response whereby, on the basis of an alert ahead of an IT crisis which might still be avoidable, measures are taken to avert the imminent crisis or to mitigate the crisis situation which is already acute.

General overview of processes

The early crisis detection and mitigation processes are illustrated below in Figure 1 – Figure 3:

Figure 1: Statuses in UP KRITIS communications

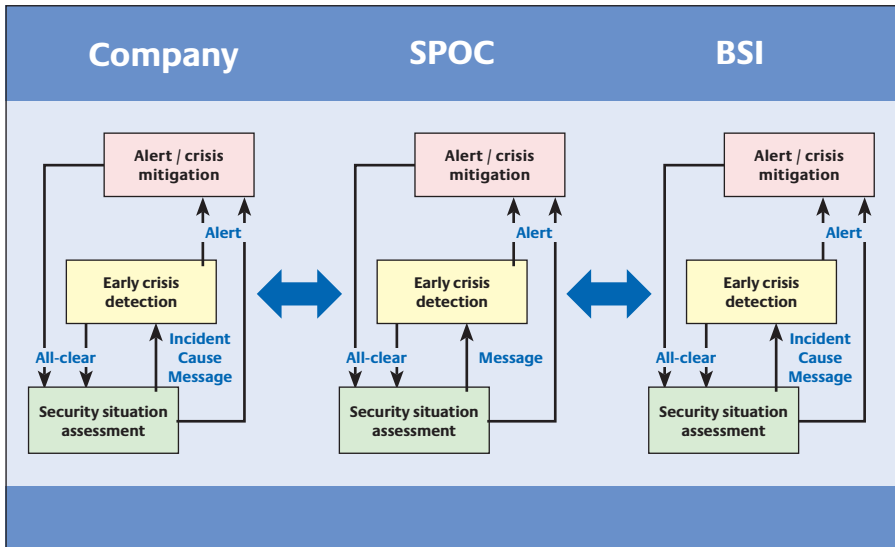


Figure 2: Lines of communication from companies to the BSI via SPOCs

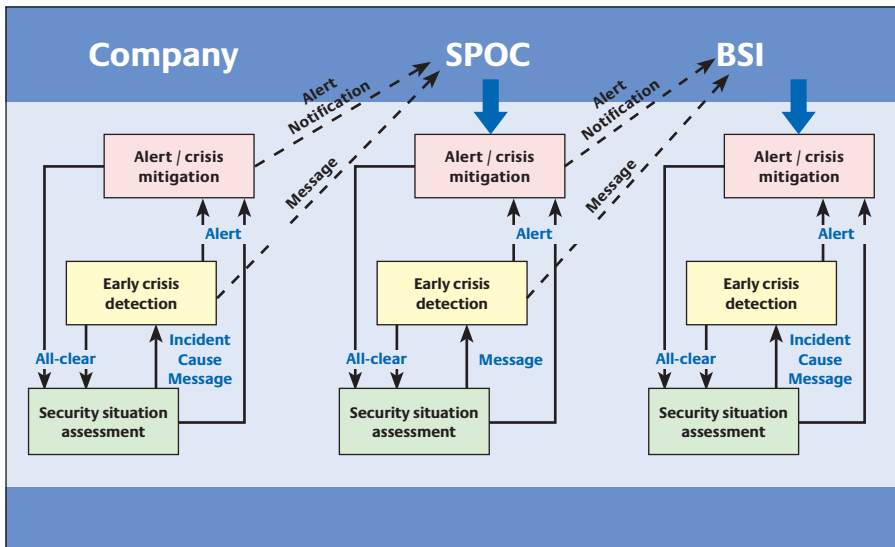
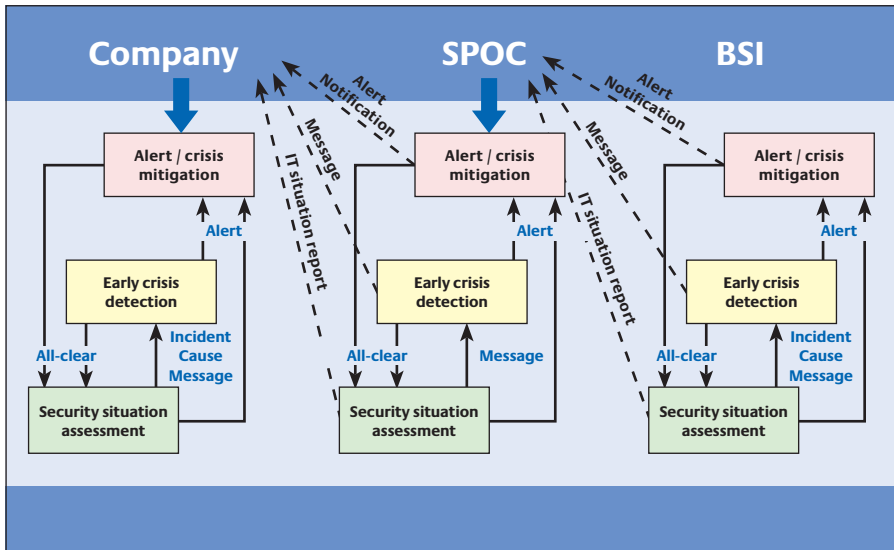


Figure 3: Lines of communication from the BSI to companies via SPOCs



The coloured boxes depict the statuses and indicate the operations and tasks associated with the respective status. The continuous lines indicate transitions from one status to another as a result of events and decisions in the companies, SPOCs and the BSI IT Situation Centre. The dashed lines show the flow of communications between the communication partners.

The status transition in the companies may be associated with a transfer of responsibility to other members of staff or functions in the company. Companies, SPOCs and the BSI IT Situation Centre cannot presume to know the current status of another unit as this can change at any time due to external events or internal processes.

Information on the IT security situation

The tasks undertaken by companies, SPOCs and the BSI IT Situation Centre are based on information on the IT security situation which the organisations acquire through their external sources of information or as a result of their own internal operations.

Information which can be reported to the outside world or may come in from the outside world can be of the following types:

- Information on the IT security situation
- Alerts by companies, SPOCs or the BSI IT Situation Centre
- Information about the company's own status to other organisations
- All-clears after an alert or after a crisis has subsided.

If a piece of information on the IT security situation is reported, it should – to the greatest possible extent – be given attributes for the purpose of its evaluation. These include:

- Consequences (none, for companies, for the [sub]-sector, across sectors)
- Circumstances (extent, probable duration, cause, trigger)
- Urgency.

General framework for information exchange

The general framework conditions in accordance with UP KRITIS with respect to handling, passing on and protection of information and the sources of information are as follows:

- The rapid transmission of information always takes priority over its analysis and evaluation.
- Information is exchanged on a voluntary basis.
- The exchange of information is based on the belief and trust that the parties participating in communications will not suffer any repercussions as a result of reporting incidents.
- Sensitive information is treated confidentially by all those involved in order to minimise the risks associated with sharing the information. The so-called “Traffic Light Protocol” (TLP) is recommended as a system of indicators for the sensitivity of information. The colours denote the following different levels of sensitivity:

TLP Red: Information may only be exchanged within the group of persons present in a meeting and bound by the TLP. Documents may only be passed on by the recipient subject to the sender's consent.

TLP Amber: If it serves the purposes of the working group, members may pass on information to colleagues in their own organisations or to other organisations (e. g. consultants) (need-to-know principle).

TLP Green: Information may be passed on to other organisations but may not be published or released to the mass media.

TLP White: The information is not subject to any restrictions and may be passed on to anyone, including the mass media.

The protocol is laid down in a procedural policy to which the parties pledge their compliance.

- It is necessary to differentiate between urgency, importance and confidentiality requirements in order not to jeopardise the smooth flow of information. For example, an accumulation of messages from various sources about a particular circumstance can increase the urgency of the information without necessitating a heightened degree of confidentiality.

In exceptional cases the information which has to be transmitted may be classified. The information is then passed on as set out in the federal government's classified documents directive.

3.2 Security situation assessment

Today companies already observe the IT security situation in relation to their own interests. They have their own individual mechanisms for gathering, analysing and evaluating information, which allow an up-to-the-minute appraisal of the IT security situation.

The objective of the IT security situation assessment status (green) is to detect incidents which may indicate the development of a crisis or provoke a critical situation extending beyond an individual company as early as possible. The options for taking adequate protective measures es-

essentially depend on how early the developments are recognised and communicated. Information with the potential to impact on the IT security situation or indications of an IT crisis is therefore reported as promptly as possible to the BSI IT Situation Centre via the SPOCs. The BSI IT Situation Centre, in turn, acts as quickly as possible to provide the companies with information on the IT security situation.

The SPOC is on standby to communicate and respond in a crisis relating to the IT security situation. It does not issue any IT security reports of its own but communicates and coordinates.

If, in the context of diagnosing the IT security situation assessment, an incident is detected which is indicative or suggestive of an IT crisis, the company or the BSI IT Situation Centre enters into the early crisis detection process. This can also be produced by a message sent via the SPOC, e. g. an IT security situational pictures issued by the BSI warning of an acute situation.

3.3 Early crisis detection

Companies

Early crisis detection is a process whereby a company analyses and evaluates a message about the IT security situation which has been received or information which it has itself obtained in order to be able to decide what action to take next. If an IT crisis is looming or impending, the company will alert the SPOC or the BSI IT Situation Centre as quickly as possible. Should the crisis materialise, the company will change to alert / crisis mitigation or, if the all-clear is sounded, return to normal operations and the IT security situation assessment status.

The rapid forwarding of information is crucial for the detection of incidents or events which indicate a potential IT crisis. Forwarding an item of information is always voluntary. As such, the person who is party to the information decides what to do with an item of information. The companies are guided by the following principles when deciding whether to pass on a piece of information:

- Information about any events which could develop into crises is relevant for the effective early detection of crises. It is therefore important to pass on information which may be indicative of crises rather than just information about crises which have already occurred.
- A piece of information may be irrelevant to the person who is party to it, but the same information may very well be of relevance to other operators of critical infrastructures. Persons sending information potentially decide whether a piece of information is worth reporting. This entails looking beyond the concerns of their own companies and considering, as far as they are able, the relevance of the information for other companies or sectors. Given their knowledge of their own sub-sectors, the recipients of the information can assess the importance of that information for their companies or sectors.
- The senders act to the best of their knowledge and belief but cannot guarantee that the information is correct.
- Seen in isolation, a piece of information can be of minor importance but it can take on greater significance in the context of other pieces of information. For example, a disruption to operations which is insignificant for the purposes of the sector affected could develop into a full-blown IT crisis in connection with problems in other sectors.
- As a general principle, if there is any doubt as to whether a piece of information should be transmitted or not, it should always be forwarded.

SPOC

The SPOC receives information from the companies which it processes in accordance with its remit (see section 2.2 “Single Point of Contact [SPOC]”) and relays to the BSI IT Situation Centre. Conversely, the SPOC receives IT security situational pictures from the BSI and sends them to the companies in its sub-sector. The SPOC moves into early crisis detection status if it receives information which indicates or signals an IT crisis. This information may have been received from companies in its sector or from the BSI.

The analysis and evaluation of information is of lesser importance than the rapid forwarding of the information to the companies in its sector or to the BSI IT Situation Centre.

BSI IT Situation Centre

The BSI IT Situation Centre continually issues updated national IT security situational pictures and circulates them to various bodies including the SPOCs. In a manner analogous to the companies and the SPOCs, the BSI IT Situation Centre moves into early crisis detection mode if an incident or event is detected or reported which is indicative of an IT crisis.

3.4 Alerts and crisis mitigation

This present concept document shows how a rapid and coordinated communication process can be maintained in an IT crisis in order to limit damage and to allow a due response on the part of the companies and government bodies. It is not intended to be a set of specific procedural instructions.

Companies, SPOCs and the BSI IT Situation Centre raise an alert if an IT crisis is impending or has already occurred. They generally issue the alert at early crisis detection status if, for example, the analysis and evaluation of information confirm the evidence pointing to an IT crisis.

There need not be an actual crisis to issue an alert but there can be a quantifiable risk of a crisis occurring. An IT crisis might be able to be averted or its impact mitigated on the basis of the information communicated and the measures taken. The all-clear is given if an alert has been raised but an IT crisis has not manifested itself.

The BSI IT Situation Centre communicates with the SPOCs if an IT crisis is impending or has already occurred. There can, if the mitigation of the crisis so dictates, be direct communication between individual companies and the BSI IT Situation Centre. The SPOCs maintain communications with the companies in their sub-sector. The SPOCs also have the details of persons in the companies whom they can contact in the event of a crisis.

The assignment of crisis mitigation tasks will depend on the type, circumstances and potential effects of the IT crisis in any given case. When mitigating the crisis, the companies need information as to the courses of action which are open to them and those which are not. Recommendations for action issued by security specialists in the companies or from the BSI IT Situation Centre and communicated to the companies and SPOCs are

therefore of great benefit for the sub-sectors and the companies. Moreover, communications between companies and SPOCs, on the one hand, and those between SPOCs and the BSI IT Situation Centre, on the other hand, ensure that measures are in place to contain or overcome the IT crisis and these measures can be optimised.

Companies, SPOCs and the BSI IT Situation Centre keep each other informed about the progress being made in mitigating and ending the crisis, but mitigating the actual crisis takes priority over any such briefing processes.

3.5 Regular exchange of information

The exchange of information serves to refine possible solutions for early crisis detection and crisis mitigation. This might involve identifying problems and solutions and discussing examples of “good practice”. This is particularly useful in the crisis follow-up process where participants explore the “lessons learned”.

Solutions to problems worked out in the context of regular information-sharing sessions are conducive to a sustained approach as they enable a continual refinement of the early crisis detection and crisis mitigation concept.

Views on the implementation of the concept and its refinement are shared informally in the communications platform setting.

3.6 Summary in tabular form

Table 1: Parties, tasks and means of communication involved in the crisis management statuses

	Structures and parties involved	Tasks/ operations	Means of communication
Regular exchange of information	<ul style="list-style-type: none"> • BSI IT Situation Centre • Companies • SPOCs 	<ul style="list-style-type: none"> • Compare notes • Crisis follow-up (“lessons learned”) 	<ul style="list-style-type: none"> • Meeting • Telephone • Conference call • Fax • E-mail • Communication platform • Video conference
IT security situation assessment	<ul style="list-style-type: none"> • BSI IT Situation Centre • Companies 	<ul style="list-style-type: none"> • Assess situation • Prepare and circulate IT security situational picture 	<ul style="list-style-type: none"> • Telephone • Conference call • Fax • E-mail • Video conference
Early crisis detection	<ul style="list-style-type: none"> • BSI IT Situation Centre • Companies • SPOCs 	<ul style="list-style-type: none"> • Share information about IT security situation • Conduct analysis • Evaluate situation • Summarise information • Make decision • Alert • Sound the all-clear 	<ul style="list-style-type: none"> • SMS • Telephone • Conference call • Fax • E-mail • Video conference <p>High availability:</p> <ul style="list-style-type: none"> • Mobile communications • Satellite telephone
Alerts and crisis mitigation	<ul style="list-style-type: none"> • Contact person in company or SPOC (depending on crisis situation) • BSI IT Situation Centre and other crisis situation centres • Relevant disaster control squads where necessary (state level) 	<ul style="list-style-type: none"> • Provide recommendations • Execute crisis management • Coordinate countermeasures • Exchange information and recommendations • Coordination with other situation centres 	<ul style="list-style-type: none"> • SMS • Telephone • Conference call • Fax • E-mail • Pager • Video conference <p>High availability:</p> <ul style="list-style-type: none"> • Mobile communications • Satellite telephone

3.7 Communications technology

Multiple back-up systems have to be built into the communications technology in the interests of achieving the communications structure outlined in this concept for the early detection and mitigation of crises.

The following communication media are used:

- E-mail
- Telephone (several numbers) and
- Fax.

In case of elevated availability requirements the following may be used as a general rule:

- Mobile telephones
- Satellite telephones.

Checks should be made on the need for priority circuits in landline and mobile networks.

The working group will go on to review, evaluate and decide on the means of communication which are to be used. Regular tests will be conducted using the chosen means of communication. Reference in this regard may be made to the exercise concept prepared by the “Emergency and Crisis Exercises” working group.

4 Actual implementation and further procedures

This concept is scheduled to be adopted in live operations in January 2009. The BSI IT Situation Centre is already capable of functioning as required. The first SPOC structures have been set up and others are in the setup or conception phase.

The parties involved in UP KRITIS will start the regular exchange of information in January 2009. The plan is to hold three plenary sessions a year initially with activities continuing in the working groups. There are also plans to set up further sub-groups of Working Group 2 “Crisis Response and Mitigation”. The following tasks have already been identified and will be worked on by experts in two sub-groups.

1) Implementation and coordination:

This means the specification of concrete measures for the setting up of structures for early crisis detection and crisis mitigation processes. The content and format of messages are two of the elements requiring coordination.

2) Means of communication:

Use and, where applicable, development of appropriate procedures for confidential communications (e. g.: Chiasmus, ElcroDAT 6.2, Topsec, SINA, VPS, etc.) and for multiple redundant structures.

Working Group 4 (“National and International Collaboration”) will hold its meetings in association with these plenaries. Working Group 4 is tasked with liaising with the parties involved in UP KRITIS and coordinating the sharing of information at national and international level. The remit of Working Group 4 evolved during the meetings of Working Group 2 in 2008 and is now set to continue. In order to support the exchange of communications on international operations, a technical platform will be set up which will act as a channel for the circulation of international documents bearing reference to CIIP and CIP. The technical development and initial configuration of this platform will be based on the specifications put forward by the working group.

The concept on the early detection and mitigation of crises will be evaluated after an appropriate period of time – allowing at least two years – and

will be further refined if necessary. This will involve interpreting the lessons learned in the simulation games and exercises and incorporating the results in an updated version of the concept.

Existing contacts between the UP KRITIS working groups also serve as a basis for a reciprocal exchange of experience and for the incorporation of the concept in exercises planned by Working Group 1. As they continue with their work, the members of Working Groups 1 and 4 will seek to create the foundation for future participation in interstate/international exercises and simulation games exploring aspects of IT.

Annex

Abbreviations

24/7	Twenty-four hours a day and seven days a week
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht [Federal Financial Supervisory Authority]
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [Federal Office of Civil Protection and Disaster Assistance]
BAK	Bundeskriminalamt [Federal Criminal Police Office]
BMI	Bundesministerium des Innern [Federal Ministry of the Interior]
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway]
BSI	Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security]
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
IT	Information technology
KRITIS	Kritische Infrastrukturen [Critical Infrastructures]
LÜKEX	Länderübergreifende Krisenmanagement Exercise [Interstate crisis management exercise]
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen [National Plan for Information Infrastructure Protection]
SPOC	Single Point of Contact
TLP	Traffic Light Protocol
UP	Umsetzungsplan [Implementation Plan]
UP KRITIS	Umsetzungsplan KRITIS [CIP Implementation Plan]

Glossary

- BSI IT Situation Centre** The BSI IT Situation Centre has a reliable overview of the current IT security situation in Germany at all times and is thus able to make a rapid and competent assessment of the need for action and the possible courses of action in the event of IT security incidents both at government level and in commerce. It guarantees a rapid response to serious incidents in order to enable opportune countermeasures to be taken and largely avert loss or damage.
- Crisis** An abnormal situation which develops suddenly or gradually and which carries the inherent threat of injury to life and limb and has the potential to cause damage to major material assets and to seriously threaten the political, social or economic system, and one which necessitates a decision – often from a position of uncertainty without being in possession of the full facts.
- Crisis mitigation** The taking of measures aimed at resolving an acute crisis, minimising its repercussions, and restoring things to normality as quickly as possible.
- Crisis management** Creation of the conceptual, organisational and procedural prerequisites required to manage the abnormal situation which has arisen and restore things to normality as quickly as possible.
- Crisis prevention** All measures aimed at preventing incidents which have the potential, on their own or together, to wreak effects of crisis proportions.

Critical infrastructure Critical infrastructures are organisations and facilities of strategic importance for the community, the failure or disruption of which would result in long-term supply shortages, major disturbances in public security or other dramatic consequences.

In Germany the following areas are classed as critical infrastructure:

- Transport and traffic (aviation, maritime shipping, railways, local transport, inland waterway transport, roads, postal service)
- Energy (electricity, nuclear power plants, mineral oil, gas)
- Hazardous substances (chemicals and biological substances, hazardous materials transportation, armaments industry)
- Information technology and telecommunications
- Finance, banking and insurance (banks, insurance companies, financial service providers, stock exchanges)
- Supply systems (health service, emergency and rescue services, disaster control, food and water supply, waste disposal)
- Public authorities, government and the judiciary (government institutions)
- Other (media, large research institutions, prominent or highly symbolic buildings, cultural assets)

Early crisis detection The detection and reporting of incidents which can, on their own or together, cause or indicate developments of crisis proportions. Early crisis detection is part of crisis prevention.

Federal Administration Federal departments and their institutions and agencies, e. g. BSI, BKA, BBK, BNetzA, BaFin (cf. Article 86 of the German Constitution).

Information infrastructure

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

IT crisis

An IT crisis is said to exist in the context of UP KRITIS if organisations and facilities of importance for the general public experience or might experience failure or disruption directly or indirectly related to IT, which results in long-lasting supply shortages, major disruptions to public security or other dramatic consequences.

IT security

IT security denotes a status in which the availability, integrity and confidentiality of information and information technology are protected by appropriate safeguards.

Operators of critical infrastructures

Operators of critical infrastructures are private enterprises or public authorities which provide services in the critical infrastructures.

Sanitisation

Sanitisation is the term used to denote the process whereby classified items of information are filtered out of messages. The aim of sanitisation is to protect the legitimate interests of those sharing information if the relevant information is received simultaneously.

SPOC

Single Point of Contact. Firmly established function in a sub-sector acting as a central communications platform and reporting point (outgoing and incoming) for the companies in the sub-sector.

UP KRITIS partners	All the public authorities, stakeholder groups / business associations, companies, etc. which work together (e. g. in working groups) and participate in exercises in the context of the UP KRITIS.
UP KRITIS collaboration	Adoption of the concepts as well as tests and execution of the processes set out in the NPSI and the UP KRITIS by the operators of critical infrastructures and the Federal Administration.

References

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Nationaler Plan zum Schutz der Informationsinfrastrukturen [National Plan for Information Infrastructure Protection]. Berlin, 2005

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen [CIP Implementation Plan of the National Plan for Information Infrastructure Protection]. Berlin, 2007

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Schutz Kritischer Infrastrukturen – Basisschutzkonzept [Protection of Critical Infrastructures – Baseline Protection Concept]. Berlin, 2005

Participating UP KRITIS partners

Allianz Deutschland AG

Arcor AG & Co. KG

Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] (BSI)

Bundesanstalt für Finanzdienstleistungsaufsicht [Federal Financial Supervisory Authority] (BaFin)

Bundesverband deutscher Banken [Association of German Banks]

Commerzbank AG

Deutsche Bank AG

Deutsche Börse Group

Deutsche Bundesbank

Deutsche Postbank AG

Deutsche Telekom AG

DFS Deutsche Flugsicherung GmbH

Dresdner Bank AG

eco e. V. – Verband der Deutschen Internetwirtschaft [eco – Association of the German Internet Industry]

(E-Plus Group) E-Plus Mobilfunk GmbH & Co KG

European Central Bank

Gesamtverband der Deutschen Versicherungswirtschaft e. V. [German Insurance Association]

HUK-COBURG

Mineralölwirtschaftsverband [Association of the German Petroleum Industry]

RWE Aktiengesellschaft

RWE Energy Aktiengesellschaft

SIZ Informatikzentrum der Sparkassenorganisation GmbH

Telefónica O2 Germany GmbH & Co. OHG

Vodafone D2 GmbH

Imprint

Published by:

Bundesministerium des Innern
Alt-Moabit 101 D, 10559 Berlin
www.bmi.bund.de

Edited by:

Arbeitsgruppenleitung UP KRITIS, Geschäftsstelle UP KRITIS
(Bundesamt für die Sicherheit in der Informationstechnik)

Design and production:

MEDIA CONSULTA Deutschland GmbH

Status:

December 2008