



Bundesministerium
des Innern

Nationaler Plan

zum Schutz der
Informationsinfrastrukturen
Umsetzungsplan KRITIS



Früherkennung und Bewältigung von IT-Krisen

Umsetzungsplan KRITIS
Arbeitsgruppe 2
„Krisenreaktion und -bewältigung“

www.bmi.bund.de

Vorwort

Spätestens mit den Terrorangriffen in New York, Madrid und London wurde die Verwundbarkeit moderner industrieller Infrastrukturen der Weltöffentlichkeit vor Augen geführt. Natürlich gab es auch vor dem 11. September 2001 Angriffe auf verschiedenste Lebensadern hoch entwickelter Industrie- und Dienstleistungsgesellschaften; erinnert sei an die Giftgasangriffe in Tokio im Frühjahr 1995. Jedoch rückte der Stellenwert funktionierender Verbindungswege, Versorgungsstränge, Kommunikationskanäle etc. – kurz: Infrastrukturen – erst nach New York auch Nichtexperten ins Bewusstsein.

In Deutschland ist ein wichtiges Ergebnis dieser neuen Entwicklung die durch Staat und Wirtschaft gemeinsam getragene Vorgehensweise zur Sicherung von gesamtgesellschaftlich relevanten Infrastrukturen. Diese Vorgehensweise nach dem Public Private Partnership-Modell (PPP-Modell) hat sich gegenüber getrenntem staatlichen und privatwirtschaftlichen Handeln als langfristig erfolgreicher herausgestellt, steht doch als Ergebnis eine von beiden Seiten goutierte und somit auch in Krisensituationen belastbare Vorgehensweise.

Zum Erkenntnisgewinn des gemeinsamen Handelns hat auch die Tatsache beigetragen, dass der Schutz vitaler Infrastrukturen unserer Gesellschaft nur innerhalb des jeweiligen Sektors betrieben wurde. Es hat sich jedoch gezeigt, dass der gemeinsame, arbeitsteilige Ansatz der Sicherung von Kritischen Infrastrukturen (KRITIS) die beste Chance bietet, diese auch in Krisenzeiten in den Dienst der Bevölkerung stellen zu können. Natürlich legte sich der PPP-Ansatz nicht über Nacht wie Tau über den kritischen Strukturacker, ganz im Gegenteil bedurfte es der breiten Überzeugungsarbeit an vielen Fronten, bis schlussendlich die Saat aufgehen konnte.

Das verbindende Element der wachsenden KRITIS-Gemeinschaft ist der im Juni 2005 durch die Bundesregierung beschlossene „Nationale Plan zum Schutz der Informationsinfrastrukturen“ (NPSI). Dieser Plan fungiert als Referenzrahmen für Informationsinfrastrukturen, der das strategische Vieleck zu deren Schutz aufspannt. Bereits im August 2005 wurde vom Bundesministerium des Innern (BMI) als physisches Pendant zum NPSI das Basisschutzkonzept „Schutz Kritischer Infrastrukturen“ als Empfehlung für Unternehmen herausgegeben. Anfang 2006 wurden dann die Arbeiten am Umsetzungsplan KRITIS (UP KRITIS) aufgenommen. Nach der Veröf-

fentlichung des Plans im September 2007 fingen die Arbeiten der praktischen Auskleidung des theoretischen Umsetzungsplans an, deren Ergebnis bezüglich der Früherkennung und Bewältigung von IT-Krisen mit dem vorliegenden Dokument vorgestellt wird.

Inhalt

1	Einleitung und Motivation	5
2	Beteiligte Organisationen	10
2.1	Unternehmen	10
2.2	Single Point of Contact (SPOC)	12
2.3	IT-Lagezentrum des Bundesamtes für die Sicherheit in der Informationstechnik (BSI)	14
2.4	Kommunikationsplattform zum informellen Informationsaustausch	16
2.5	Sonstige Kommunikationsstrukturen	17
3	Prozesse zur Krisenfrüherkennung und Krisenbewältigung	18
3.1	Grundlagen	19
3.2	Sicherheitslagefeststellung	23
3.3	Krisenfrüherkennung	24
3.4	Alarmierung und Krisenbewältigung	26
3.5	Regelmäßiger Informationsaustausch	27
3.6	Zusammenfassende tabellarische Übersicht	28
3.7	Kommunikationstechnik	29
4	Konkrete Umsetzung und weiteres Vorgehen	30

Anhang	32
Abkürzungen	33
Glossar	34
Literaturverzeichnis	38
Beteiligte UP-KRITIS-Partner	39

Abbildungen

Abbildung 1: Zustände in der Kommunikation des UP KRITIS	20
Abbildung 2: Kommunikationsfluss von Unternehmen über SPOCs an das BSI	20
Abbildung 3: Kommunikationsfluss vom BSI über SPOCs an Unternehmen	21

Tabellen

Tabelle 1: Beteiligte, Aufgaben und Kommunikationsmittel in den Zuständen des Krisenmanagements	28
--	-----------

1 Einleitung und Motivation

Die Bedeutung von Kritischen Infrastrukturen liegt vor allem in den Dienstleistungen, die für eine moderne Industriegesellschaft unverzichtbar sind. Die Verfügbarkeit der Dienstleistungen hängt in zunehmend starkem Maße vom Funktionieren der Informationsinfrastruktur ab. Die Informationstechnik (IT) ist heute zum Betrieb sowie zur Steuerung und Überwachung von Prozessen weitestgehend unverzichtbar. Bestehende Abhängigkeiten voneinander über die Grenzen von Branchen und Sektoren hinweg werden durch die gemeinsame Nutzung von Internet und Telekommunikationsnetzen noch verstärkt.

Die Bundesregierung hat diese Entwicklung zum Anlass genommen, den „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI)¹ als übergreifende IT-Sicherheitsstrategie des Bundes zu verabschieden. Der NPSI betont den Schutz der Informationsinfrastrukturen als gesamtgesellschaftliche Aufgabe, die ein abgestimmtes und von allen Verantwortlichen unterstütztes Vorgehen erfordert. Angesprochen sind hier insbesondere die Bundesverwaltung und die Betreiber Kritischer Infrastrukturen.

Bereitstellung und Betrieb von Kritischen Infrastrukturen erfolgen in Deutschland größtenteils in privatwirtschaftlicher Verantwortung, das heißt in der Verantwortung einzelner Unternehmen. IT-Sicherheit war bisher dementsprechend eine Aufgabe, die weitestgehend innerhalb einzelner Unternehmen und Organisationen wahrgenommen wurde. Diese Zuständigkeiten bleiben unberührt, müssen aber um unternehmens- und branchenübergreifende Komponenten ergänzt werden.

In Übereinstimmung mit dem NPSI haben Wirtschaft und Bundesregierung den Umsetzungsplan Kritische Infrastrukturen (UP KRITIS)¹ erarbeitet, der vom Bundeskabinett am 5. September 2007 verabschiedet wurde. Ein Ergebnis des UP KRITIS sind Empfehlungen zur Prävention und Reaktion auf Krisen, die maßgeblich durch Ausfall oder Einschränkung der IT bedingt sind. Diese werden nachstehend als IT-Krisen bezeichnet.

¹ Verfügbar unter www.bmi.bund.de.

Es ist nicht ausgeschlossen, dass eine IT-Krise ihren Ursprung außerhalb der IT hat und beispielsweise infolge eines natürlichen Ereignisses oder eines Ausfalls von Versorgungskapazitäten entsteht. Vorfälle außerhalb oder innerhalb der IT, die sich auf die IT auswirken, können wiederum Auslöser für weitere Vorfälle sein, die in ihrem Zusammenwirken für die IT-Infrastruktur krisenhafte Ausmaße annehmen. Für die Krisenfrüherkennung ist es daher erforderlich, alle Ereignisse zu beobachten und zu melden, die Auswirkungen auf die IT haben können, und die Beobachtung nicht auf Vorfälle innerhalb der IT zu beschränken.

Krisen verlaufen oft nicht kalkulierbar und beschränken sich nicht verlässlich vorhersagbar auf einzelne Unternehmen oder Branchen. Ihre frühzeitige Erkennung und Bewältigung ist aufgrund starker, aber nicht immer unmittelbar transparenter Abhängigkeiten den einzelnen Betroffenen unter Umständen gar nicht möglich. Erst der Informationsaustausch mit den richtigen Ansprechpartnern schafft die benötigte Transparenz und ermöglicht im Krisenfall wirkungsvolles Handeln. Schäden können nicht allein als unmittelbare Folge eines Auslösers, sondern vor allem auch durch späte und unzureichende Kommunikation im Vorfeld und während der Bewältigung der Krise entstehen.

Der NPSI und der UP KRITIS betrachten daher die Krisenfrüherkennung und -bewältigung vor allem als eine Herausforderung an die Kommunikation zwischen den Unternehmen und Organisationen unterschiedlicher Branchen und Sektoren, aber auch zwischen Organisationen und staatlichen Stellen.

Ziele des Dokuments

Die kommunikative Vernetzung ist damit die wichtigste Voraussetzung sowohl für die Früherkennung als auch für die Reaktion im Krisenfall. Deswegen sieht der UP KRITIS vor, dass ein Konzept zur Schaffung geeigneter Kommunikationsstrukturen gemeinsam von Experten aus Wirtschaft und Bundesverwaltung erstellt wird. Seit April 2007 haben sich ausgewiesene Fachleute intensiv mit den Grundlagen für eine branchenübergreifende, effektive Früherkennung und Bewältigung von Krisen von begrenztem bis zu nationalem Ausmaß befasst. Das vorliegende Dokument ist das Ergebnis dieser Arbeiten.

Fokussiert werden besonders die branchenübergreifenden Kommunikationsstrukturen und Prozesse, die von einem Regelaustausch, der IT-Lageanalyse über Warnung und Alarmierung bis zur koordinierten Krisenbewältigung reichen.

Es werden Anforderungen für die an der Kommunikationsstruktur beteiligten Organisationen in Hinblick auf Fähigkeiten, Schnittstellen und genutzte Kommunikationsmittel erarbeitet. Single Points of Contact (SPOCs) stehen im Mittelpunkt der Kommunikationsstruktur, um den Kommunikationsaufwand jedes einzelnen Beteiligten zu minimieren und die Kommunikationswege zu strukturieren. Im Konzept werden die für einen wirksamen Informationsaustausch erforderlichen Prozesse definiert, um alle beteiligten Kommunikationspartner miteinander zu verbinden.

Die geschaffene Kommunikationsstruktur ergänzt die bereits vorhandenen Einrichtungen und Regelungen in den Unternehmen, Branchen und in der Bundesverwaltung. Sie schafft die geeignete Grundlage dafür, dass zukünftig IT-Krisen im Verbund von Privatwirtschaft und dem nationalen IT-Lagezentrum beim Bundesamt für Sicherheit in der Informationstechnik (BSI) effektiv begegnet werden kann.

Die Gewinnung verlässlicher Informationen basiert auf einer übergreifenden Betrachtung, die aus einer Vielzahl lokaler Sichten zusammengesetzt ist. Erst durch den aktiven und gemeinschaftlichen Beitrag der Teilnehmer am UP KRITIS wird diese übergreifende Perspektive ermöglicht. Nur durch gemeinsames Handeln lässt sich ein realistisches und übergreifendes IT-Sicherheitslagebild erstellen, welches den beteiligten Unternehmen und Branchen zugutekommt, weil potenzielle Schäden durch frühzeitige und zielgerichtete Maßnahmen begrenzt werden können. Mit dem gemeinsamen Verständnis der Bedrohung ist darüber hinaus ein gut abgestimmtes Krisenmanagement möglich.

Bereits heute informieren sich Unternehmen innerhalb ihrer Branche über die Sicherheit ihrer IT-Infrastrukturen, da Schäden durch technische Abhängigkeiten zwischen den Unternehmen verstärkt werden können. Auch sind bereits erste Kommunikationsstrukturen, die in einem Krisenfall über die Grenzen des eigenen Unternehmens hinaus führen, etabliert. In Teilbereichen bestehen bereits brancheninterne Eskalations- und Meldewege, welche auch die zuständigen Behörden und Polizeien einbeziehen. Während also auf den Ebenen der Unternehmen und Organisationen sowie in einigen Branchen bereits geeignete Strukturen zur Krisenreaktion und

Krisenbewältigung bestehen, sind diese aus Sicht der Bundesregierung und der Betreiber Kritischer Infrastrukturen branchen- und sektorenübergreifend noch aufzubauen.

Im vorliegenden Konzept werden sowohl sektoren- als auch branchenübergreifende Strukturen und Prozesse beschrieben.²

Nutzen für die Unternehmen

Branchenübergreifend arbeiten Betreiber Kritischer Infrastrukturen und die Bundesregierung zur Krisenreaktion und -bewältigung an einer belastbaren Kommunikationsstruktur, die aus einem „Netzwerk des Vertrauens“ besteht und in der das BSI eine zentrale Rolle einnimmt. Das BSI steht als wettbewerbsneutrale staatliche Institution für den vertraulichen Umgang mit den empfangenen Informationen und sensiblen Daten. In dieser Kommunikationsinfrastruktur sollen Unternehmen und BSI sowohl Informationsgeber als auch Informationsempfänger sein. Gesetzliche Vorgaben, Datenschutzaspekte und die benötigte Vertrauenswürdigkeit werden bei der Etablierung der Kommunikationsinfrastrukturen berücksichtigt und sind eine unverzichtbare Grundlage der Zusammenarbeit.

Die Mitarbeit am UP KRITIS ist nicht nur ein Unternehmensbeitrag zur Stärkung des Wirtschaftsstandortes Deutschland, sondern liegt auch im Interesse der Anteilseigner, der Kunden und der Mitarbeiter des Unternehmens, da potenzielle Schäden aus IT-Krisen besser abgewendet oder zumindest gemindert werden können. Sie ist Bestandteil der Risikoversorge und steht damit im wirtschaftlichen Interesse eines Unternehmens.

Die Unternehmen können aufgrund der branchenübergreifenden Kommunikation frühzeitig über Informationen verfügen, die ihnen eine zusätzliche Vorlaufzeit zur Reaktion auf Vorfälle und für die Ergreifung von Maßnahmen verschaffen. Im Vorfeld einer IT-Krise oder während des Krisenmanagements können notwendige Maßnahmen, die möglicherweise kostenintensiv sind, auf Grundlage einer breiten und fundierten Kenntnis der IT-Sicherheitslage ergriffen werden.

² Eine textliche Differenzierung erfolgt nur im Fall tatsächlicher Unterschiede. Ansonsten wird von branchenübergreifender Kommunikation gesprochen.

Im Rahmen der Zusammenarbeit am UP KRITIS werden alle Unternehmen gleichberechtigt behandelt, damit gemeinsam und frühzeitig auf eine IT-Krise reagiert werden kann. Darüber hinaus sollen branchenübergreifend vertrauenswürdige und fachkompetente Ansprechpartner verfügbar sein, die Lösungen zur Bewältigung einer IT-Krise aufzeigen können. Die gemeinsame Terminologie erleichtert die branchenübergreifende Koordination im Krisenfall. Aber auch die Kosten in Bezug auf die Entwicklung von Lösungen zur Krisenfrüherkennung und -bewältigung lassen sich durch branchenübergreifenden Transfer von Know-how reduzieren. Gemeinsame Übungen verbessern zusätzlich die eigene Krisenreaktionsfähigkeit.

Aufgabenverteilung

Die Aufgabenverteilung kann folgendermaßen beschrieben werden: Die Unternehmen setzen Maßnahmen um, die der Kommunikation und der Weitergabe von Informationen dienen. SPOCs sorgen für den unternehmensübergreifenden Informationsaustausch mit dem BSI. Branchenübergreifend wird so kommuniziert, dass die von Unternehmen oder dem BSI gewonnenen Informationen zur Krisenfrüherkennung und -bewältigung über die SPOCs allen Beteiligten zur Verfügung stehen.

Die Teilnehmer der Arbeitsgruppe „Krisenreaktion und -bewältigung“ haben mit dem vorliegenden Dokument ein Konzept für eine Kommunikationsstruktur zur Krisenfrüherkennung und -bewältigung geschaffen und unterstützen dessen Umsetzung. Die auf der Grundlage dieses Dokuments eingerichteten Kommunikationsprozesse werden im Rahmen des durch die Arbeitsgruppe „Notfall- und Krisenübungen“ erarbeiteten Konzepts für Notfall- und Krisenübungen geprobt.

Nachhaltigkeit wird dadurch erreicht, dass unter Federführung des Bundesministeriums des Innern das Konzept fortgeschrieben und den sich ändernden Rahmenbedingungen angepasst wird.

2 Beteiligte Organisationen

In diesem Kapitel werden die an der Kommunikationsstruktur im Sinne des UP KRITIS beteiligten Organisationen und ihre Rolle im Rahmen eines branchenübergreifenden Informationsaustausches beschrieben. Bereits vorhandene Strukturen und konzeptionelle Ansätze werden dabei einbezogen. Beispiele hierfür sind das IT-Lagezentrum des BSI (BSI-Lagezentrum) sowie Einrichtungen in den Unternehmen, die den Grundgedanken des UP KRITIS bereits heute leben. Als neue verbindende Elemente werden Single Points of Contact beschrieben. Dadurch sind Unternehmen in der Lage, über einen SPOC mit dem BSI-Lagezentrum zu kommunizieren und dabei Informationen zur Krisenfrüherkennung und -bewältigung auszutauschen. Im Folgenden werden die Teilnehmer und deren Organisationen mit ihren jeweiligen Aufgaben und Aktivitäten, den dazu notwendigen Fähigkeiten, den Schnittstellen und den erforderlichen Kommunikationsmitteln beschrieben.

2.1 Unternehmen

Für die gesamte Wirtschaft ist IT-Sicherheit zur Aufrechterhaltung ihrer Geschäfts- und Produktionsprozesse unverzichtbar. Daher haben Unternehmen bereits heute geeignete Strukturen zur Krisenfrüherkennung und -bewältigung etabliert. Die Unternehmen besitzen darüber hinaus auch fundiertes Know-how zu ihrer Branche sowie über bewährte Kommunikationsmöglichkeiten. Damit verfügen sie über zentrale Fähigkeiten, die für eine effektive und effiziente, branchenübergreifende Umsetzung der Ziele des UP KRITIS unverzichtbar sind.

Fähigkeiten und Aufgaben

Die Unternehmen kennen grundsätzlich ihre eigene IT-Sicherheitslage. Sie haben Know-how zur fachlichen Analyse und Bewertung von Vorfällen hinsichtlich deren Kritikalität für das Unternehmen und können somit ihre IT-Sicherheitslage besonders gut beurteilen. Die Unternehmen nutzen dieses Know-how, um im Rahmen ihrer unternehmensinternen Sicherheitslagefeststellung Vorfälle zu erkennen und zu melden. Die Beurteilung, ob für ein Unternehmen eine Krise droht, kann dabei insbesondere auch aus der Bewertung von externen Informationen und deren Auswirkung für das Unternehmen erfolgen.

Die Unternehmen sollen unter Einbeziehung der bekannten Sachlage und in der Überzeugung, nach bestem Wissen und Gewissen zu handeln, dafür sorgen, dass Informationen zur IT-Sicherheitslage über den SPOC ihrer Branche an das BSI-Lagezentrum gelangen (vergleiche dazu Abschnitt 3.3). Umgekehrt sollen Unternehmen sicherstellen, dass vom SPOC bzw. vom BSI eingehende Informationen, insbesondere IT-Sicherheitslagebilder, den zuständigen Stellen im Unternehmen übermittelt werden. Entsprechende Regelungen hierzu sollen in die Organisations- und Prozessdokumentation der Unternehmen eingearbeitet werden. Die Weitergabe einer Information erfolgt stets freiwillig.

Unternehmen haben ein vitales Interesse an der Fähigkeit zu einer schnellen Reaktion im Krisenfall. Deshalb soll die Erreichbarkeit der Unternehmen für die SPOCs idealerweise an allen Tagen rund um die Uhr (24/7), mindestens jedoch während der branchenüblichen Arbeitszeiten, sichergestellt werden.

Schnittstellen

Unternehmen einer Branche tauschen oftmals Informationen zur IT-Sicherheitslage untereinander aus. Im Rahmen der Umsetzung des Konzepts richten sie darüber hinaus eine Kommunikationsschnittstelle zum SPOC der Unternehmensbranche ein, über den künftig Meldungen zur IT-Sicherheitslage weitergegeben werden und gegebenenfalls alarmiert wird.

Unternehmen, Großunternehmen und international agierende Konzerne können auch direkt mit dem BSI-Lagezentrum kommunizieren, insbesondere falls eine Branche keinen zentralen SPOC eingerichtet hat oder die Verfügbarkeit des SPOCs nicht in vollem Maße gegeben ist.

Es gibt Ansprechstellen in den Unternehmen zum Austausch von Informationen außerhalb der Krisenbewältigung. Im Fall einer IT-Krise ist es möglich, dass in Abhängigkeit von der konkreten Situation und Bedrohungslage die Verantwortung für die Kommunikationsführung mit IT-Bezug innerhalb des Unternehmens wechselt. Zur Aufrechterhaltung der Kommunikation ist es daher erforderlich, dass die jeweils zuständigen Unternehmenseinheiten dieses Konzept kennen und beachten. Bei einem Zuständigkeitswechsel sollen die Unternehmen ihre Kommunikationspartner über die Veränderung informieren. Die Unternehmen sind dafür verantwortlich, dem SPOC Änderungen der Kontaktdaten zeitnah zu melden.

2.2 Single Point of Contact (SPOC)

Für die Früherkennung und Bewältigung von IT-Krisen ist es unerlässlich, dass die Betreiber Kritischer Infrastrukturen und das BSI-Lagezentrum miteinander kommunizieren. Ein bilateraler Informationsaustausch zwischen allen Unternehmen und dem BSI-Lagezentrum ist aufgrund der großen Anzahl an Unternehmen nicht praktikabel. Deshalb dient der in den einzelnen Branchen zu etablierende SPOC als Meldestelle und als Bindeglied zwischen Unternehmen und dem BSI-Lagezentrum. Der SPOC ist eine fest etablierte Funktion der Branche und kann dabei auch in einem Unternehmen angesiedelt sein.

Ein SPOC soll grundlegende technische und organisatorische Fähigkeiten besitzen, über möglichst alle einsetzbaren Kommunikationsmittel verfügen und aufgrund der Informationen aus den Unternehmen die aktuelle IT-Sicherheitslage seiner Branche kennen. Die Unternehmen haben zu dem SPOC ihrer Branche ein ausgereiftes und belastbares Vertrauensverhältnis.

Die zentrale Aufgabe des SPOCs ist die schnelle, unverfälschte und zuverlässige Weiterleitung von Informationen und die Alarmierung der Unternehmen der eigenen Branche bzw. des BSI-Lagezentrums.³ Der SPOC zeichnet sich daher durch eine hohe Reaktionsgeschwindigkeit aus, die sowohl bei der Krisenfrüherkennung als auch bei einer Alarmierung zum Tragen kommt.

Wünschenswert sind Branchen-Know-how sowie branchenspezifische IT-Sicherheitskompetenz, die den SPOC beispielsweise befähigt, branchenfremden Personen Meldungen aus seiner Branche zu erklären. Jedoch muss der SPOC keine eigene IT-Sicherheitslagefeststellung durchführen und daher nicht unbedingt selbst über ausgeprägte technische Expertise und Know-how in der Analyse und Bewertung von Vorfällen verfügen.

Der SPOC sollte gegebenenfalls gleichartige Meldungen aus verschiedenen Unternehmen seiner Branche vor der Weiterleitung verdichten und damit den Informationsfluss auf Branchenebene bündeln.

Falls vom Meldenden angefordert, bereinigt der SPOC Meldungen vor ihrer Weiterleitung von schutzbedürftigen Informationsanteilen. Vom meldenden Unternehmen müssen dazu die entsprechenden Bestandteile

³ Das vorliegende Konzept begründet aber keine Meldeverpflichtung für den SPOC.

kenntlich gemacht werden. Ziel dieser als Sanitarisierung bezeichneten Maßnahme ist die Wahrung der berechtigten Schutzinteressen der am Informationsaustausch Beteiligten bei gleichzeitigem Erhalt der relevanten Informationen. Nicht zuletzt aus diesem Grund ist die Effizienz des SPOCs davon abhängig, dass er das Vertrauen der Unternehmen seiner Branche genießt.

Im Rahmen des Krisenmanagements kann der SPOC ferner eine Koordinierungsfunktion in der Kommunikation zwischen den Unternehmen seiner Branche übernehmen und sich beispielsweise an der Abstimmung von unternehmensübergreifenden Maßnahmen innerhalb seiner Branche beteiligen.

Das Unternehmen, das die Funktion des SPOCs für eine Branche übernimmt, sollte während der Krisenbewältigung zusätzliche Ressourcen bereitstellen können. In Betracht kommen insbesondere zusätzliche Expertise oder organisatorische Unterstützung.

Da einzelne SPOCs in der Anfangsphase der Konzeptumsetzung unter Umständen noch nicht vollständig einsatzfähig sind, sind Entwicklungsstufen für seine Etablierung zweckmäßig. In der Errichtungsphase wird deswegen übergangsweise noch das Erfordernis nach direkter Kommunikation der Unternehmen mit dem BSI-Lagezentrum bestehen. Ein SPOC kann sich zunächst auf die Weiterleitung von Informationen beschränken, während später die Fähigkeit zur Bewertung und Analyse hinzukommen kann. Priorität hat jedoch stets die schnelle und unverfälschte Weiterleitung von Informationen.

Da der SPOC auch Meldungen zur Krisenfrüherkennung und Alarmierung weiterleitet, soll er an sieben Tagen in der Woche rund um die Uhr (24/7) erreichbar und sofort reaktionsfähig sein. Da im Krisenfall möglicherweise Ausfälle von Kommunikationssystemen den Informationsaustausch behindern, soll er über die in Abschnitt 3.6 aufgeführten Kommunikationsmöglichkeiten verfügen.

Schnittstellen

Alle SPOCs verfügen über Schnittstellen zum BSI-Lagezentrum und zu möglichst hochverfügbaren Ansprechpartnern in den Unternehmen ihrer Branche. Der SPOC ist Meldestelle für die Unternehmen einer Branche, in dem er Informationen aufnimmt, die an ihn herangetragen werden und

diese an die Unternehmen oder zum BSI weiterleitet. Für das BSI ist der SPOC vorrangiger Ansprechpartner für die Branche.

Der SPOC pflegt die Adressliste der Ansprechstellen in den Unternehmen seiner Branche. Das BSI pflegt die Adressliste aller SPOCs. Die SPOCs sind dafür verantwortlich, dem BSI Änderungen der Kontaktdaten zeitnah zu melden.

2.3 IT-Lagezentrum des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Um den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können, wurde das nationale IT-Lagezentrum des BSI (BSI-Lagezentrum) eingerichtet.

Fähigkeiten und Aufgaben

Das BSI-Lagezentrum erhält Informationen aus einer Vielzahl von Quellen der Bereiche Technik, Sicherheitsbehörden, Polizei und Wirtschaft, die teilweise der Privatwirtschaft nicht zur Verfügung stehen. Die etablierten und bewährten Kontakte zu anderen Regierungsstellen und zu internationalen Partnern werden ebenfalls zur Erstellung des nationalen IT-Sicherheitslagebildes genutzt.

Das IT-Sicherheitslagebild fasst die aktuelle IT-Sicherheitslage in Deutschland kurz und übersichtlich zusammen und bewertet diese unter anderem auch im Hinblick auf Handlungsbedarf und Handlungsoptionen. Angesprochen wird die Zielebene der Amtsleitungen bzw. des Managements, insbesondere das IT-Sicherheitsmanagement (CISO).

Das BSI zeichnet sich durch eine breit angelegte und in den Fachabteilungen spezialisierte IT-Sicherheitskompetenz aus, die dem BSI-Lagezentrum zur Aufbereitung, Bewertung und der zielgruppengerechten Bereitstellung von Informationen zur Verfügung steht. Aufgrund des Zusammenwirkens von Informationsquellen und technischer Kompetenz des BSI kann ein erheblich über typische CERT-Meldungen hinausgehendes IT-Sicherheitslagebild gewonnen werden. Der inhaltliche Zugewinn, der sich durch Verdichtung ergibt, fließt als Information in das IT-Sicherheitslagebild ein.

Das BSI-Lagezentrum verfügt außerdem über technische Möglichkeiten zur Gewinnung von Informationen zur nationalen IT-Sicherheitslage. Dazu gehört unter anderem ein Sensornetz zur Erfassung von Unregelmäßigkeiten im Internet.

Das Konzept zur Krisenfrüherkennung und -bewältigung ist ein wesentlicher Beitrag der UP-KRITIS-Partner, um mit sanitarierten und verdichteten Informationen zur IT-Sicherheitslage aus der Wirtschaft die Erstellung von aktuellen IT-Sicherheitslagebildern zu unterstützen. Das so erweiterte IT-Sicherheitslagebild wird den UP-KRITIS-Partnern zur Verfügung gestellt.

Im Krisenmanagement werden über das IT-Sicherheitslagebild hinaus kontinuierlich Informationen und technische Einschätzungen zur aktuellen IT-Lage verteilt. Das BSI-Lagezentrum stellt Handlungsempfehlungen bereit, unterstützt die Kommunikation zwischen den Beteiligten und koordiniert die Krisenbewältigung.

Das BSI-Lagezentrum ist zentraler Ansprechpartner bei der Bewältigung von IT-Krisen. Alarmierungen werden schnellstmöglich an Wirtschaft und Regierungsstellen weitergeleitet. Das BSI-Lagezentrum ist an sieben Tagen in der Woche rund um die Uhr (24/7) erreichbar und reaktionsfähig. Die Ressourcen können für den Fall einer IT-Krise in Personalstärke und Fachkompetenz erweitert werden.

Schnittstellen

Das BSI-Lagezentrum kommuniziert mit den Unternehmen über die in den Branchen geschaffenen SPOCs. Es ist auch Schnittstelle der Unternehmen zu den staatlichen Krisenstäben.

Das nationale IT-Sicherheitslagebild wird den Unternehmen über die SPOCs zur Verfügung gestellt. Umgekehrt erhält das BSI-Lagezentrum über die SPOCs Informationen zur IT-Sicherheitslage in den Unternehmen.

Die Adressliste aller etablierten SPOCs wird vom BSI gepflegt. Der SPOC pflegt die Adressliste der Ansprechstellen in den Unternehmen seiner Branche.

2.4 Kommunikationsplattform zum informellen Informationsaustausch

Die Teilnehmer am UP KRITIS haben einen regelmäßigen Informationsaustausch initiiert, der unabhängig von Krisensituationen, also auch außerhalb von Krisenfrüherkennung und Krisenbewältigung, auf informeller Basis erfolgt. Dazu wird eine gemeinsame Kommunikationsplattform etabliert, durch welche die Möglichkeit zum vertraulichen Informationsaustausch über Entwicklungen und Tendenzen im Hinblick auf die nationale IT-Sicherheitslage angeboten wird.

Im Rahmen der Kommunikationsplattform soll unter anderem die Entwicklung von Lösungsmöglichkeiten und der Austausch von „Good Practices“ zur Krisenfrüherkennung und Krisenbewältigung gefördert werden.

Die Teilnehmer an der Kommunikationsplattform sollen Experten für IT-Sicherheitsbelange ihrer Branche sein. Sie sollen in der Lage sein, Probleme ihrer Branche in geeigneter Form branchenfremden Teilnehmern, beispielsweise im Rahmen von themenspezifischen Workshops, zur Diskussion zu stellen.

Der Teilnehmerkreis der Kommunikationsplattform ist nicht auf die am UP KRITIS Beteiligten beschränkt. Die Kommunikationsplattform kann thematisch in Interessengruppen gegliedert werden und durch unterschiedliche Fachleute je nach Themenstellung besetzt sein. Interessengruppen können sich frei und nach Bedarf in eigener Regie treffen. Durch eine kontinuierliche Teilnahme mit geringer Fluktuation der teilnehmenden Personen wird die wichtige Vertrauensbildung bei der Zusammenarbeit gefördert.

Die Kommunikationsplattform hat anders als die SPOCs keine operative Rolle in der Krisenfrüherkennung und Krisenbewältigung. Die mit der Kommunikationsplattform verbundene Aufgabenstellung macht daher nur eine Erreichbarkeit nach Absprache erforderlich. Die Leiter der Arbeitsgruppen organisieren geschäftsführend die Kommunikationsplattform.

2.5 Sonstige Kommunikationsstrukturen

Die Gesellschaft, staatliche Einrichtungen, Branchen und einzelne Unternehmen können von Krisen unterschiedlicher Ursachen und Auswirkungen betroffen sein. Die zur Bewältigung von Krisen ohne IT-Bezug etablierten Prozesse und Strukturen werden hier nicht behandelt und durch die hier beschriebenen und auf IT-Krisen beschränkten Strukturen nicht substituiert.

Aufgrund der föderalen Struktur der Bundesrepublik Deutschland wird auch in Zukunft eine unterschiedliche Zuständigkeit für Krisenfrüherkennung und Krisenbewältigung auf staatlicher Seite bestehen bleiben. Durch bundesweite bzw. länderübergreifende Übungen unter Einbeziehung der Wirtschaft (zum Beispiel LÜKEX) wird aber das Zusammenspiel zwischen den Beteiligten weiter optimiert.

3 Prozesse zur Krisenfrüherkennung und Krisenbewältigung

Betreiber Kritischer Infrastrukturen benötigen aktuelle und verlässliche Informationen sowie qualitativ hochwertige Analysen und Bewertungen, um Krisen frühzeitig erkennen bzw. bewältigen und dabei gleichzeitig ihrem wirtschaftlichen und gesellschaftlichen Auftrag nachkommen zu können. Fundierte Entscheidungen und wirksame Maßnahmen erfordern eine globale Sicht auf die jeweilige Lage, in der viele lokale Sichten auf aktuelle und verlässliche Informationen bereits verdichtet sind. Dieses Konzept zur Krisenfrüherkennung und Krisenbewältigung bietet den am UP KRITIS Beteiligten wohldefinierte Prozesse für die Kommunikation und für adäquate Entscheidungen über Aufgaben und Aktivitäten an.

Die aktive Umsetzung und Einhaltung der nachfolgend beschriebenen Prozesse durch alle Beteiligten gewährleistet, dass rechtzeitig Maßnahmen zur Krisenvermeidung bzw. zur Krisenbewältigung ergriffen werden können. Allen Beteiligten wird daher empfohlen, die nachfolgend dargestellten Prozesse für die Krisenfrüherkennung und Krisenbewältigung zu nutzen. Durch die flächendeckende Umsetzung der Prozesse und durch branchenübergreifende Kommunikation und Einbeziehung des BSI-Lagezentrums kann eine wirkungsvolle Früherkennung und Bewältigung von Krisensituationen für die in Deutschland genutzten kritischen IT-Infrastrukturen erreicht werden. Die Einübung und Validierung der hier beschriebenen Prozesse wird durch das Konzept „Notfall- und Krisenübungen in Kritischen Infrastrukturen“ geplant.

In den nachfolgenden Abschnitten werden zunächst die Grundlagen zur Prozessbeschreibung eingeführt und danach die Prozesse zur Krisenfrüherkennung und Krisenbewältigung visualisiert. In den weiteren Abschnitten werden die Prozesse im Detail dargelegt und erläutert.

3.1 Grundlagen

Zustände

Den nachfolgend beschriebenen Prozessen liegen die Zustände

- IT-Sicherheitslagefeststellung (Farbe Grün),
- Krisenfrüherkennung (Farbe Gelb),
- Alarmiert/Krisenbewältigung (Farbe Rot)

zugrunde, welche die Unternehmen, SPOCs und das BSI-Lagezentrum annehmen können. Den Zuständen sind die Ampelfarben Grün, Gelb und Rot als Ausdruck der Dringlichkeit des jeweiligen Zustands zugeordnet. Während die IT-Sicherheitslagefeststellung (Grün) ein normales Maß an Beobachtungsaktivität außerhalb jeder Krise beinhaltet, ist die Krisenfrüherkennung (Gelb) durch eine erhöhte Aufmerksamkeit gekennzeichnet, ausgelöst durch Vorfälle, die über das normalerweise beobachtete Geschehen hinausragen und auf eine mögliche IT-Krise hindeuten. Im Zustand „Alarmiert/Krisenbewältigung“ (Rot) werden aufgrund einer Alarmierung im Vorfeld einer möglicherweise noch abwendbaren IT-Krise Maßnahmen zur Abwehr oder Bewältigung der sich anbahnenden oder bereits akuten Krisensituation eingeleitet.

Überblick zu den Prozessen

Die Prozesse der Krisenfrüherkennung und Krisenbewältigung sind nachfolgend in den Abbildungen 1 bis 3 visualisiert:

Abbildung 1: Zustände in der Kommunikation des UP KRITIS

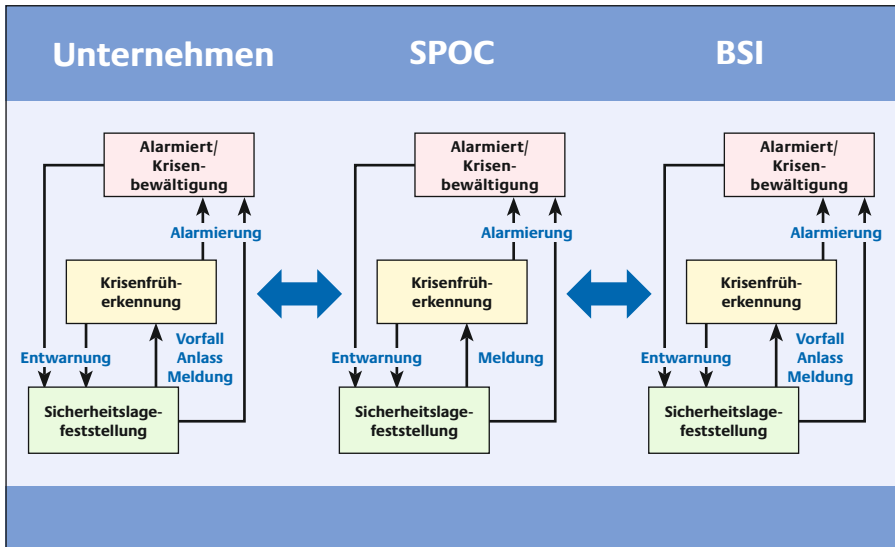


Abbildung 2: Kommunikationsfluss von Unternehmen über SPOCs an das BSI

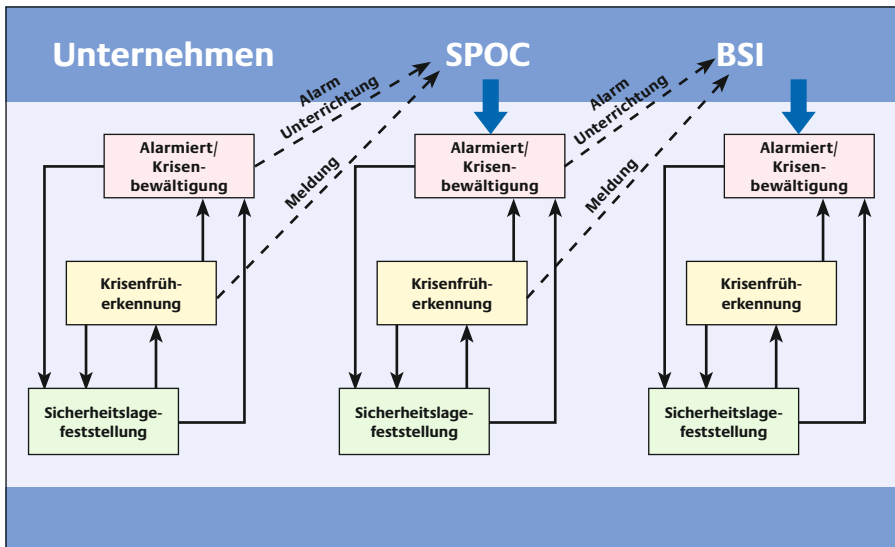
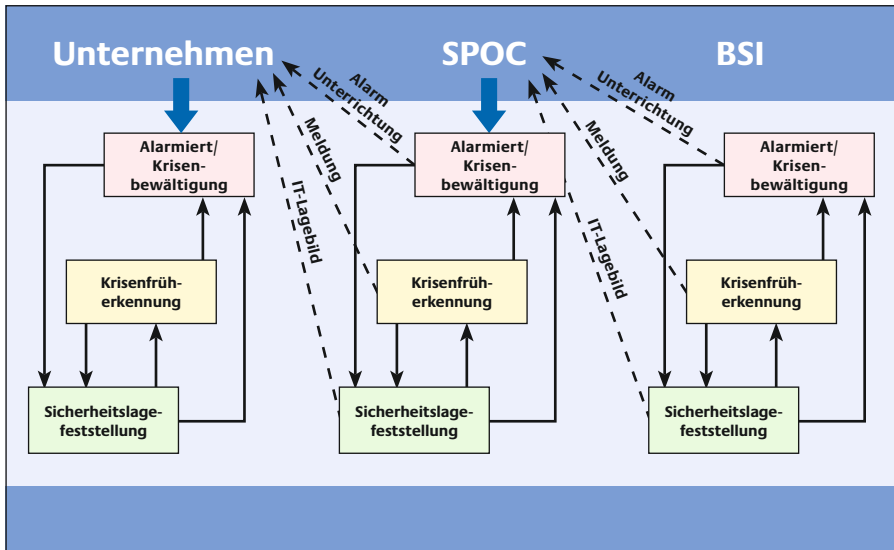


Abbildung 3: Kommunikationsfluss vom BSI über SPOCs an Unternehmen



Die farbigen Kästen geben die Zustände wieder und deuten an, welche Aktivitäten und Aufgaben mit dem jeweiligen Zustand verbunden sind. Die durchgezogenen Linien stehen für Zustandsübergänge aufgrund von Ereignissen und Entscheidungen innerhalb der Unternehmen, SPOCs und dem BSI-Lagezentrum. Die gestrichelten Linien zeigen die Nachrichtenflüsse zwischen den Kommunikationspartnern auf.

Mit dem Zustandsübergang innerhalb der Unternehmen ist möglicherweise auch eine Übertragung von Verantwortung auf andere Mitarbeiter bzw. Funktionen im Unternehmen verbunden. Unternehmen, SPOCs und das BSI-Lagezentrum können nicht davon ausgehen, den aktuellen Zustand einer anderen Einheit zu kennen, da sich dieser durch äußere Ereignisse oder interne Abläufe jederzeit verändern kann.

Informationen zur IT-Sicherheitslage

Den Aufgaben von Unternehmen, SPOCs und BSI-Lagezentrum liegen Informationen zur IT-Sicherheitslage zugrunde, die die Organisationen über ihre externen Informationsquellen erhalten oder die sie aufgrund ihrer internen Aktivitäten selbst gewinnen.

Bei Meldungen, die nach außen gehen oder von außen hereinkommen, kann es sich handeln um:

- Informationen zur IT-Sicherheitslage
- Alarmierungen durch Unternehmen, SPOCs oder das BSI-Lagezentrum
- die Unterrichtung anderer Organisationen über den eigenen Zustand
- Entwarnungen nach einer Alarmierung oder nach dem Abklingen einer Krise

Wird eine Information zur IT-Sicherheitslage gemeldet, dann sollte sie – so weit wie möglich – mit Attributen im Sinne einer Bewertung versehen sein. Dazu gehören:

- Auswirkungen (keine, auf Unternehmen, auf Branche, branchenübergreifend)
- Sachverhalt (Ausdehnung, voraussichtliche Dauer, Grund, Auslöser)
- Dringlichkeit

Rahmenbedingungen zum Informationsaustausch

Die Rahmenbedingungen gemäß dem UP KRITIS bezüglich Umgang, Weitergabe und Schutz der Informationen und der Informationsquellen sind:

- Die schnelle Weitergabe von Informationen hat stets Vorrang vor Analyse und Bewertung.
- Der Informationsaustausch erfolgt auf freiwilliger Basis.
- Der Informationsaustausch basiert auf dem Vertrauen, dass aufgrund der Meldung von Vorfällen kein Schaden für die an der Kommunikation beteiligten Partner entstehen darf.
- Sensible Informationen werden von allen Beteiligten vertraulich behandelt, um die mit dem Informationsaustausch verbundenen Risiken zu minimieren. Zur Kennzeichnung von Information hinsichtlich ihrer Sensitivität wird das sogenannte „Traffic Light Protocol“ (TLP) vorgeschlagen. Danach werden die folgenden Sensitivitätsgrade unterschieden:

TLP-Red: Informationen dürfen nur im Kreise der auf das TLP verpflichteten, in einer Besprechung anwesenden Personen ausgetauscht werden. Dokumente dürfen vom Empfänger nur nach Genehmigung durch den Absender weitergegeben werden.

TLP-Amber: Wenn es den Zielen der Arbeitsgruppe dient, dürfen Informationen auch an Kollegen in der eigenen Organisation oder an andere Organisationen (zum Beispiel Berater) weitergegeben werden („Need-to-know“-Prinzip).

TLP-Green: Informationen dürfen auch an andere Organisationen weitergegeben, aber nicht veröffentlicht oder den Massenmedien zugänglich gemacht werden.

TLP-White: Informationen dürfen uneingeschränkt an jeden, einschließlich der Massenmedien, weitergegeben werden.

Die Regelung wird in einer Verfahrensregelung verankert, zu deren Einhaltung sich die Partner verpflichten.

- Um einen reibungslosen Informationsfluss nicht zu gefährden, ist es notwendig, zwischen Dringlichkeit, Wichtigkeit und Geheimhaltungsbedarf von Informationen zu differenzieren. Beispielsweise kann aus einer Häufung von Nachrichten aus verschiedenen Quellen zu einem bestimmten Sachverhalt eine Erhöhung der Dringlichkeit resultieren, ohne dass gleichzeitig ein erhöhter Grad an Geheimhaltung erforderlich wäre.

In Ausnahmefällen kann es sein, dass auch Informationen weitergegeben werden müssen, die als Verschlussache (VS) eingestuft sind. Die Weitergabe erfolgt dann auf der Grundlage der Verschlussachenanweisung des Bundes.

3.2 Sicherheitslagefeststellung

Bereits heute beobachten Unternehmen die IT-Sicherheitslage für ihre eigenen Sicherheitsbelange. Sie verfügen über individuelle Mechanismen zur Sammlung, Analyse und Bewertung von Informationen, die zu einer aktuellen Einschätzung der IT-Sicherheitslage beitragen.

Zielsetzung der IT-Sicherheitslagefeststellung (Grün) ist das möglichst frühzeitige Erkennen von Vorfällen, die Anzeichen oder Anlass für eine krisenhafte Entwicklung über ein einzelnes Unternehmen hinaus sein können. Die Möglichkeiten zur Ergreifung von adäquaten Schutzmaßnahmen hängen entscheidend davon ab, wie frühzeitig Erkenntnisse vorliegen und kommuniziert werden. Informationen mit potenziellen Auswirkungen auf die IT-Sicherheitslage oder Anzeichen einer IT-Krise werden daher möglichst unverzüglich über die SPOCs an das BSI-Lagezentrum gemeldet. Das BSI-Lagezentrum gibt seinerseits schnellstmöglich Informationen zur IT-Sicherheitslage über die SPOCs in die Unternehmen.

Zur IT-Sicherheitslagefeststellung steht der SPOC in Bereitschaft für die Krisenkommunikation und -reaktion. Er erstellt keine eigenen IT-Sicherheitslagebilder, sondern kommuniziert und koordiniert.

Wird im Rahmen der IT-Sicherheitslagefeststellung ein Vorfall oder ein Anlass erkannt, der auf eine IT-Krise hindeutet, dann tritt das Unternehmen bzw. das BSI-Lagezentrum in die Krisenfrüherkennung ein. Dies kann auch dadurch bewirkt werden, dass über den SPOC eine entsprechende Meldung, zum Beispiel ein akutes IT-Sicherheitslagebild des BSI, versandt wird.

3.3 Krisenfrüherkennung

Unternehmen

Innerhalb der Krisenfrüherkennung analysiert und bewertet das Unternehmen die erhaltene Meldung oder selbst gewonnene Informationen zur IT-Sicherheitslage, um über die weitere Vorgehensweise entscheiden zu können. Wenn sich eine IT-Krise abzeichnet oder unmittelbar bevorsteht, wird das Unternehmen den SPOC oder das BSI-Lagezentrum schnellstmöglich alarmieren. Gegebenenfalls wird das Unternehmen entweder in die Krisenbewältigung eintreten oder im Rahmen einer Entwarnung wieder in den Normalbetrieb der Sicherheitslagefeststellung zurückkehren.

Die schnelle Weiterleitung von Informationen hat zentrale Bedeutung für das Erkennen von Vorfällen oder Anlässen, die auf eine IT-Krise hindeuten. Die Weitergabe einer Information erfolgt stets freiwillig. Der Informationsigentümer entscheidet also, wie er mit einer Information verfährt.

Die Unternehmen lassen sich bei der Entscheidung, ob eine Information weitergegeben werden soll, von folgenden Grundsätzen leiten:

- Informationen über alle Ereignisse, aus denen Krisen entstehen können, sind von Bedeutung für eine effektive Krisenfrüherkennung. Es werden daher nicht nur Informationen über eingetretene Krisen gemeldet, sondern auch Informationen, die Indikatoren von Krisen sein können.
- Eine Information ohne Relevanz für den Informationsbesitzer kann für andere Betreiber Kritischer Infrastrukturen sehr wohl von Bedeutung sein. Der potenzielle Sender einer Information entscheidet über die Meldewürdigkeit einer Information also nicht allein aus Sicht seines Unternehmens, sondern berücksichtigt im Rahmen seiner Möglichkeiten die Relevanz für andere Unternehmen bzw. Branchen. Der Empfänger der Information kann mit seinem Branchenwissen einschätzen, welche Bedeutung diese Information für sein Unternehmen bzw. seine Branche hat.
- Der Sender handelt nach bestem Wissen und Gewissen, übernimmt jedoch keine Gewähr für die Korrektheit der Information.
- Eine Information kann für sich allein gesehen nur von geringer Bedeutung sein, sie kann aber im Zusammenhang mit anderen Informationen an Wichtigkeit gewinnen. So könnte sich zum Beispiel aus einer Störung, die aus Sicht der betroffenen Branche vernachlässigbar ist, im Zusammenspiel mit Störungen in anderen Branchen eine IT-Krise entwickeln.
- Immer dann, wenn Zweifel bestehen, ob eine Information weiterzugeben ist oder nicht, sollte die Information weitergegeben werden.

SPOC

Der SPOC erhält Meldungen der Unternehmen, die er gemäß seiner Aufgabenstellung bearbeitet (siehe Abschnitt 2.2 „Single Point of Contact [SPOC]“) und an das BSI-Lagezentrum weiterleitet. Umgekehrt nimmt der SPOC IT-Sicherheitslagebilder des BSI entgegen und sendet sie an die Unternehmen seiner Branche. Der SPOC geht in die Krisenfrüherkennung über, wenn er Meldungen erhält, die auf eine IT-Krise hindeuten oder eine IT-Krise ankündigen. Dies können Meldungen von Unternehmen seiner Branche oder des BSI sein.

Die Analyse und Bewertung von Informationen ist von geringerer Bedeutung als die schnelle Weiterleitung der Information an die Unternehmen seiner Branche oder an das BSI-Lagezentrum.

IT-Lagezentrum des BSI

Das IT-Lagezentrum des BSI erstellt kontinuierlich aktuelle nationale IT-Sicherheitslagebilder und leitet diese unter anderem an die SPOCs weiter. Analog zu den Unternehmen und zu den SPOCs geht das BSI-Lagezentrum in die Krisenfrüherkennung über, wenn ein Vorfall oder ein Anlass erkannt oder gemeldet wird, der auf eine IT-Krise hindeutet.

3.4 Alarmierung und Krisenbewältigung

Das vorliegende Konzept zeigt auf, wie innerhalb einer IT-Krise eine schnelle und abgestimmte Kommunikation aufrechterhalten werden kann, um den Unternehmen und den staatlichen Stellen eine rechtzeitige Reaktion zu ermöglichen und Schäden einzugrenzen. Es ist nicht als konkrete Handlungsanweisung zu verstehen.

Unternehmen, SPOCs und das BSI-Lagezentrum alarmieren, wenn eine IT-Krise bevorsteht oder bereits eingetreten ist. Sie alarmieren im Regelfall aus der Krisenfrüherkennung heraus, wenn sich zum Beispiel durch die Analyse und Bewertung von Informationen die Anzeichen verfestigen, die auf eine IT-Krise hindeuten.

Im Falle der Alarmierung muss noch keine Krise vorliegen, es kann jedoch ein konkretes Eintrittsrisiko bestehen. Möglicherweise kann aufgrund der kommunizierten Informationen und durch entsprechende Maßnahmen eine IT-Krise abgewendet oder in ihren Auswirkungen gemildert werden. Falls es nach einer Alarmierung nicht zu einer IT-Krise kommt, wird Entwarnung gemeldet.

Im Falle einer sich abzeichnenden oder bereits eingetretenen IT-Krise kommuniziert das BSI-Lagezentrum mit den SPOCs. Falls für die Krisenbewältigung erforderlich, kommunizieren einzelne Unternehmen und das BSI-Lagezentrum unmittelbar miteinander. Die SPOCs halten die Kommunikation zu den Unternehmen ihrer Branche aufrecht. Auch die Ansprechpartner in den Unternehmen für den Krisenfall sind den SPOCs bekannt.

Die Aufgabenstellung, die sich aus der Krisenbewältigung ergibt, hängt von der Art, den Umständen und den potenziellen Auswirkungen der jeweiligen IT-Krise ab. Für die Krisenbewältigung benötigen die Unternehmen Informationen darüber, welche Handlungsoptionen bestehen und welche nicht. Daher sind Handlungsempfehlungen, die von Sicherheitsspezialisten der Unternehmen oder des BSI-Lagezentrums ausgesprochen und an die Unternehmen und SPOCs kommuniziert werden, von hohem Nutzen für die Branchen und Unternehmen. Darüber hinaus stellt die Kommunikation zwischen Unternehmen und SPOCs einerseits sowie SPOCs und BSI-Lagezentrum andererseits sicher, dass Maßnahmen zur Eindämmung oder Beseitigung der IT-Krise koordiniert und optimiert werden können.

Unternehmen, SPOCs und BSI-Lagezentrum informieren sich gegenseitig über den Fortgang der Krisenbewältigung und die Beendigung der Krise, jedoch ist die Unterrichtung gegenüber der eigentlichen Krisenbewältigung nachrangig.

3.5 Regelmäßiger Informationsaustausch

Der Informationsaustausch dient dazu, Lösungsmöglichkeiten zur Krisenfrüherkennung und Krisenbewältigung weiterzuentwickeln. Dazu werden unter anderem Probleme und Lösungen bzw. „Good Practices“ aufbereitet und zur Diskussion gestellt. Dies gilt insbesondere für die Aufarbeitung von Krisen im Sinne des Ansatzes „Lessons learned“.

Im Rahmen des regelmäßigen Informationsaustauschs entwickelte Problemlösungen dienen der Nachhaltigkeit, da so eine kontinuierliche Weiterentwicklung des Konzepts zur Krisenfrüherkennung und Krisenbewältigung ermöglicht wird.

Die Umsetzung des Konzepts und seine Weiterentwicklung sind Gegenstand des informellen Informationsaustausches im Rahmen der Kommunikationsplattform.

3.6 Zusammenfassende tabellarische Übersicht

Tabelle 1: Beteiligte, Aufgaben und Kommunikationsmittel in den Zuständen des Krisenmanagements

	Strukturen und Beteiligte	Aufgaben/ Aktivitäten	Kommunikationsmittel
Regelmäßiger Informationsaustausch	<ul style="list-style-type: none"> • BSI-Lagezentrum • Unternehmen • SPOCs 	<ul style="list-style-type: none"> • Erfahrungsaustausch • Krisennachbearbeitung („Lessons learned“) 	<ul style="list-style-type: none"> • Besprechung • Telefon • Telefonkonferenz • Fax • E-Mail • Kommunikationsplattform • Videokonferenz
IT-Sicherheitslagefeststellung	<ul style="list-style-type: none"> • BSI-Lagezentrum • Unternehmen 	<ul style="list-style-type: none"> • Einschätzung der Lage • Erstellung IT-Sicherheitslagebild und Weiterleitung 	<ul style="list-style-type: none"> • Telefon • Telefonkonferenz • Fax • E-Mail • Videokonferenz
Krisenfrüherkennung	<ul style="list-style-type: none"> • BSI-Lagezentrum • Unternehmen • SPOCs 	<ul style="list-style-type: none"> • Gegenseitige Information zur IT-Sicherheitslage • Analyse • Bewertung • Verdichtung • Entscheidung • Alarmierung • Entwarnung 	<ul style="list-style-type: none"> • SMS • Telefon • Telefonkonferenz • Fax • E-Mail • Videokonferenz <p>Hochverfügbarkeit:</p> <ul style="list-style-type: none"> • Mobilfunk • Satellitentelefon
Alarmierung und Krisenbewältigung	<ul style="list-style-type: none"> • Ansprechpartner im Unternehmen oder SPOC (je nach Krisenlage) • BSI-Lagezentrum und krisenbezogene andere Lagezentren • gegebenenfalls zuständige Katastrophenschutzstäbe (Landesebene) 	<ul style="list-style-type: none"> • Bereitstellung von Empfehlungen • Krisenmanagement • Koordination von Gegenmaßnahmen • Austausch, Information und Empfehlungen • Koordination mit anderen Lagezentren 	<ul style="list-style-type: none"> • SMS • Telefon • Telefonkonferenz • Fax • E-Mail • Pager • Videokonferenz <p>Hochverfügbarkeit:</p> <ul style="list-style-type: none"> • Mobilfunk • Satellitentelefon

3.7 Kommunikationstechnik

Im Interesse der in diesem Konzept beschriebenen Kommunikationsstruktur zur Früherkennung und Bewältigung von Krisen wird empfohlen, mehrfach redundante Kommunikationstechnik vorzusehen.

Als Kommunikationsmedien werden

- E-Mail,
- Telefon (mehrere Nummern) und
- Fax

verwendet. Für eine erhöhte Verfügbarkeit können in der Regel

- Mobiltelefone und
- Satellitentelefone

eingesetzt werden. Der Bedarf an Vorrangschaltungen in Fest- und Mobilfunknetzen sollte geprüft werden.

Die einzusetzenden Kommunikationsmittel werden im Rahmen der weiteren Arbeiten der Arbeitsgruppe geprüft, bewertet und beschlossen. Der Einsatz der Kommunikationsmittel wird regelmäßig geprobt. Hierzu wird auf das Übungskonzept der Arbeitsgruppe „Notfall- und Krisenübungen“ verwiesen.

4 Konkrete Umsetzung und weiteres Vorgehen

Der Starttermin für die Produktivphase dieses vorliegenden Konzepts ist für den Januar 2009 beschlossen. Das BSI-Lagezentrum ist zu diesem Zeitpunkt bereits arbeitsfähig. Erste SPOC-Strukturen sind bereits eingerichtet, andere befinden sich in der Aufbau- oder Konzeptionsphase.

Die Teilnehmer des UP KRITIS nehmen die Regelkommunikation im Januar 2009 auf. Anfänglich sind drei Plenarsitzungen jährlich geplant, auch die Tätigkeit in den Arbeitsgruppen wird fortgesetzt.

Aus der Arbeitsgruppe 2 („Krisenreaktion und -bewältigung“) heraus ist die Gründung weiterer Unterarbeitsgruppen vorgesehen. Folgende Aufgaben sind bereits identifiziert und werden von Fachleuten in zwei Unterarbeitsgruppen bearbeitet:

- 1) Implementierung und Koordinierung:
Hierunter werden Festlegungen von konkreten Maßnahmen zum Aufbau der Strukturen zur Krisenfrüherkennung und -bewältigung verstanden. Unter anderem werden auch Inhalt und Formate von Meldungen abgestimmt.
- 2) Kommunikationsmittel:
Einsatz und gegebenenfalls Entwicklung von geeigneten Verfahren für vertrauliche Kommunikation (zum Beispiel Chiasmus, Elcro-DAT 6.2, Topsec, SINA, VPS etc.) sowie für mehrfach redundante Strukturen.

Verbunden mit diesen Plenarsitzungen finden die Sitzungen der Arbeitsgruppe 4 („Nationale und internationale Zusammenarbeit“) statt. Aufgabe der Arbeitsgruppe 4 ist die Koordination und Abstimmung zwischen den am UP KRITIS beteiligten Parteien zum Austausch von Informationen auf nationaler und internationaler Ebene. Die Arbeit der Arbeitsgruppe 4 hat im Rahmen der Sitzungen der Arbeitsgruppe 2 im Jahr 2008 begonnen und wird nunmehr kontinuierlich weitergeführt. Zur Unterstützung des Kommunikationsaustausches über internationale Aktivitäten soll eine technische Plattform betrieben werden, über die internationale Dokumente mit CIIP- und CIP-Bezug zur Verfügung gestellt werden. Techni-

sche Entwicklung und Inbetriebnahme dieser Plattform erfolgen auf Basis von durch die Arbeitsgruppe spezifizierten Anforderungen.

Das Konzept zur Früherkennung und Bewältigung von Krisen wird nach einem angemessenen Zeitraum – frühestens aber nach zwei Jahren – evaluiert und falls erforderlich weiterentwickelt. Dabei werden die Erfahrungen aus Planspielen und Übungen einbezogen, deren Ergebnisse in eine Fortschreibung des Konzepts einfließen sollen.

Bestehende Kontakte zwischen den Arbeitsgruppen des UP KRITIS dienen auch zum gegenseitigen Austausch von Erfahrungen und zur Einbindung des Konzepts in die geplanten Übungen der Arbeitsgruppe 1. Die Teilnehmer der Arbeitsgruppen 1 und 4 streben in ihrer weiteren Arbeit an, die Grundlagen für eine zukünftige Teilnahme an länderübergreifenden und internationalen Übungen und Planspielen unter IT-Aspekten zu schaffen.

Anhang

Abkürzungen

24/7	Sieben Tage in der Woche rund um die Uhr
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BAK	Bundeskriminalamt
BMI	Bundesministerium des Innern
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
IT	Informationstechnik
KRITIS	Kritische Infrastrukturen
LÜKEX	Länderübergreifende Krisenmanagement Exercise
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
SPOC	Single Point of Contact
TLP	Traffic Light Protocol
UP KRITIS	Umsetzungsplan KRITIS
VS	Verschlusssache

Glossar

Betreiber Kritischer Infrastrukturen	Betreiber Kritischer Infrastrukturen sind privatwirtschaftliche Unternehmen oder Behörden, die Dienstleistungen in den Kritischen Infrastrukturen erbringen.
Bundesverwaltung	Bundesressorts und deren Geschäftsbereichsbehörden wie zum Beispiel BSI, BKA, BBK, BNetzA, BaFin (vgl. Artikel 86 Grundgesetz).
Informationsinfrastruktur	Die Gesamtheit der IT-Anteile einer Infrastruktur wird als deren Informationsinfrastruktur bezeichnet.
IT-Krise	Eine IT-Krise im Kontext des UP KRITIS liegt vor, wenn mittelbar oder unmittelbar ITbedingt ein Ausfall oder eine Beeinträchtigung von Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen mit nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen eintritt bzw. zu erwarten ist.
IT-Lagezentrum des BSI	Das BSI-Lagezentrum verfügt jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland, um den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können. Es stellt die schnelle Reaktion auf schwerwiegende Vorfälle sicher, um so rechtzeitige Gegenmaßnahmen zu ermöglichen und Schäden in größerem Ausmaß zu vermeiden.

IT-Sicherheit	IT-Sicherheit ist der Zustand, in dem Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.
Krise	Eine vom Normalzustand abweichende, sich plötzlich oder schleichend entwickelnde Lage, die durch ein Risikopotenzial gekennzeichnet ist, das Gefahren und Schäden für Leib und Leben von Menschen, bedeutende Sachwerte, schwerwiegende Gefährdungen des politischen, sozialen oder wirtschaftlichen Systems in sich birgt und der Entscheidung – oftmals unter Unsicherheit und unvollständiger Information – bedarf.
Krisenbewältigung	Die Durchführung von Maßnahmen mit dem Ziel der schnellstmöglichen Zurückführung einer akuten Krisensituation in den Normalzustand und der Minimierung ihrer Auswirkungen.
Krisenfrüherkennung	Erkennung und Meldung von Vorfällen, die einzeln oder in ihrem Zusammenwirken Ursachen oder Anzeichen für krisenhafte Entwicklungen sein können. Die Krisenfrüherkennung ist Teil der Krisenprävention.
Krisenmanagement	Schaffung von konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen, die eine schnellstmögliche Zurückführung der eingetretenen außergewöhnlichen Situation in den Normalzustand unterstützen.
Krisenprävention	Alle Maßnahmen mit dem Ziel, mögliche Vorfälle, die einzeln oder in ihrem Zusammenwirken krisenhafte Auswirkungen haben können, zu vermeiden.

Kritische Infrastruktur

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten. In Deutschland werden folgende Sektoren den Kritischen Infrastrukturen zugeordnet:

- Transport und Verkehr (Luftfahrt, Seeschifffahrt, Bahn, Nahverkehr, Binnenschifffahrt, Straße, Postwesen)
- Energie (Elektrizität, Kernkraftwerke, Mineralöl, Gas)
- Gefahrstoffe (Chemie- und Biostoffe, Gefahrguttransporte, Rüstungsindustrie)
- Informationstechnik und Telekommunikation
- Finanz-, Geld- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen)
- Versorgung (Gesundheits-, Notfall- und Rettungswesen, Katastrophenschutz, Lebensmittel- und Wasserversorgung, Entsorgung)
- Behörden, Verwaltung und Justiz (staatliche Einrichtungen)
- Sonstiges (Medien, Großforschungseinrichtungen sowie herausragende oder symbolträchtige Bauwerke, Kulturgut)

Sanitarisierung

Sanitarisierung ist die Bereinigung einer Meldung von schutzbedürftigen Informationsanteilen. Ziel der Sanitarisierung ist die Wahrung der berechtigten Schutzinteressen der am Informationsaustausch Beteiligten bei gleichzeitigem Erhalt der relevanten Informationen.

SPOC	Single Point of Contact: Fest etablierte Funktion in einer Branche, die für die Unternehmen der Branche zentrale Kommunikationsplattform und Meldestelle aus und in die Unternehmen ist.
UP-KRITIS-Partner	Alle Behörden, Interessenverbände, Unternehmen usw., die im Rahmen des Umsetzungsplans Kritische Infrastrukturen zusammenarbeiten (zum Beispiel in Arbeitsgruppen) und an Übungen teilnehmen.
UP-KRITIS-Zusammenarbeit	Realisierung der Konzepte sowie Einübung und Durchführung der Prozesse aus NPSI und dem UP KRITIS durch die Betreiber Kritischer Infrastrukturen und die Bundesverwaltung.

Literaturverzeichnis

Bundesministerium des Innern (Hrsg.): Nationaler Plan zum Schutz der Informationsinfrastrukturen. Berlin, 2005.

Bundesministerium des Innern (Hrsg.): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. Berlin, 2007.

Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Berlin, 2005.

Beteiligte UP-KRITIS-Partner

Allianz Deutschland AG
Arcor AG & Co. KG
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Bundesverband deutscher Banken
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
(E-Plus Gruppe) E-Plus Mobilfunk GmbH & Co. KG
Europäische Zentralbank
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
HUK-COBURG
Mineralölwirtschaftsverband
RWE Aktiengesellschaft
RWE Energy Aktiengesellschaft
SIZ Informatikzentrum der Sparkassenorganisation GmbH
Telefónica O₂ Germany GmbH & Co. OHG
Vodafone D2 GmbH

Impressum

Herausgeber:

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

Redaktion:

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

Gestaltung und Produktion:

MEDIA CONSULTA Deutschland GmbH

Druck:

Silber Druck oHG

Auflage:

1.000 Exemplare

Stand:

Dezember 2008