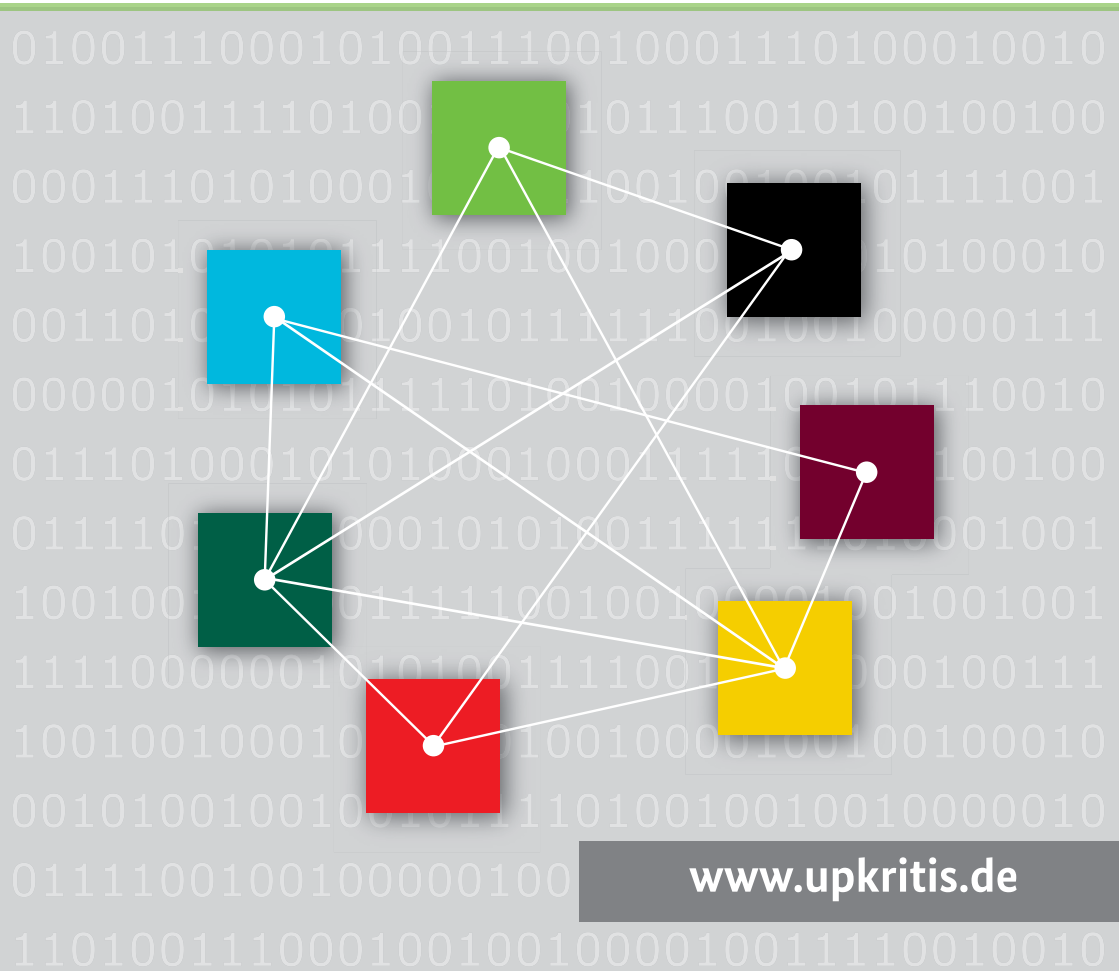
UP KRITIS

UP KRITIS

Öffentlich-Private Partnerschaft
zum Schutz Kritischer Infrastrukturen

- Grundlagen und Ziele -



www.upkritis.de

Inhaltsverzeichnis

1 Einleitung und Motivation

1 Einleitung und Motivation

Deutschland gehört zu den führenden industriell und technologisch geprägten Nationen. Die Bedeutung des Wirtschaftsstandortes Deutschland und die Sicherstellung der Wettbewerbsfähigkeit in einer globalisierten Welt als Voraussetzungen für Wohlstand und Fortschritt sind maßgeblich vom Vorhandensein hochleistungsfähiger und funktionstüchtiger Infrastrukturen abhängig. Eine schwerwiegende Störung oder gar eine Unterbrechung der über diese Infrastrukturen erbrachten Dienstleistungen kann negative Folgen für unsere Gesellschaft haben; in manchen Fällen kann ein Ausfall sogar zu massiven Beeinträchtigungen im gesellschaftlichen Zusammenleben führen. Ist ein Ausfall kaum oder gar nicht tolerierbar, so handelt es sich um für die Gesellschaft unverzichtbare und deswegen kritische Dienstleistungen, die von so genannten Kritischen Infrastrukturen erbracht werden. Die KRITIS-Strategie der Bundesregierung definiert Kritische Infrastrukturen wie folgt:

Kritische Infrastrukturen (KRITIS) 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 würden.

In Deutschland werden Organisationen und Einrichtungen aus den Bereichen Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur zu den Kritischen Infrastrukturen gezählt (siehe Abbildung 1).

Die Betreiber dieser Kritischen Infrastrukturen, unabhängig davon, ob privatwirtschaftlich oder öffentlich-rechtlich organisiert, erbringen die kritischen, für die Versorgung der Bevölkerung zwingend notwendigen Dienstleistungen in hoher Qualität und Stabilität. Die ausgeprägte Widerstandsfähigkeit dieser kritischen Dienstleistungen gegen vielfältige Bedrohungen ist Beweis für das Verantwortungsbewusstsein der KRITIS-Betreiber und bildet eine wesentliche Grundlage für das Funktionieren der Gesellschaft.

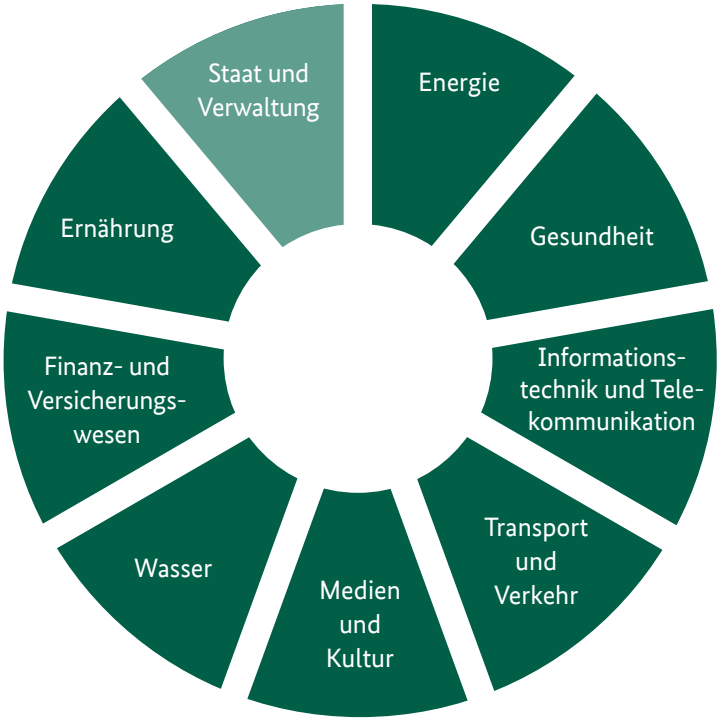


Abbildung 1: Die Sektoren Kritischer Infrastrukturen in Deutschland

Der Schutz der Kritischen Infrastrukturen zur Aufrechterhaltung der Versorgung der Bevölkerung ist ein fortlaufender Prozess, der sich angesichts stetig verändernder Rahmenbedingungen permanent weiterentwickeln muss. Dies haben Wirtschaft und Staat schon vor Jahren erkannt und als wichtige nationale Aufgabe aufgegriffen. Die Bundesregierung verfolgt beim Schutz Kritischer Infrastrukturen strategisch und in der operativen Umsetzung einen ganzheitlichen Ansatz, in dessen Rahmen in den Jahren 2005 und 2006 in Zusammenarbeit mit Betreibern Kritischer Infrastrukturen der Umsetzungsplan KRITIS entstand. Mit der Veröffentlichung des Umsetzungsplans im Jahr 2007 wurde diese öffentlich-private – inzwischen UP KRITIS genannte – Zusammenarbeit institutionalisiert. Gemeinsames Ziel ist es, den Schutz der Kritischen Infrastrukturen branchen- und sektorübergreifend zu verbessern.

Gegenüber 2007 hat sich insbesondere die IT-Bedrohungslage massiv verschärft. Die Bundesregierung hat darauf reagiert, indem sie die Strategien und Konzepte zum Schutz der Kritischen Infrastrukturen weiterentwickelt und an die aktuellen Gegebenheiten angepasst hat. Im Jahr 2009 veröffentlichte das Bundesministerium des Innern (BMI) die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“, in der auch auf die besonderen Risiken und Gefährdungen für Informationsinfrastrukturen Bezug genommen wird. 2011 folgte die „Cyber-Sicherheitsstrategie für Deutschland“ mit dem Thema „Schutz der kritischen Informationsinfrastrukturen“ als Kernanliegen. Viele andere Aktivitäten, wie die Gründung des Cyber-Sicherheitsrats und des Cyber-Abwehrzentrums, tragen seitdem maßgeblich zum KRITIS-Schutz bei.

Der Schutz vor Gefahren mit IT-Bezug, insbesondere vor Cyber-Angriffen, ist einer der zentralen Bestandteile eines All-Gefahrenansatzes; er wird in ein operatives Risiko- und Krisenmanagement integriert. Da kritische Dienstleistungen mittels kritischer (Produktions-)Prozesse erbracht werden, muss sich der Schutz vorrangig auf diese Prozesse konzentrieren.

In nahezu allen kritischen Prozessen ist Informationstechnik inzwischen ein zentraler und unverzichtbarer Bestandteil geworden. Gleichzeitig befindet sich diese seit Jahren in einer bemerkenswert dynamischen Entwicklung, die eine sich ständig ändernde Bedrohungslage mit sich bringt. Aus diesen Gründen kommt dem Schutz der Informationsinfrastrukturen im UP KRITIS eine besondere Bedeutung zu.

Der UP KRITIS behandelt aber auch über IT hinausgehende Themen, um die Verfügbarkeit und Robustheit der Kritischen Infrastrukturen zu erhalten und zu stärken. Für einen umfassenden Schutz der Kritischen Infrastrukturen müssen physischer Schutz und IT-Sicherheit gemeinsam gedacht und gelebt werden.

Die branchenübergreifende Zusammenarbeit von Wirtschaft und Staat im UP KRITIS hat sich zu einem Erfolgsmodell entwickelt. Die beteiligten Organisationen arbeiten auf Basis gegenseitigen Vertrauens zusammen. Sie tauschen sich untereinander aus und lernen voneinander im Hinblick auf den Schutz Kritischer Infrastrukturen. Gemeinsam kommen alle Beteiligten so zu besseren Lösungen. Im Rahmen des UP KRITIS werden Konzepte entwickelt, Kontakte geknüpft, Übungen abgehalten sowie ein gemeinsames Vorgehen zum (IT-)Krisenmanagement erarbeitet und etabliert.

Um auch in den nächsten Jahren weiterhin konstruktiv zusammenarbeiten zu können, wurden 2013 die Ziele und die Struktur des UP KRITIS an die neuen Aufgaben und Herausforderungen angepasst. Das Ergebnis dieser Anpassungen ist im vorliegenden Dokument niedergeschrieben. Mit der Fortschreibung des UP KRITIS sind zugleich die Grundlagen geschaffen, branchenspezifische Sicherheitsanforderungen kooperativ zu erarbeiten, die Widerstandsfähigkeit (Resilienz) der Kritischen Infrastrukturen in Deutschland weiter zu verbessern sowie relevante Gesetzesvorhaben aktiv zu begleiten. Die am UP KRITIS beteiligten Organisationen arbeiten auf dieser Basis auch in den folgenden Jahren gemeinsam daran, die Versorgung mit kritischen Dienstleistungen auch im Zeitalter von allgegenwärtiger IT optimal zu gewährleisten.

2 Erreichtes

2 Erreichtes

Seit Verabschiedung des Umsetzungsplans KRITIS im Jahr 2007 arbeiten Unternehmen und Bundesregierung im UP KRITIS gemeinsam daran, die Kritischen Infrastrukturen und insbesondere die zugrunde liegenden Informationsinfrastrukturen nachhaltig abzusichern. Mit der Idee, Kompetenz und Know-how von Wirtschaft und Staat in Bezug auf den Schutz kritischer Informationsinfrastrukturen zusammenzuführen, wurde vor allem die **unternehmens- und branchenübergreifende Kommunikation** gefördert, die sich inzwischen in allen Bereichen des UP KRITIS etabliert hat.

Das entstandene „Wir-Gefühl" hat die vertrauensvolle Zusammenarbeit der Beteiligten erheblich gestärkt. Es wurden viele Kontakte geknüpft, auch zwischen den Branchen. Zudem konnte ein gegenseitiges Verständnis für die Auffassungen und Positionen der Partner entwickelt werden. Dies hat die Zusammenarbeit trotz bestehender unterschiedlicher Aufgabenstellungen gefördert und wesentlich zur Erreichung der gesetzten Ziele beigetragen.

Es ist somit gelungen, ein **Netzwerk des Vertrauens** zwischen den Mitgliedern des UP KRITIS aufzubauen und dieses zu einem funktionsfähigen Instrument der schnellen und zuverlässigen Kommunikation auch in denkbaren Krisensituationen aufwachsen zu lassen. Damit verfügt die Bundesrepublik Deutschland über ein Instrument, das es ermöglicht, in einer Krise schnell zu handeln und die Krisenbewältigung als gemeinsame Aufgabe von Wirtschaft und Staat zu verstehen.

Eine konkrete Aufgabe des UP KRITIS war die **Erarbeitung und Umsetzung von gemeinsamen Empfehlungen**. In den etablierten Arbeitsgruppen wurden die beiden grundlegenden Konzepte *„Früherkennung und Bewältigung von IT-Krisen"* sowie *„IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen"* erarbeitet.

Die Konzepte wurden veröffentlicht und im UP KRITIS umgesetzt:

» Auf Grundlage der **Übungsroadmap** aus dem Konzept zu IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen wurden mehrfach Übungen durchgeführt. Sowohl einfache Übungen zur Kommunikationsüberprüfung als auch komplexe Übungen wie die Teilnahme an der LÜKEX-Übungsreihe oder dedizierte Tischübungen haben zur Optimierung der gemeinsamen Krisenkommunikationsstrukturen und -prozesse geführt. Mit den Übungen „Bundessonderlage IT 2009“ sowie „Eltville 13“ konnten die Mitglieder des UP KRITIS insbesondere IT-Krisenszenarien intensiv beüben und im Verlaufe der Übung Verbesserungspotenziale identifizieren sowie Lösungen zur Bewältigung von Störungen kritischer Prozesse entwickeln.

» Die intensive Vorbereitung und die Einbindung von UP-KRITIS-Mitgliedern in die Übung „LÜKEX 2011“ („IT-Sicherheit in Deutschland“) konnte nicht zuletzt die Fähigkeiten der Beteiligten, IT-Krisen in der Praxis schnell und erfolgreich zu bewältigen, weiter stärken. Die gewonnenen Erfahrungen fließen fortlaufend in die Maßnahmen der beteiligten Unternehmen zur IT-Sicherheit und zum BCM ein. Auch die Teilnahme an der EU-Übung „Cyber Europe 2012“ war ein großer Erfolg und hat gezeigt, dass eine grenzüberschreitende Zusammenarbeit im Krisenfall möglich und hilfreich ist. Grundlage für die **operative Zusammenarbeit** ist das Konzeptpapier zur Früherkennung und Bewältigung von IT-Krisen, das u.a. mit der Einrichtung von mehreren „Single Point of Contact“ (SPOC) und der Etablierung von Notfallkontakten umgesetzt wurde. Vertreter von Staat und Wirtschaft haben gemeinsam Prozesse für die Krisenreaktion festgelegt, die sich bei verschiedenen Vorfällen bereits bewährt haben. Das Lagezentrum des BSI hat Lageinformationen, Meldungen und Analysen an die Unternehmen verschickt, und aus den Unternehmen wurden – teilweise über die SPOC – Vorfälle und Auffälligkeiten gemeldet.

Im Sinne der **Optimierung des Krisenmanagements** konnten an der AKNZ zwei mehrtägige Schulungen durchgeführt werden, um das Verständnis für die Zusammenarbeit von Staat und Wirtschaft in spezifischen Krisensituationen zu vertiefen. Mit der verstärkten Einbindung des BBK ist es zudem gelungen, **IT-Sicherheit und BCM** in Kritischen Infrastrukturen im Interesse eines umfassenden KRITIS-Schutzes stärker zu verknüpfen. Eine **Studie zu potenziellen Krisenszenarien** hat dazu beigetragen, dass die beteiligten Organisationen eine gemeinsame Sicht auf mögliche IT-Krisen und entsprechende Handlungsmöglichkeiten entwickeln konnten.

Zur **Identifizierung kritischer Prozesse und ihrer IT-Abhängigkeiten** wurde im UP KRITIS darüber hinaus eine Studie erstellt, in der für ausgewählte Branchen die kritischen Prozesse ermittelt und ein Überblick über deren Abhängigkeitsgeflecht gegeben wurde. Die Studie wurde 2012 abgeschlossen und bildet seither die Basis für weiterführende Untersuchungen und Maßnahmen. Die Studie ist Grundlage für einen Überblick über die kritischen Dienstleistungen in Deutschland (einschließlich der Abhängigkeiten voneinander), der die Planung von geeigneten Maßnahmen gegen Versorgungsausfälle im Interesse der Bevölkerung unterstützt.

Um eine **bessere nationale und internationale Zusammenarbeit** zu gewährleisten, wurde das Plenum regelmäßig über relevante europäische Aktivitäten zum Schutz Kritischer Infrastrukturen informiert. Die Auswirkungen auf Deutschland wurden im Plenum diskutiert, teilweise wurden eigene Positionen entwickelt, die das BSI in die EU-Gremien transportiert hat. Für die Teilnehmer des UP KRITIS wurde damit die Möglichkeit geschaffen, auf europäischer Ebene im Sinne der Interessen Deutschlands frühzeitig Einfluss auf dortige Entscheidungen mit Bezug zum UP KRITIS zu nehmen.

Grundlage für die erfolgreiche inhaltliche Arbeit waren einige organisatorische Rahmensetzungen:

» Mit den Grundsätzen zur Zusammenarbeit im Rahmen des Umsetzungsplans KRITIS und der Unterzeichnung einer Vereinbarung zum „Traffic Light Protocol“ (TLP) durch alle UP-KRITIS-Mitglieder wurde eine **verlässliche Grundlage für die Zusammenarbeit im UP KRITIS unter Wahrung der notwendigen Vertraulichkeit etabliert.**

» Zur Unterstützung des Plenums und der Arbeitsgruppen wurde zudem eine **technische Plattform zum Informations- und Dokumentenaustausch sowie zur Diskussion** eingerichtet, die den UP-KRITIS-Mitgliedern Zugriff auf Dokumente, Protokolle und andere Ergebnisse aus der gemeinsamen Arbeit ermöglicht.

» Die **Geschäftsstelle** im BSI hat die umfangreichen Arbeiten in den Arbeitsgruppen und Unterarbeitsgruppen unterstützt und administrative Tätigkeiten übernommen.

Der Schutz Kritischer Infrastrukturen steht ebenso wie das Thema „Cyber-Sicherheit“ heute im Fokus von Politik und Wirtschaft. Nicht zuletzt durch die langjährige Arbeit des UP KRITIS ist in allen Bereichen unserer Gesellschaft das Bewusstsein für die Notwendigkeit, Kritische Infrastrukturen in Deutschland besonders zu schützen, gewachsen. Da die Bedeutung der IT beim Betrieb der Kritischen Infrastrukturen weiterhin zunimmt, kommen auf den UP KRITIS kontinuierlich neue Herausforderungen zu. Um diese zu meistern und um die aufgebauten Strukturen erfolgreich fortzuführen, wurden die Ziele und Maßnahmen 2013 mit der Fortschreibung im Hinblick auf die aktuellen Bedürfnisse überarbeitet.

3 Vision

3 Vision

Die Partnerschaft UP KRITIS leistet seit ihrem offiziellen Start im Jahr 2007 einen wesentlichen Beitrag zur verlässlichen Bereitstellung der kritischen Dienstleistungen für die Bevölkerung in Deutschland. Der Schwerpunkt liegt dabei auf einem effektiven Zusammenwirken von IT-Sicherheit und der Aufrechterhaltung kritischer Geschäftsprozesse (BCM). Leitbild des UP KRITIS ist die Zusammenarbeit der Betreiber Kritischer Infrastrukturen mit staatlichen Stellen zur Stärkung der Kompetenz der deutschen Wirtschaft und der Bundesregierung in gemeinsamer Verantwortung insbesondere für die IT-Sicherheit in den Prozessen Kritischer Infrastrukturen.

Verschiedene Maßnahmen sollen dazu beitragen, dass alle Betreiber Kritischer Infrastrukturen ein hohes Sicherheitsniveau im Allgemeinen und der in den Unternehmen eingesetzten IT im Besonderen bewahren und angemessen weiter entwickeln. Die langfristige Zusammenarbeit zur Erkennung und Bewältigung von IT-Krisen soll sowohl branchenintern als auch branchen- und sektorübergreifend gemeinsam mit der Bundesregierung gefördert werden. Die Zusammenarbeit im UP KRITIS folgt dabei der Vision:

In gemeinsamer Verantwortung von Staat und Wirtschaft leistet der UP KRITIS einen zentralen Beitrag zum Schutz der Kritischen Infrastrukturen mit dem Ziel, die Versorgung der Bevölkerung mit wichtigen, teils lebenswichtigen Gütern und Dienstleistungen (kritischen Dienstleistungen) sicherzustellen sowie erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen zu vermeiden.

Aufgrund der Bedeutung der Informationstechnik für kritische Prozesse bildet dabei die IT in den kritischen Prozessen den Schwerpunkt der Arbeiten.

In den letzten Jahren hat sich gezeigt, dass eine getrennte Betrachtung der physischen Sicherheit und der IT-Sicherheit für das gemeinsame Ziel „Schutz Kritischer Infrastrukturen“ nicht ausreichend ist. Unumgänglich für den Erfolg von Maßnahmen und Projekten zur Sicherheit der kritischen Prozesse ist die Zusammenarbeit aller relevanten Akteure: das heißt die Zusammenarbeit der auf IT und IT-Sicherheit spezialisierten Bereiche mit den Experten für den physischen Schutz, für die Aufrechterhaltung der Geschäftsprozesse (BCM) und für das Krisenmanagement.

Die Betrachtung der kritischen Prozesse im UP KRITIS soll den präventiven Aspekt, d. h. die Vermeidung von Ausfällen Kritischer Infrastrukturen stärken, die Reaktion auf Dennoch-Ausfälle verbessern und auf Nachhaltigkeit ausgelegt sein, um die Verfügbarkeit der Kritischen Infrastrukturen zu gewährleisten. Hierzu nimmt die KRITIS-Wirtschaft ihre Verantwortung im UP KRITIS wahr und arbeitet eigenverantwortlich an der Umsetzung der vorgegebenen Ziele. Der Staat unterstützt die Arbeit der Wirtschaft im UP KRITIS und gleicht deren Ergebnisse mit den staatlichen Erfordernissen zum KRITIS-Schutz ab.

In dem Bewusstsein, dass einzelne Akteure aus Staat und Wirtschaft alleine nicht so widerstandsfähig agieren können wie eine gut vernetzte Gruppe, soll der UP KRITIS weiter gestärkt und ausgebaut werden.

4 Ziele

4 Ziele

Der UP KRITIS verfolgt das zentrale Ziel, die Resilienz der Kritischen Infrastrukturen, und hier insbesondere die Resilienz der kritischen Informationsinfrastrukturen, zu erhöhen und auf einem hohen, der Bedeutung der Kritischen Infrastruktur angemessenen Niveau zu stabilisieren.

Resiliente Kritische Infrastrukturen sind widerstandsfähig gegen Störungen jeder Art, passen sich neuen Bedingungen an und reagieren flexibel auf Veränderungen, um die Versorgungssicherheit der Bevölkerung möglichst uneingeschränkt gewährleisten zu können.

Zur Erreichung dieses Gesamtziels wurden von den Beteiligten Unterziele in verschiedenen Bereichen definiert, die in den nachfolgenden Abschnitten beschrieben sind.

Im Anhang werden einzelne Maßnahmen beschrieben, die in den nächsten Jahren umgesetzt werden sollen. Dabei wird sowohl auf strategisch-konzeptioneller als auch auf operativ-technischer Ebene gearbeitet. Die strategisch-konzeptionellen Maßnahmen werden in den Gremien des UP KRITIS bearbeitet, die operativ-technischen Maßnahmen werden durch die beteiligten Organisationen bzw. über die im UP KRITIS zwischen den Teilnehmern aufgebauten Kommunikationsstrukturen umgesetzt.

4.1 Gemeinsame Analysen, Empfehlungen und Vorgaben

Es ist eine strategische Aufgabe der Unternehmen, die Robustheit der ihren Prozessen zugrunde liegenden IT-Systeme zu gewährleisten. Der UP KRITIS wird sich über Standards, Normen und bewährte Vorgehensweisen austauschen sowie Analysen, Empfehlungen und Vorgaben zur Verbesserung der IT-Sicherheit Kritischer Infrastrukturen erarbeiten und umsetzen. Bei Bedarf werden zudem diesbezügliche Forschungsaktivitäten begleitet und unterstützt.

Aufgrund der zentralen Bedeutung und der Allgegenwärtigkeit von IT-Komponenten soll deren Widerstandsfähigkeit insbesondere in den kritischen Geschäftsprozessen gefördert und deren Toleranz gegenüber Störungen gestärkt werden. Soweit erforderlich, will der UP KRITIS bestehende Analysen um bisher nicht in die Betrachtung einbezogene Prozesse und deren IT-Abhängigkeiten erweitern.

Die am UP KRITIS Beteiligten setzen sich darüber hinaus das Ziel, die langfristige Bedrohungs- und Risikosituation gemeinsam zu analysieren und zu bewerten, um so vorhandene und zu erwartende Risiken für die Versorgungssicherheit frühzeitig zu erkennen.

4.2 Gemeinsames Handeln gegenüber Dritten

Ziel des UP KRITIS ist es, Dritte dazu zu bewegen, durch ihre Handlungen zum Schutz der Kritischen Infrastrukturen und somit zur Versorgungssicherheit beizutragen. Hierbei kann es sich z. B. um europäische Institutionen, Hersteller von Produkten oder Dienstleister handeln.

Aus dieser Motivation heraus sollen gemeinsame Interessen und Positionen im UP KRITIS identifiziert und abgestimmt werden, die als Grundlage für ein gemeinsames und effektives Auftreten gegenüber Dritten dienen.

4.3 Gemeinsame Lageeinschätzung

Die Mitglieder des UP KRITIS verfolgen das Ziel, sich über Vorkommnisse auszutauschen, die aktuelle Bedrohungs- und Risikosituation gemeinsam zu analysieren und zu bewerten und somit jederzeit über eine einheitliche Einschätzung der IT-Sicherheitslage der Kritischen Infrastrukturen zu verfügen.

4.4 Koordinierte Krisenreaktion und -bewältigung

Alle am UP KRITIS beteiligten Organisationen haben das Ziel, Krisenmanagementstrukturen zu etablieren bzw. etablierte Strukturen zu optimieren und zu betreiben.

Um auf potentielle Krisen optimal vorbereitet zu sein, setzt sich der UP KRITIS das Ziel, diese Krisenmanagementstrukturen branchen- und sektorübergreifend zu verknüpfen sowie insbesondere gemeinsame Krisenkommunikationsstrukturen und -prozesse weiter auszubauen. Bei Bedarf werden hierzu weitere Branchen-SPOC etabliert.

Durch die operativ-technische Zusammenarbeit im UP KRITIS sollen zudem eingetretene Krisen gemeinsam und schnell bewältigt werden.

4.5 Notfall- und Krisenübungen

Der UP KRITIS setzt sich das Ziel, verschiedenartige Notfall- und Krisenübungen gemeinsam zu planen und durchzuführen, an nationalen und internationalen Übungen Dritter teilzunehmen oder deren Ergebnisse auszuwerten. Bei Übungen wird insbesondere erprobt, ob die vereinbarten Kommunikationsbeziehungen aufgebaut und aufrechterhalten werden können und ob die gemeinsamen Krisenmanagementstrukturen und -prozesse effizient und effektiv sind.

4.6 Ausweitung der Branchenabdeckung

Der UP KRITIS verfolgt das Ziel, alle KRITIS-Branchen angemessen in die Zusammenarbeit einzubinden. Nur so kann die Versorgungssicherheit in Deutschland umfassend gewährleistet werden.

4.7 Vertrauensvolle Zusammenarbeit

Die am UP KRITIS beteiligten Organisationen arbeiten auf der Basis gegenseitigen Vertrauens stringent und zielorientiert zusammen. Diese vertrauensvolle Zusammenarbeit soll auch in Zukunft fortgeführt und weiter ausgebaut werden. Der UP KRITIS verfolgt damit das Ziel, dass die Beteiligten voneinander im Hinblick auf den Schutz Kritischer Infrastrukturen lernen und gemeinsam zu besseren Lösungen kommen. Hierfür finden im UP KRITIS ein Erfahrungsaustausch und ein zielgerichteter Know-how-Transfer statt.

5 Organisationsstruktur

5 Organisationsstruktur

Seit Beginn der Zusammenarbeit im UP KRITIS haben sich die teilnehmenden Unternehmen, Verbände und Behörden zur Erreichung der vereinbarten Ziele regelmäßig in Arbeitsgruppen getroffen; parallel dazu wurden spezielle Themen in Unterarbeitsgruppen bearbeitet, die aus den Arbeitsgruppen initiiert wurden. Inhaltlich hat sich diese Arbeitsweise bewährt. Sie erlaubt jedoch keine weitere Ausdehnung des Teilnehmerkreises, da die Anzahl der Teilnehmer in den Arbeitsgruppen sonst zu groß wäre.

Der UP KRITIS verfolgt jedoch das Ziel, möglichst viele Organisationen aus allen KRITIS-Branchen zu erreichen. Daher wird mit der Fortschreibung des UP KRITIS eine neue Organisationsstruktur eingeführt, die fortan eine einfache Aufnahme neuer Organisationen in den UP KRITIS erlaubt und gleichzeitig ein effektives Arbeiten in einer modifizierten Gremienstruktur sicherstellt.

5.1 Aufnahme einer Organisation in den UP KRITIS

Die Aufnahme in den UP KRITIS erfolgt zunächst als Teilnehmer. Bei Wunsch zur aktiveren Mitarbeit kann eine Organisation darauf aufbauend auch Partner im UP KRITIS werden.

5.1.1 Teilnehmer des UP KRITIS

Alle Organisationen mit Sitz in Deutschland, die Kritische Infrastrukturen in Deutschland betreiben, nationale Fach- und Branchenverbände aus den KRITIS-Sektoren sowie die zuständigen Behörden können beantragen, Teilnehmer des UP KRITIS zu werden. Teilnehmer benennen für ihre Organisation Vertreter, die Zugriff auf Produkte des UP KRITIS sowie auf das Informationsangebot der Allianz für Cyber-Sicherheit einschließlich der darin enthaltenen vertraulichen Inhalte erhalten. Insbesondere erhalten alle Teilnehmer des UP KRITIS die vom BSI bereitgestellten Lageinformationen und Warnmeldungen zur IT-Sicherheit.

Um das gemeinsame IT-Lagebild zu stärken, sollen alle Teilnehmer das BSI über gravierende IT-Sicherheitsvorfälle informieren.

5.1.2 Partner im UP KRITIS / Mitglied in einem Arbeitskreis

Die Teilnehmer des UP KRITIS können für ihre Vertreter die Aufnahme in Branchenarbeitskreise (BAK) und Themenarbeitskreise (TAK) beantragen, um sich an brancheninternen oder themenspezifischen Aktivitäten im UP KRITIS aktiv zu beteiligen. Um den Austausch mit der Länderebene zu verstetigen, können auch Vertreter der Länder von den Arbeitskreisen eingeladen werden.

Werden Vertreter eines Teilnehmers (d.h. einer teilnehmenden Organisation) als Mitglied in einen Arbeitskreis des UP KRITIS aufgenommen, so werden diese Organisationen Partner im UP KRITIS.

Alle Mitglieder der Arbeitskreise arbeiten aktiv und selbständig an den Zielen und Projekten des UP KRITIS mit. Jeder Arbeitskreis des UP KRITIS bildet einen eigenen Informationsverbund, innerhalb dessen Informationen vertraulich ausgetauscht werden können.

5.2 Formen der Zusammenarbeit im UP KRITIS

Im UP KRITIS wird zwischen zwei Formen der Zusammenarbeit unterschieden:

» der operativ-technischen Zusammenarbeit zwischen allen Teilnehmern des UP KRITIS sowie

» der strategisch-konzeptionellen Zusammenarbeit in den eingerichteten Gremien.

5.2.1 Strukturen zur operativ-technischen Zusammenarbeit im UP KRITIS

Auf operativ-technischer Ebene werden die bewährten Strukturen des UP KRITIS weitergeführt: Branchen können SPOC etablieren, die den Informationsaustausch mit den Unternehmen ihrer Branche übernehmen. Unternehmen aus Branchen ohne SPOC können direkt mit dem BSI Informationen austauschen. Der Ablauf der Kommunikation bleibt in der bisherigen Form, wie in Abbildung 2 gezeigt, erhalten.

Alle Teilnehmer des UP KRITIS beteiligen sich an der operativ-technischen Zusammenarbeit.

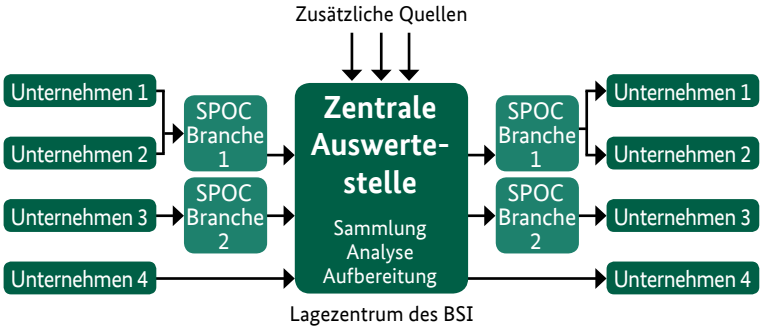


Abbildung 2: Kommunikationsstruktur der operativ-technischen Zusammenarbeit im UP KRITIS

5.2.2 Gremien zur strategisch-konzeptionellen Mitarbeit im UP KRITIS

Zentrale Bestandteile der neuen Organisationsstruktur sind Arbeitskreise für den fachlichen Austausch, das branchenübergreifende Plenum und ein auf hoher Ebene eingerichteter Rat (siehe Abbildung 3). Der Stab und die Geschäftsstelle unterstützen diese Gremien.

Die strategisch-konzeptionelle Mitarbeit obliegt den Partnern im UP KRITIS.

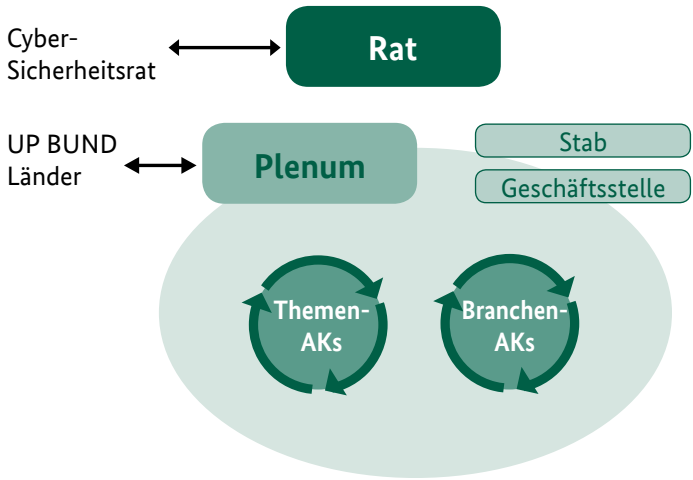


Abbildung 3: Neue Organisationsstruktur des UP KRITIS

Branchenarbeitskreise

In jeder KRITIS-Branche soll ein geeigneter Branchenarbeitskreis (BAK) zu IT-/Cyber-Sicherheit existieren[1]. Dieser kann sich zusätzlich auch mit verwandten Themen wie BCM, Krisenmanagement und Notfallplanung beschäftigen. Der BAK dient innerhalb der Branche sowie mit den zuständigen Behörden insbesondere der Vernetzung, dem vertrauensvollen Informationsaustausch und der Entwicklung gemeinsamer Positionen und Dokumente (z. B. Rahmenwerke für die Branche). Existieren in Branchen außerhalb des UP KRITIS bereits Arbeitskreise zu IT-/Cyber-Sicherheit, werden diese eingeladen, mit dem UP KRITIS zusammenzuarbeiten bzw. direkt im UP KRITIS mitzuwirken. Gibt es in einer Branche noch keinen BAK zu IT-/Cyber-Sicherheit, dann soll ein solcher durch UP-KRITIS-Teilnehmer aus der Branche gegründet werden.

Themenarbeitskreise

Themenarbeitskreise (TAK) dienen dem branchenübergreifenden, vertrauensvollen Informationsaustausch und der Entwicklung gemeinsamer Positionen und Dokumente. TAK werden zu sektor- und branchenübergreifenden Themen gegründet (z. B. Industrielle Steuerungssysteme, Übungen, SPOC-Erfahrungsaustausch, BCM, Krisenmanagement).

Plenum

Das Plenum ist das branchen- und themenübergreifende Kooperationsgremium des UP KRITIS. Es dient dem Informationsaustausch, setzt die strategischen Arbeitsschwerpunkte des UP KRITIS, entscheidet über Gründung oder Auflösung von TAK sowie über die Anbindung von BAK, führt die Ergebnisse der Arbeitskreise zusammen, ermöglicht einen Austausch zwischen diesen und plant das weitere gemeinsame Vorgehen.

1 Bei Bedarf können Branchenarbeitskreise auch mehrere Branchen umfassen.

Das Plenum setzt sich aus Vertretern der KRITIS-Betreiber, ihrer Fach- und Branchenverbände und des Staates zusammen. Mitglieder des Plenums sind insbesondere die Sprecher der Arbeitskreise sowie die Mitglieder des Stabs und der Geschäftsstelle. Für die Verbindung zum UP Bund und zu den Ländern soll jeweils eine fest benannte Verbindungsperson als ständiger Gast am Plenum teilnehmen. Weitere Gäste (z. B. aus der Forschung) können anlassbezogen zum Plenum eingeladen werden.

Stab

Zwischen den Plenumssitzungen koordiniert der Stab die Fortsetzung der Arbeiten und bereitet strategische Ziele und Maßnahmen vor. Mitglieder des Stabs sind drei vom Plenum gewählte Vertreter der Wirtschaft sowie je ein Vertreter von BMI, BSI und BBK.

Geschäftsstelle

Die Geschäftsstelle ist Dienstleister für organisatorische Belange im UP KRITIS. Sie wird vom BSI betrieben und unterstützt insbesondere Rat, Stab und Plenum.

Rat

Der Rat stärkt die partnerschaftliche Zusammenarbeit im UP KRITIS und gibt Impulse für strategische Ziele und Projekte im UP KRITIS. Darüber hinaus setzen sich die Mitglieder des Rates im Unternehmen, in der Branche und bei den Interessenvertretern in Politik und Wirtschaft für die personellen, organisatorischen und finanziellen Belange des UP KRITIS ein, damit dieser seine Aufgaben im Interesse des Schutzes der Kritischen Infrastrukturen mit angemessenen Ressourcen und der erforderlichen Unterstützung des Managements aus Wirtschaft und Staat erfüllen kann. Hierzu wird der Rat auch ein Mitglied in den Cyber-Sicherheitsrat entsenden. Der Rat setzt sich aus hochrangigen Entscheidungsträgern der Betreiber Kritischer Infrastrukturen und des Staates zusammen.

6 Zusammenfassung und Ausblick

6 Zusammenfassung und Ausblick

Kritische Infrastrukturen (KRITIS) sind die Lebensadern unserer Gesellschaft. Sie sind für das Funktionieren von Staat, Wirtschaft und Gesellschaft in Deutschland von zentraler Bedeutung. Da ihr Ausfall oder ihre Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen nach sich ziehen könnte, ist die Aufrechterhaltung der Versorgung der Bevölkerung mit kritischen Dienstleistungen eine wichtige nationale Aufgabe.

Die Betreiber Kritischer Infrastrukturen sind sich dieser Verantwortung bewusst. Sie verfolgen daher mit hoher Priorität das Ziel, die kritischen Dienstleistungen störungsfrei zu erbringen.

Die Bundesregierung hat die Notwendigkeit für die gemeinsame Wahrnehmung dieser Verantwortung erkannt und deshalb im Jahr 2005 den „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) verabschiedet, aus dem in den Jahren 2005 und 2006 der Umsetzungsplan KRITIS (UP KRITIS) entstand. Seither arbeiten Staat und Wirtschaft in enger Partnerschaft gemeinsam an der kontinuierlichen Verbesserung des (IT-)Schutzes der Kritischen Infrastrukturen. Im Rahmen des UP KRITIS werden Kontakte geknüpft, Konzepte entwickelt, Übungen abgehalten sowie ein gemeinsames Vorgehen zum (IT-)Krisenmanagement erarbeitet und etabliert. Zwischen den Beteiligten hat sich ein Netzwerk des Vertrauens gebildet, in dem Erfahrungen und (vertrauliche) Informationen ausgetauscht werden und ein Know-how-Transfer stattfindet. Dadurch lernen alle Beteiligten voneinander und kommen so zu besseren Lösungen.

Auf operativer Ebene entstand eine enge Kooperation, bei der sektorübergreifend Krisenmanagementstrukturen aufgebaut wurden, die inzwischen, auch über mehrere SPOC, in den Branchen verankert sind. Gemeinsame Übungen zeigten Optimierungsbedarf auf, bewiesen aber auch die Wirksamkeit der schon aufgebauten Strukturen und Prozesse, die sich auch in Reallagen bewährt haben.

Die branchenübergreifende Zusammenarbeit ist ein wichtiger Mehrwert des UP KRITIS und soll auch in Zukunft gepflegt und ausgebaut werden. Um zukünftig einen größeren Teilnehmerkreis zu erreichen, hierbei aber weiterhin arbeitsfähig zu bleiben, wurde eine neue Organisationsstruktur mit einem zweistufigen Teilnahmemodell geschaffen, die es erlaubt, alle Betreiber Kritischer Infrastrukturen in Deutschland als Teilnehmer in den UP KRITIS aufzunehmen. Teilnehmer erhalten Lageinformationen und Warnmeldungen zur IT-Sicherheit vom BSI und können sich im Rahmen der operativen Zusammenarbeit anlassbezogen über besondere Vorkommnisse austauschen. Darüber hinaus können ihre Vertreter in Branchen- und Themenarbeitskreisen mitarbeiten, die sich brancheninternen bzw. branchenübergreifenden Themen widmen.

In den vergangenen sechs Jahren hat sich die Cyber-Bedrohungslage massiv verschärft. Vorfälle wie Stuxnet, Duqu und weitere zeigen, dass Kritische Infrastrukturen zunehmend in den Fokus der Angreifer geraten. Gleichzeitig nehmen auch Angriffe durch große Organisationen oder Staaten weiterhin zu. Auf diese Professionalisierung der Angreifer müssen Staat und Wirtschaft adäquat reagieren. Mit der Cyber-Sicherheitsstrategie hat die Bundesregierung 2011 diverse Maßnahmen in die Wege geleitet, und auch der UP KRITIS stellt sich mit der Fortschreibung auf diese neuen Rahmenbedingungen ein.

Die gemeinsame Arbeit im UP KRITIS hat deutlich gezeigt, dass eine ausschließliche Betrachtung von IT-/Cyber-Sicherheit nicht zielführend ist: IT- und physische Sicherheit müssen gemeinsam gedacht und gelebt werden. Daher widmet sich der UP KRITIS neben dem zentralen Thema IT-/Cyber-Sicherheit auch anderen Sicherheitsthemen wie dem physischen KRITIS-Schutz und der Aufrechterhaltung der kritischen Geschäftsprozesse (BCM).

Für die nächsten Jahre hat sich der UP KRITIS neue Ziele gesetzt: Neben dem Ausbau der vertrauensvollen Zusammenarbeit und der Ausweitung der Branchenabdeckung durch die Erweiterung des Teilnehmerkreises sind dies die Durchführung von Übungen, die gemeinsame Lageeinschätzung, die Erarbeitung gemeinsamer Analysen, Empfehlungen und Vorgaben, die koordinierte Krisenreaktion und -bewältigung sowie das gemeinsame Handeln gegenüber Dritten. Dazu soll auch die Sichtbarkeit des UP KRITIS auf nationaler und europäischer politischer Ebene erhöht werden. Durch einen Sitz des UP KRITIS im Cyber-Sicherheitsrat wird seine Bedeutung auf politischer Ebene gestärkt.

Der UP KRITIS hat sich zu einem Erfolgsmodell einer öffentlich-privaten Partnerschaft entwickelt und gezeigt, wie eine vertrauensvolle branchen- und sektorübergreifende Zusammenarbeit zwischen Wirtschaft und Staat auf freiwilliger Basis funktionieren kann.

Durch die aktualisierten Ziele und Aufgaben, seine neue Organisationsstruktur und die überarbeiteten Grundsätze der Zusammenarbeit ist der UP KRITIS gut aufgestellt, um die Resilienz der deutschen Kritischen Infrastrukturen auch zukünftig zu erhöhen bzw. auf einem hohen, der Bedeutung der Kritischen Infrastrukturen angemessenen Niveau zu stabilisieren und den (Cyber-)Herausforderungen der kommenden Jahre effektiv zu begegnen.

7 Abkürzungsverzeichnis

7 Abkürzungsverzeichnis

AKNZ	Akademie für Krisenmanagement, Notfallplanung und Zivilschutz des BBK
BAK	Branchenarbeitskreis
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management (Aufrechterhaltung der Geschäftsprozesse)
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
IT	Informationstechnik
IKT	Informations- und Kommunikationstechnik
KRITIS	Kritische Infrastrukturen
LÜKEX	Länderübergreifende Krisenmanagement Übung/ Exercise
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
SPOC	Single Point of Contact
TAK	Themenarbeitskreis
TLP	Traffic Light Protocol
UP KRITIS	Bezeichnung (Name) für die in diesem Dokument beschriebene Zusammenarbeit von Wirtschaft und Staat

8 Literatur

8 Literatur

» Bundesministerium des Innern (Hrsg.):
Nationale Strategie zum Schutz Kritischer Infrastrukturen.
Berlin, 2009

» Bundesministerium des Innern (Hrsg.):
Cyber-Sicherheitsstrategie für Deutschland.
Berlin, 2011

» Bundesministerium des Innern (Hrsg.):
Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informations-infrastrukturen.
Berlin, 2007

» Bundesministerium des Innern (Hrsg.):
Früherkennung und Bewältigung von IT-Krisen.
Berlin, 2008

» Bundesministerium des Innern (Hrsg.):
IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen.
Berlin, 2008

» Bundesministerium des Innern (Hrsg.):
Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden.
2. Aufl. Berlin, 2011

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

Alle Dokumente sind auf www.upkritis.de
unter „Publikationen“ verlinkt

9 Glossar

9 Glossar

All-Gefahrenansatz *(engl. all-hazard approach)*	Berücksichtigung aller (bekannten) Gefahren gleichermaßen, z. B. bei Durchführung einer Risikoanalyse, und nicht nur einzelner Bereiche wie Terrorismus oder Sabotage.
Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Betreiber Kritischer Infrastrukturen sind (privatwirtschaftliche oder öffentlich-rechtliche) Organisationen aus den Branchen der Kritischen Infrastrukturen, die Einrichtungen betreiben, die für das Funktionieren der kritischen Dienstleistungen erforderlich sind.
Cyber-Sicherheit	(Globale) Cyber-Sicherheit ist der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind. Cyber-Sicherheit in Deutschland ist demnach der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind. Cyber-Sicherheit (in Deutschland) entsteht durch die Summe von geeigneten und angemessenen Maßnahmen.
Informationstechnik (IT)	Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören die Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung, Ausgabe und die Löschung von Informationen.
IT-Abhängigkeit	IT-Abhängigkeit eines Prozesses besteht genau dann, wenn die erfolgreiche Durchführung des Prozesses vom ordnungsgemäßen Funktionieren von IT abhängt.

Informations-infrastruktur	Gesamtheit der IT-Anteile einer Infrastruktur.
Infrastruktur	Infrastruktur bezeichnet alle staatlichen und privaten Einrichtungen, die für eine ausreichende Daseinsvorsorge und wirtschaftliche Entwicklung als erforderlich gelten. Die Infrastruktur wird meist unterteilt in technische Infrastruktur (z. B. Einrichtungen der Verkehrs- und Nachrichtenübermittlung, der Energie- und Wasserversorgung oder der Entsorgung) und soziale Infrastruktur (z. B. Schulen, Krankenhäuser, Einkaufsstätten oder kulturelle Einrichtungen).
Interdependenz	Eine Interdependenz ist die gegenseitige vollständige oder partielle Abhängigkeit mehrerer Güter oder Dienstleistungen.
IT-Sicherheit	IT-Sicherheit ist der Zustand, in dem Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Informationstechnik durch angemessene Maßnahmen gewährleistet sind.
IT-Krise	Eine IT-Krise im Kontext des UP KRITIS liegt vor, wenn mittelbar oder unmittelbar IT-bedingt 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 beziehungsweise zu erwarten ist.

Kritische Infrastrukturen	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 einträten. In Deutschland werden folgende Sektoren (und Branchen) den Kritischen Infrastrukturen zugeordnet: » Transport und Verkehr (Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik) » Energie (Elektrizität, Mineralöl, Gas) » Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnik) » Finanz- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen) » Staat und Verwaltung (Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall- und Rettungswesen einschließlich Katastrophenschutz) » Ernährung (Ernährungswirtschaft, Lebensmittelhandel) » Wasser (Öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung) » Gesundheit (Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore) » Medien und Kultur (Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke)

Kritische Dienstleistungen *(engl. vital services)*	Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der Öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten.
Kritischer Prozess	Kritische (Geschäfts-)Prozesse sind Fachaufgaben, die eine hohe Bedeutung für die Wertschöpfung der Institution haben. Die Klassifizierung in unkritische, wenig kritische, kritische und hoch kritische Geschäftsprozesse kann z. B. anhand bekannter Schadensszenarien aus der Schutzbedarfsfeststellung nach IT-Grundschutz erfolgen.
Resilienz	Resilienz ist die Fähigkeit eines Systems, mit Veränderungen umgehen zu können. Resilienz bedeutet Widerstandsfähigkeit gegen Störungen jeder Art, Anpassungsfähigkeit an neue Bedingungen und eine flexible Reaktion auf Veränderungen mit dem Ziel, das System – z. B. einen Betrieb oder einen Prozess – aufrecht zu erhalten.
UP KRITIS	Der UP KRITIS ist die Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland.

Umsetzungsplan KRITIS	Resultierend aus dem 2005 vom BMI veröffentlichten Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) wurde in den Folgejahren der Umsetzungsplan KRITIS geschrieben, der den UP KRITIS, die Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen, beschreibt. Der Umsetzungsplan wurde 2007 veröffentlicht und wird durch die Veröffentlichung des vorliegenden Dokuments abgelöst.
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.

10 Anhang: Konkretisierung der Ziele durch Maßnahmen

10 Anhang: Konkretisierung der Ziele durch Maßnahmen

Zur Realisierung der beschriebenen Ziele sollen die folgenden Maßnahmen in den beteiligten Organisationen, in der operativ-technischen Zusammenarbeit der Teilnehmer sowie in den Gremien des UP KRITIS umgesetzt werden.

10.1 Gemeinsame Analysen, Empfehlungen und Vorgaben

M1:		Auf Grundlage der Struktur und Aufgaben der KRITIS-Sektoren und ihrer Branchen soll – unter Berücksichtigung möglicher branchenübergreifender Interdependenzen – die Identifikation und Beschreibung der kritischen Dienstleistungen in den Branchen sowie der hierfür benötigten kritischen Prozesse fortgeführt werden. Die Identifizierung von weiteren kritischen Dienstleistungen und der hierfür benötigten kritischen Prozesse sowie deren IT-Abhängigkeiten soll, um eine Vergleichbarkeit für Folgemaßnahmen sicherzustellen, analog der bereits durchgeführten IKT-Studie in der Zuständigkeit der Branchenarbeitskreise erfolgen.
	M1.1:	Die Ergebnisse aus den Branchen werden anschließend branchenübergreifend betrachtet und bewertet.
M2:		Um geeignete Empfehlungen zum Schutz der kritischen Prozesse geben zu können, muss die mittel- und langfristige Bedrohungs- und Risikosituation über einen All-Gefahrenansatz analysiert und bewertet werden.

M3:		Der UP KRITIS entwickelt branchenspezifische Sicherheitsstandards zum Schutz derjenigen informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind. Bereits bestehende Regelungen, Standards, Rahmenwerke und Empfehlungen aus den einzelnen Branchen, insbesondere solche mit IT-Relevanz, werden einbezogen und mit Blick auf ihre Übertragbarkeit auch branchenübergreifend herangezogen.
	M3.1:	Hierzu sollen zunächst die Regelwerke in den Branchen zusammengestellt und miteinander verglichen werden.

In regelmäßigen Abständen soll – insbesondere mit Blick auf die IT-Relevanz – evaluiert werden, ob die identifizierten kritischen Prozesse und deren Abhängigkeiten Veränderungen erfahren haben und ob die anzuwendenden Regelwerke einer Überarbeitung bedürfen.

M4:		Um ein effizientes Benchmarking der Branchen im Hinblick auf ihre Resilienz durchführen zu können, wird die Entwicklung eines geeigneten und allgemein akzeptierten abstrakten Modells zum brancheninternen, aber auch branchenübergreifenden Vergleich angestrebt (z. B. ein Reifegradmodell).
	M4.1:	Ein solches konsentiertes Modell soll in allen Branchen einheitlich zur Anwendung kommen und muss deshalb Raum für branchenspezifische Anforderungen lassen.
	M4.2:	Die Ergebnisse des Benchmarking werden branchenübergreifend ausgetauscht und bewertet.
	M4.3:	Sollte sich daraus Handlungsbedarf ergeben, wird dieser in den Branchen aufgegriffen.

Auch der Informationsaustausch zu weiteren branchenspezifischen Vorgehensweisen und Ergebnissen, z. B. beim Risikomanagement, ist eine wesentliche Komponente, um „Best-Practice"-Vorgehensweisen zu etablieren.

M5:		Neben eigenen Analysen des UP KRITIS sollen auch externe Studien und Analysen, z. B. zu lang anhaltenden und großflächigen Ausfällen von IT-Kerntechnologien, dahingehend überprüft werden, ob und wie die Ergebnisse für den UP KRITIS nutzbar sind.

10.2 Gemeinsames Handeln gegenüber Dritten

Der effektive Schutz Kritischer Infrastrukturen erfordert neben den Arbeiten der Mitglieder des UP KRITIS auch angemessene Rahmenbedingungen in Bezug auf eine erhöhte Versorgungssicherheit und die Bereitstellung entsprechender Produkte und Dienstleistungen durch Dritte außerhalb des UP KRITIS.

M6:		Aus dieser Motivation heraus sollen gemeinsame Interessen und Positionen im UP KRITIS identifiziert und abgestimmt werden, um als Grundlage für ein gemeinsames und effektives Auftreten gegenüber Dritten dienen zu können.
M7:		Die Belange Kritischer Infrastrukturen und ihres besonderen Schutzbedarfes müssen nachhaltig gegenüber den zuständigen Stellen vertreten werden. Deshalb wird der UP KRITIS – soweit dies zielführend ist – zu aktuellen Themen mit KRITIS-Relevanz (z. B. zur IT-Sicherheitsperspektive bei technologischen Entwicklungen oder zu entsprechenden Initiativen der EU, des Bundes und der Länder) auf nationaler und internationaler Ebene Stellung beziehen und ggf. von Dritten Aktivitäten einfordern (z. B. zum Schließen von Schwachstellen in Produkten).

Der UP KRITIS wird seinerseits seine Ergebnisse und Erkenntnisse mit Dritten teilen. Diese Dritten können neben Partnerorganisationen auch beispielsweise Hersteller oder Forschungseinrichtungen sein.

10.3 Gemeinsame Lageeinschätzung

Die Teilnehmer des UP KRITIS sollen jederzeit über eine gemeinsame Einschätzung der IT-Sicherheitslage der Kritischen Infrastrukturen verfügen.

M8:		Dazu tauschen sie sich über aktuelle Vorkommnisse aus und analysieren und bewerten gemeinsam die jeweils vorliegende Bedrohungs- und Risikosituation.
M9:		Für den Austausch über aktuelle Vorkommnisse und Lagen sind Kommunikationsstrukturen (wie beispielsweise über SPOC) weiter aus- bzw. neu aufzubauen.
	M9.1:	Über diese Strukturen sollen Beobachtungen, Einschätzungen, Bedrohungen sowie Einschränkungen der Verfügbarkeit der kritischen Dienstleistungen von den KRITIS-Betreibern an das BSI gemeldet werden.
	M9.2:	Das BSI erstellt hieraus Lagebilder und Frühwarnungen und stellt diese zeitnah den KRITIS-Betreibern zur Verfügung.
	M9.3:	Darüber hinaus sollen Lagebilder Dritter analysiert und ggf. deren Informationen genutzt werden.
	M9.4:	Zur gemeinsamen Analyse und Bewertung der Bedrohungs- und Risikosituation sollen regelmäßig oder anlassbezogen Telefonkonferenzen zum Lagebild stattfinden, zu denen das BSI die IT-Sicherheitsverantwortlichen der KRITIS-Betreiber einlädt.

	M9.5:	Um den Informationsaustausch für alle Beteiligten effektiv und sinnvoll zu gestalten, müssen die Themen, Inhalte und Formate des Austauschs festgelegt werden. Dies erfolgt im Rahmen des TAK „Operativer Informationsaustausch“, in dem alle Beteiligten ihre Erwartungen formulieren und miteinander abgleichen.
M10:		Neben dem Austausch über Vorkommnisse und Lagen soll ein Austausch zu den Vorgehensweisen bei der Lagefortschreibung in allen Organisationen stattfinden. Hierzu ist es erforderlich, dass die CERTs und Lagezentren der KRITIS-Betreiber in der jeweiligen Organisation und organisationsübergreifend enger zusammenarbeiten, damit durch den Austausch von CERT-Informationen auch das nationale Lagewesen unterstützt wird.
M11:		Es soll ein Konzept für Bedrohungsanalysen und Prognosen erstellt werden, das dann von den beteiligten Organisationen genutzt werden kann. Die Erfahrungen bei der Anwendung dieses Konzepts sollen an den TAK „Operativer Informationsaustausch“ zurückgemeldet werden, um ggf. erforderliche Anpassungen vornehmen zu können.

10.4 Koordinierte Krisenreaktion und -bewältigung

M12:		Die Rahmenbedingungen für eine national koordinierte Krisenreaktion werden im Rahmen eines Themenarbeitskreises (TAK) weiterentwickelt.
M13:		Auf der Grundlage von szenarienbasierten Analysen soll die Krisenreaktion optimiert werden.
M14:		Es sollen geeignete Krisenmanagementstrukturen branchen- und sektorübergreifend etabliert, optimiert und betrieben werden, die im Krisenfall unverzüglich arbeitsfähig sein müssen. Hierzu zählt auch,
	M14.1:	die Krisenkommunikation weiter auf- und auszubauen,
	M14.2:	Krisenkommunikationsprozesse, -wege und -ansprechpartner zu definieren,
	M14.3:	eine 24/7-Erreichbarkeit zu gewährleisten,
	M14.4:	geeignete technische Systeme (z. B. ein Krisenkommunikationssystem inkl. Notfallkommunikation) einzuführen und
	M14.5:	bei Bedarf in weiteren Branchen SPOC zu etablieren.
M15:		Es ist zu prüfen, ob im Krisenfall eine operativ-technische Zusammenarbeit zwischen den KRITIS-Organisationen etabliert werden kann.
	M15.1:	Es sollen Handlungsanweisungen und Verfahren für eine Zusammenarbeit im Krisenfall entwickelt werden.
	M15.2:	Möglichkeiten zur gegenseitigen Unterstützung (z. B. durch Hilfestellung von Experten oder bereitgestellte Technik) sollen geschaffen werden.
M16:		Nach der Bewältigung einer Krise soll die Krisenkommunikation einschließlich der verwendeten technischen Systeme evaluiert und ggf. Verbesserungsmöglichkeiten gemeinsam umgesetzt werden.

10.5 Notfall- und Krisenübungen

Bei Übungen wird insbesondere erprobt, ob die vereinbarten Kommunikationsbeziehungen aufgebaut und aufrechterhalten werden können und ob die gemeinsamen Krisenmanagementstrukturen und -prozesse effizient und effektiv sind.

M17:		Im Rahmen des UP KRITIS werden verschiedenartige Notfall- und Krisenübungen gemeinsam geplant und durchgeführt.
	M17.1:	Es soll an nationalen und internationalen Übungen Dritter teilgenommen werden.
	M17.2:	Die Übungen müssen anschließend evaluiert, die Ergebnisse sollen in die Praxis umgesetzt werden.
M18:		Übungskonzepte und Ergebnisse von Übungen Dritter sollen im Hinblick auf ihre Relevanz für den UP KRITIS ausgewertet werden.
M19:		Es sollen Rahmenszenarien entwickelt und Übungsszenarien fortgeschrieben werden.
M20:		Für die Durchführung von Übungen wird das bestehende Übungskonzept fortgeschrieben.
	M20.1:	Für die verschiedenen Übungsarten werden spezifische Übungspläne erarbeitet, dabei werden feste Übungszyklen vereinbart. Zusätzlich können anlassbezogen Übungen durchgeführt werden.

10.6 Ausweitung der Branchenabdeckung

Da noch nicht alle KRITIS-Branchen in ausreichendem Umfang in die Gremienarbeit des UP KRITIS eingebunden sind, müssen derzeitige Defizite in Bezug auf die Branchenabdeckung identifiziert und zeitnah beseitigt werden.

M21:		Hierzu sollen Organisationen in bislang nicht oder kaum vertretenen Branchen gezielt angesprochen und zur Mitarbeit motiviert werden.
M22:		Zur Unterstützung wird ein Marketingkonzept für die Partnerschaft im UP KRITIS entwickelt.
M23:		Neben bereits bestehenden Arbeitskreisen des UP KRITIS sollen zur Vertiefung und Erweiterung der branchenspezifischen KRITIS-Zusammenarbeit weitere Branchenarbeitskreise gegründet werden.
	M23.1:	Bereits bestehende Branchenarbeitskreise außerhalb des UP KRITIS sollen darin bestärkt und unterstützt werden, Themen der IT-Sicherheit aufzugreifen; eine Zusammenarbeit dieser Branchenarbeitskreise mit dem UP KRITIS oder eine Assoziierung wird angestrebt.
	M23.2:	Durch ein Monitoring wird sichergestellt, dass der UP KRITIS jederzeit einen Überblick über die aktiven Branchenarbeitskreise und über die Fortschritte hinsichtlich der Branchenabdeckung hat.

10.7 Vertrauensvolle Zusammenarbeit

M24:		Im UP KRITIS tauschen sich Betreiber Kritischer Infrastrukturen und Vertreter staatlicher Stellen über politische, technologische und branchenspezifische aktuelle Fragen und Entwicklungen sowie deren Auswirkungen auf Kritische Infrastrukturen aus. Diesbezügliche Themen, die in Themenarbeitskreisen (TAK) behandelt werden sollen, werden vom Plenum des UP KRITIS beschlossen.

M25:		Die Mitglieder des UP KRITIS informieren sich gegenseitig vertraulich über Vorkommnisse, insbesondere über IT-/Cyber-Sicherheitsvorfälle, über Ausfälle von kritischen Dienstleistungen und über Bedrohungen, die zu solchen Ausfällen führen können.

Für den Austausch von Informationen haben sich die Vertreter der teilnehmenden Organisationen und die Mitglieder zur Vertraulichkeit gemäß Traffic Light Protocol (TLP) verpflichtet. Die weiteren Pflichten der Mitglieder im Rahmen der Zusammenarbeit sind in den parallel zur Fortschreibung überarbeiteten Grundsätzen der Zusammenarbeit geregelt.

Für den Austausch untereinander und zur Erleichterung der Kooperation kann für die Gremien des UP KRITIS eine geeignete technische Informationsplattform genutzt und bedarfsgerecht ausgebaut werden.

Bei der Bearbeitung von Themen, die dem Schutz Kritischer Infrastrukturen dienen, beziehen die Mitglieder des UP KRITIS auch bestehende interne und externe Arbeitsergebnisse ein.

Den Mitgliedern ist bewusst, dass das Know-how der Experten angesichts der sich ständig ändernden Bedrohungslage und der zunehmenden Bedeutung funktionierender IT für die Prozesse Kritischer Infrastrukturen fortlaufend aktualisiert werden muss.

M26:		Hierfür sollen Schulungen durchgeführt und gegenseitige Hospitationen ermöglicht werden, um voneinander lernen zu können.

Impressum

Herausgeber
Geschäftsstelle des UP KRITIS

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik
Geschäftsstelle UP KRITIS
Godesberger Allee 185-189
53175 Bonn
E-Mail: upkritis@bsi.bund.de
Internet: www.upkritis.de
Telefon: +49 (0) 22899 9582 5089
Telefax: +49 (0) 22899 109582 5088

Stand
Februar 2014

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
UP KRITIS
Themenarbeitskreis Fortschreibung

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

www.upkritis.de