Bundesministerium
des Innern

Nationaler Plan
zum Schutz der
Informationsinfrastrukturen
Umsetzungsplan KRITIS

Umsetzungsplan KRITIS

des Nationalen Plans zum Schutz der Informationsinfrastrukturen

www.bmi.bund.de

Umsetzungsplan KRITIS

des Nationalen Plans zum Schutz der Informationsinfrastrukturen

Inhalt

1. Einleitung und Zielsetzung

Kritische Infrastrukturen (KRITIS) sind die Lebensadern unserer Gesellschaft. Die verlässliche Bereitstellung der Dienstleistungen dieser Infrastrukturen ist eine Grundvoraussetzung für die wirtschaftliche Entwicklung in unserem Land, für das Wohlergehen unserer Gesellschaft und für politische Stabilität:

>> Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. [1]

Der Schutz Kritischer Infrastrukturen wird von Bundesregierung und Wirtschaft als wichtige nationale Aufgabe gesehen, weil die Innere Sicherheit immer stärker von der IT-Sicherheit beeinflusst wird. Es werden in Deutschland die notwendigen Anstrengungen unternommen, um die IT-Infrastrukturen angemessen abzusichern. Der Umsetzungsplan KRITIS leistet einen wesentlichen Beitrag zur verlässlichen Bereitstellung der lebensnotwendigen Dienstleistungen durch einen angemessenen IT-Schutz. Die an der Erstellung beteiligten Partner haben sich hierzu folgendes Leitbild gegeben:

>> Wir arbeiten zusammen, um die Kompetenz und das Know-how der deutschen Wirtschaft und der Bundesregierung in der gemeinsamen Verantwortung für die IT-Sicherheit in den Prozessen Kritischer Infrastrukturen zu beschreiben. Durch Empfehlungen und Maßnahmen soll dazu beigetragen werden, dass alle Betreiber Kritischer Infrastrukturen ein angemessen hohes Sicherheitsniveau der Informationsinfrastrukturen im Allgemeinen und der in den Unternehmen eingesetzten IT bewahren und weiter ausbauen können. Die langfristige Zusammenarbeit zur Erkennung und Bewältigung von IT-Krisen soll branchenübergreifend gemeinsam mit der Bundesregierung gefördert werden.

[1] Definition der Kritischen Infrastrukturen in Deutschland (siehe Glossar).
[2] Bundesministerium des Innern, Nationaler Plan zum Schutz der Informationsinfrastrukturen vom Juni 2005.

>> Unser Ziel ist es, dass sich die Betreiber Kritischer Infrastrukturen aktiv zu den gemeinsamen Grundsätzen bekennen und auf Basis der nachfolgenden Empfehlungen das IT-Sicherheitsniveau in den Kritischen Infrastrukturen noch weiter erhöhen.

1.1 Motivation des Umsetzungsplans KRITIS

Moderne Informationstechnik durchdringt in zunehmendem Maße alle Lebensbereiche. Auch in den Kritischen Infrastrukturen wird immer stärker auf den Einsatz von IT gesetzt, um Prozesse effektiver und effizienter betreiben, steuern und überwachen zu können. Daraus ergeben sich zum Teil hochkomplexe IT-basierte Vernetzungen und Abhängigkeiten innerhalb und zwischen den KRITIS-Branchen.

Der Schutz der Kritischen Infrastrukturen erfordert daher auch einen angemessenen Schutz der Informationsinfrastrukturen. Die Bundesregierung hat deswegen als übergreifende IT-Sicherheitsstrategie des Bundes den „Nationalen Plan zum Schutz der Informationsinfrastrukturen“[2] (NPSI) verabschiedet. Die Umsetzung des NPSI erfolgt im Konsens zwischen den privatwirtschaftlichen Zielsetzungen der Betreiber und dem übergeordneten (Fürsorge-)Interesse des Gemeinwesens.

Der NPSI betont den Schutz der Informationsinfrastrukturen als gesamtgesellschaftliche Aufgabe, die ein abgestimmtes und von allen Verantwortlichen unterstütztes Vorgehen erfordert. Er gibt drei strategische Ziele vor:

- Prävention: Informationsinfrastrukturen angemessen schützen
- Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln
- Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen

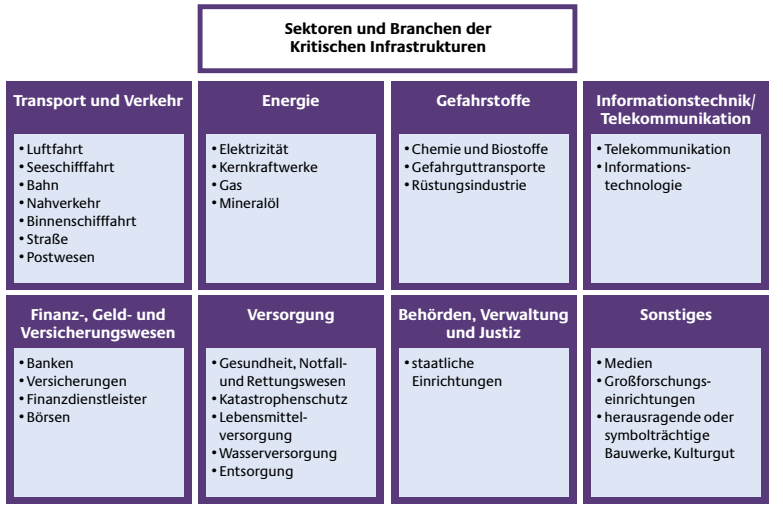
Angesprochen sind hier insbesondere die Bundesverwaltung und die Betreiber Kritischer Infrastrukturen. Die Kritischen Infrastrukturen in Deutschland sind größtenteils in privatwirtschaftlicher Verantwortung, das heißt in Verantwortung einzelner Unternehmen. IT-Sicherheit war bisher eine Aufgabe, die weitestgehend innerhalb einzelner Unternehmen und Organisationen erfüllt wurde. Diese Zuständigkeiten bleiben unberührt, müssen aber ergänzt werden.

Mit steigenden Abhängigkeiten und zunehmender unternehmensübergreifender Vernetzung von IT-Landschaften und Informationstechnologien wachsen die Anforderungen an IT-Management und IT-Sicherheitsmanagement. Demzufolge kann ein angemessener Schutz der Informationsinfrastrukturen in Deutschland – und weltweit – nicht mehr allein durch IT-Sicherheitsmaßnahmen in den Unternehmen und Organisationen erreicht werden. Vielmehr sind Maßnahmen auf mehreren Ebenen erforderlich:

- in den Unternehmen und Organisationen, um alle erforderlichen Vorkehrungen zu treffen, die in eigener Verantwortung erfolgen können,
- in den Branchen insbesondere dann, wenn die Anteile Kritischer Infrastrukturen verschiedener Unternehmen eng miteinander verflochten beziehungsweise voneinander abhängig sind, um durch abgestimmte und koordinierte Maßnahmen die Verlässlichkeit zu erhöhen,
- branchenübergreifend auf nationaler Ebene:
  - um Vorfälle (zum Beispiel Unfälle oder gezielte Angriffe) im größeren Zusammenhang richtig zu bewerten,
  - um gemeinsam und auf abgestimmte Weise auf Vorfälle reagieren zu können, die trotz der vorhandenen präventiven Maßnahmen auftreten,
  - um aus aktuellen Entwicklungen gemeinsam erforderliche Anpassungen der Maßnahmen zu entwickeln, die auch in der Fortschreibung des Umsetzungsplans KRITIS berücksichtigt werden,
- grenzüberschreitend, um Vorfälle, die nicht national begrenzt sind, richtig zu bewerten und angemessen darauf reagieren zu können:
  - innerhalb der Branchen gemeinsam mit anderen Unternehmen,
  - auf staatlicher Ebene in Abstimmung mit den Verantwortlichen anderer Staaten.

Das Bundesministerium des Innern hat daher Vertreter der Betreiber von Kritischen Infrastrukturen eingeladen, an der Entwicklung des Umsetzungsplans KRITIS mitzuwirken und ihren Sachverstand und ihre Erfahrungen, aber auch ihr Wissen um die besonderen Anforderungen der verschiedenen KRITIS-Branchen einzubringen.

Abbildung 1: Strukturierung Kritischer Infrastrukturen



Dieser gemeinsam erarbeitete Umsetzungsplan ist die Grundlage dafür, dass der Schutz der Informationsinfrastrukturen in den KRITIS-Branchen weiter verbessert und ein einheitlich hohes Basis-IT-Sicherheitsniveau erreicht wird.

Dabei sind sich alle Beteiligten ihrer gesamtgesellschaftlichen Verantwortung bewusst.

Der Umsetzungsplan KRITIS ist ein wesentlicher Beitrag Deutschlands zum angekündigten „Europäischen Programm für den Schutz Kritischer Infrastrukturen" (EPSKI). Nationale und internationale IT-Sicherheitsstrategien zum Schutz Kritischer Infrastrukturen sollen nach Möglichkeit aufeinander abgestimmt sein und sich ergänzen.

1.2 Adressaten

Der Umsetzungsplan KRITIS richtet sich grundsätzlich an die privatwirtschaftlichen Betreiber Kritischer Infrastrukturen. Dieses sind Unternehmen und Organisationen aus den Sektoren Transport und Verkehr, Energie, Gefahrstoffe, Informationstechnik und Telekommunikation, Finanz-, Geld- und Versicherungswesen, Versorgung und Sonstiges (Medien, Forschungsanlagen, Kulturgüter). Die Sektoren selbst sind in einzelne Branchen aufgeteilt (siehe Abbildung 1, Seite 7).

Wegen ihrer herausragenden gesellschaftlichen Bedeutung sind die Kritischen Infrastrukturen besonders zu schützen. Terroristische Bedrohungen, Umweltgefahren und IT-Gefährdungen sind zu berücksichtigen. Der Fokus des Umsetzungsplans KRITIS liegt dabei auf der Informationstechnik und den entsprechenden Schutzmaßnahmen im privatwirtschaftlichen Bereich. Für die Bundesverwaltung erstellt die Bundesregierung einen eigenen Umsetzungsplan (Umsetzungsplan Bund).

Die im nachfolgenden Kapitel beschriebenen Konzepte und Maßnahmen werden von den beteiligten Unternehmen als sinnvoll und auf dem „Stand der Technik" zur Sicherung der Informationstechnik eingeschätzt und sollten in allen KRITIS-Bereichen Anwendung finden. Die gemeinsam erarbeiteten Empfehlungen werden von den Verfassern des Umsetzungsplans KRITIS als notwendige Ergänzung zu bereits bestehenden Maßnahmen angesehen. Diese Empfehlungen sollten in erster Linie durch die Betreiber Kritischer Infrastrukturen in Zusammenarbeit mit der Bundesverwaltung umgesetzt werden. Die Umsetzung wird auch allen anderen Unternehmen und Branchen empfohlen, um ihre IT-Infrastruktur wirkungsvoll zu schützen.

1.3 Aufgabenteilung bei der Umsetzung von IT-Sicherheitsmaßnahmen

Die Aufgabenteilung für die Umsetzung von Maßnahmen kann für die einzelnen Ebenen folgendermaßen beschrieben werden:

- Unternehmen: Umsetzung von Maßnahmen in der jeweiligen Organisation
- Branchenebene: Betrachtung unternehmensübergreifender Aspekte, die mehrere Unternehmen der Branche betreffen
- branchenübergreifende Ebene: Umsetzung von Maßnahmen, die mehrere Branchen betreffen

Die Betreiber Kritischer Infrastrukturen stellen sich die Aufgabe, auf der Grundlage des Umsetzungsplans KRITIS die Maßnahmen fortzuführen und die Empfehlungen umzusetzen. Unter Federführung des Bundesministeriums des Innern soll der Umsetzungsplan KRITIS fortgeschrieben und den sich ständig ändernden Rahmenbedingungen im Sicherheitsumfeld angepasst werden.

2. Ausgangslage und Empfehlungen für die Zukunft

2.1 Einführung

Die Betreiber Kritischer Infrastrukturen in Deutschland sind sich ihrer Verantwortung für die Versorgung des Gemeinwesens mit lebensnotwendigen Dienstleistungen bewusst. Sie haben deshalb bereits umfängliche Maßnahmen ergriffen, um die verlässliche Bereitstellung dieser Dienstleistungen sicherzustellen. In diesem Kapitel werden zum einen die Prozesse und Maßnahmen beschrieben, die von den an der Erstellung des Umsetzungsplans KRITIS beteiligten Betreibern und Branchen in wesentlichen Teilen als IT-Basisschutz schon heute eingesetzt werden und sich bewährt haben. Diese Prozesse und Maßnahmen sollten bei jedem Betreiber Kritischer Infrastrukturen vergleichbar umgesetzt sein. Zum anderen werden Empfehlungen ausgesprochen, damit die Betreiber ihre IT-Infrastrukturen zukünftig noch besser absichern können. Anderen KRITIS-Betreibern sowie Unternehmen, die nicht zu den Kritischen Infrastrukturen gehören, werden diese zur Umsetzung empfohlen.

Das Kapitel ist in Umsetzung der strategischen Ziele des NPSI in die Bereiche Prävention, Reaktion und Nachhaltigkeit unterteilt. In diesen Unterkapiteln sind die Maßnahmen und Empfehlungen der Unternehmensebene, der Branchenebene und der branchenübergreifenden Ebene farblich voneinander abgesetzt.

Unternehmensebene
Auf dieser Ebene werden Maßnahmen und Empfehlungen beschrieben, die unternehmensintern weitgehend ohne Zusammenarbeit mit anderen Betreibern oder Dienstleistern anderer Branchen umgesetzt sind. Kooperationen unter anderem mit (meist örtlichen) Rettungsdiensten, Hilfswerken, Polizeien, Feuerwehren zählen zu dieser Ebene. Die Umsetzung der Maßnahmen und Empfehlungen ist ein kontinuierlicher Prozess, der von den Betreibern eine ständige Beobachtung der IT-Sicherheitsentwicklungen sowie schnelles und effektives Reagieren auf Veränderungen umfasst.

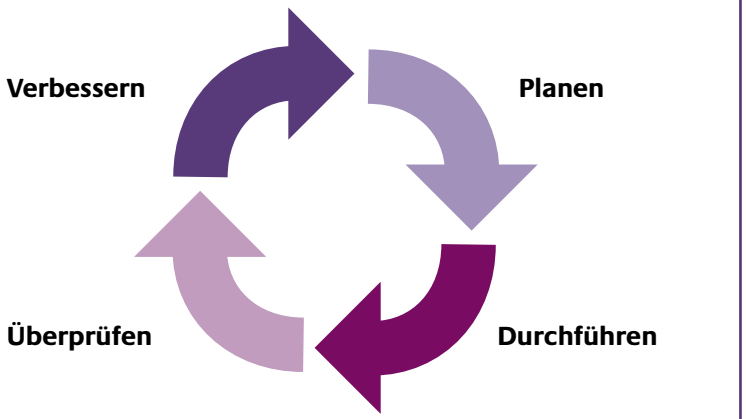
Branchenebene
Hier werden die brancheninterne Zusammenarbeit zwischen Betreibern und Verbänden dargestellt und Empfehlungen zur Verbesserung der Zusammenarbeit gegeben. Die Umsetzung der Maßnahmen soll dazu beitragen, zum Beispiel Produktionsausfälle zu verhindern oder Lieferschwierigkeiten zu minimieren. Die Kooperationen umfassen unter anderem die Festlegung von Standards und Prüfmethoden oder die Durchführung größerer Übungen. Die beschriebene Ausgangslage auf Branchenebene ist exemplarisch aus einzelnen Branchen abgeleitet und gilt nicht für alle Branchen in gleichem Maße.

Branchenübergreifende Ebene
Für die branchenübergreifende Ebene werden Maßnahmen und Empfehlungen über die unternehmens- und brancheninterne Zusammenarbeit hinaus beschrieben. Kooperationspartner dieser Ebene sind unter anderem Bundes- oder Landesbehörden und Unternehmen anderer Branchen. Aufgaben, die staatliche oder andere neutrale Stellen ohne konkrete Kooperation mit den Branchen oder Unternehmen erfüllen (Beispiele aus anderen Bereichen sind Reisewarnungen sowie Informationen über Epidemien oder andere Gesundheitsrisiken), sind hier zuzuordnen.

2.2 Prävention

Alle Betreiber Kritischer Infrastrukturen räumen präventiven Maßnahmen einen hohen Stellenwert ein, um möglichen Beeinträchtigungen der IT-Infrastruktur vorzubeugen und um die IT-Sicherheit und Verfügbarkeit der Dienstleistungen aufrechterhalten zu können. Der IT-Sicherheitsmanagementprozess als geplantes und organisiertes Vorgehen aller Beteiligten zur Durchsetzung und Aufrechterhaltung eines angemessenen IT-Sicherheitsniveaus besteht aus in sich verzahnten Einzelprozessen. Grundlage des IT-Sicherheitsmanagementprozesses und aller IT-Sicherheitsprozesse ist der Kreislauf „Planen – Durchführen – Überprüfen – Verbessern“ (siehe Abbildung 2, Seite 12).

Abbildung 2: Prozesskreislauf



Die wesentlichen Einzelprozesse werden im Folgenden beschrieben:

Im Rahmen des IT-Sicherheitsprozesses werden die kritischen Geschäftsprozesse und deren potenzielle Risiken erfasst. Die anzuwendenden Gesetze, Vorschriften und sonstigen Vereinbarungen werden herangezogen und die dort definierten Anforderungen berücksichtigt. Auf dieser Basis werden unternehmensindividuelle IT-Sicherheitskonzepte erstellt und umgesetzt. Die Mitarbeiterinnen und Mitarbeiter werden geschult und zur Einhaltung der definierten Maßnahmen verpflichtet. Wiederkehrende Notfallübungen, auch in Zusammenarbeit mit externen Stellen, runden die präventiven Maßnahmen ab. Störungen, die trotz aller Vorkehrungen auftreten, werden analysiert. Die Ergebnisse werden zur Verbesserung der Maßnahmen und Verhaltensregeln genutzt, sodass die Gefahr von Wiederholungen reduziert beziehungsweise Schäden bei zukünftigen ähnlichen Vorfällen minimiert werden.

2.2.1 Organisation der IT-Sicherheit

Für Betreiber Kritischer Infrastrukturen haben das IT-Sicherheitsmanagement und die flächendeckende Grundabsicherung eine hohe Bedeutung. Innerhalb der Betriebe sind organisatorische Strukturen etabliert, um effiziente IT-Sicherheit zu gewährleisten. Die im Rahmen des IT-Sicherheitsmanagements Verantwortlichen verfügen zur gewissenhaften Wahrnehmung ihrer Aufgaben über die notwendigen Verantwortlichkeiten, Kompetenzen und Qualifikationen. Dazu zählen der Gesamtüberblick über das Unternehmen und die wesentlichen Aufgaben sowie ein fundiertes Methodenwissen zu Konzepten und Vorgehensweisen im Bereich der IT und IT-Sicherheit. Die Bestellung eines IT-Sicherheitsbeauftragten ist ein Beitrag zur klaren Zuweisung von Verantwortlichkeiten. Zur Erzielung einer umfassenden Gesamtsicherheit innerhalb des Betriebs sind für alle Informationen, Anwendungen und IT-Komponenten die Verantwortlichkeiten definiert und zugewiesen.

2.2.2 Kritische Geschäftsprozesse

Die Betreiberziele können nur mit ordnungsgemäßem und sicherem IT-Einsatz erreicht werden. Somit hat die Identifikation von kritischen Geschäftsprozessen und der zugehörigen IT-Systeme einen hohen Stellenwert. Diese Prozesse werden besonders geschützt. Abhängigkeiten von IT oder Sprach- und Datennetzen sind erfasst. IT-Sicherheit wird bereits bei der Konzeption und Entwicklung von IT-Architekturen und IT-Systemen für kritische Geschäftsprozesse berücksichtigt. Geeignete Maßnahmen für den erhöhten Schutzbedarf kritischer Geschäftsprozesse sind in den IT-Sicherheitskonzepten enthalten. Zertifizierte IT-Systeme und IT-Lösungen bieten sich hier, sofern verfügbar, zum Einsatz an. Technische Redundanzen und organisatorische Maßnahmen stellen die Verfügbarkeit wesentlicher Komponenten sicher. Vertrauenswürdigkeit und Sicherheitskompetenz sind wesentliche Auswahlkriterien, wenn externe Dienstleistungen in Anspruch genommen werden.

Neben den unternehmensinternen Prozessen untersuchen die Betreiber Kritischer Infrastrukturen auch die Interdependenzen zu externen Prozessen hinsichtlich ihrer Kritikalität. Dabei kann es sich um externe Kommunikationsdienstleistungen oder andere fremdbezogene Dienste handeln. Sowohl der Daten- und Warenverkehr als auch die verschiedenen Transportwege werden betrachtet. Fokussiert werden mögliche Probleme, die aus Störungen der IT-Infrastruktur (sowohl in der eigenen als auch beim Kommunikationspartner) resultieren können.

Infolge der dynamischen IT-Entwicklung unterliegen die Risiken einer stetigen Veränderung. In einem kontinuierlichen Prozess wird die aktuelle Bedrohungslage auf Veränderungen untersucht und bewertet. Entsprechende Gegenmaßnahmen werden bedarfsgerecht eingeleitet.

Empfehlungen:

- Vorgaben für IT-Sicherheitsanforderungen an IT-Systemkomponenten sollten entwickelt und angewendet werden.
- Prüfkriterien für die Sicherheit von IT-Architekturen und IT-Systemen sollten angewendet, fehlende Prüfkriterien sollten entwickelt werden.
- An die Qualifikation externer Auftragnehmer sollten die gleichen Sicherheitsanforderungen wie an interne Ressourcen gestellt werden, wenn sie für IT-(Sicherheits-)Dienstleistungen eingebunden werden.
- Längerfristig sollten zertifizierte IT-Produkte unter Berücksichtigung einer Kosten-Nutzen-Analyse verstärkt zum Einsatz kommen.
- Für branchenweite kritische Prozesse sollten verstärkt zertifizierte Produkte eingesetzt werden.

2.2.3 IT-Sicherheitskonzeption

Ein angemessenes Maß an IT-Sicherheit ist nur mit aufeinander abgestimmten Maßnahmen zu erreichen. Es wird eine Gesamtkonzeption benötigt, die alle Bereiche der IT-Sicherheit einbezieht und die durchgängig umgesetzt ist. Die IT-Sicherheitsleitlinie des Betreibers definiert, welche IT-Sicherheitsziele anzustreben beziehungsweise einzuhalten sind, um die Erfüllung der Geschäftsprozesse im erforderlichen Umfang zu unterstützen. Die Anforderungen werden auch von den unternehmerischen Zielen und gegebenenfalls denen der Organisationseinheiten abgeleitet. Das Unternehmensmanagement gibt die IT-Sicherheitsleitlinie frei und setzt sie in Kraft. Die Sicherheitsleitlinie wird regelmäßig überprüft und aktualisiert.

Das IT-Sicherheitskonzept ist nach den Vorgaben der IT-Sicherheitsleitlinie ausgerichtet. Nationale und internationale Gesetze, Verordnungen, Richtlinien und Standards setzen ebenfalls einen Rahmen für die Sicherheitskonzepte. Die zu schützenden Systeme werden identifiziert. Ihr Sicherheits- und Schutzbedarf wird anhand möglicher Schadensszenarien festgelegt. Unter Berücksichtigung der identifizierten Risiken werden Maßnahmen ausgewählt und in einem IT-Sicherheitskonzept zusammengefasst. Die Entscheidung, welche konkreten Maßnahmen zu den erkannten Risiken implementiert werden müssen, wird in Abstimmung mit dem Management getroffen. Maßnahmen aus der Notfall- und Krisenmanagementplanung werden im IT-Sicherheitskonzept berücksichtigt. Das IT-Sicherheitskonzept wird nachvollziehbar umgesetzt und regelmäßig fortgeschrieben.

[3] Bundesministerium des Innern, Schutz Kritischer Infrastrukturen – Basisschutzkonzept.

Im Rahmen der Konzepterstellung wird eine Kosten-Nutzen-Analyse durchgeführt. Dazu werden den erkannten Risiken Eintrittswahrscheinlichkeiten und potenzielle Schadenshöhen (Gesundheits- und Lebensgefährdungen, materielle und immaterielle Verluste) zugeordnet. Diese werden den geschätzten Kosten wirksamer Schutzmechanismen gegenübergestellt. Das Management bestimmt für jedes Einzelrisiko, ob und in welchem Umfang eine Absicherung zu implementieren ist. Relevante Anwendungen und Abläufe werden auf der operativen Ebene zur schnellen Erkennung von Unregelmäßigkeiten überwacht.

Betreiber Kritischer Infrastrukturen sorgen auch für die physische Sicherheit ihrer IT-Anlagen. Die entsprechenden Maßnahmen sind ebenfalls im IT-Sicherheitskonzept berücksichtigt. Weiterführende Informationen und Empfehlungen zum physischen Basisschutz sind im Basisschutzkonzept[3] aufgeführt.

Die IT-Sicherheitskonzeption wird durch die Bereitstellung von branchenspezifischen Leitfäden, Richtlinien und Verfahrensbeschreibungen unterstützt.

2.2.4 Aufrechterhaltung kritischer Geschäftsprozesse

Im Rahmen des Business Continuity Managements (BCM) werden kritische Geschäftsprozesse durch Präventivmaßnahmen so abgesichert, dass diese selbst in kritischen Situationen und in Notfällen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz des Unternehmens sichergestellt bleibt sowie gravierende Auswirkungen auf das Gemeinwesen vermieden werden. Zur Schadensminimierung in Krisensituationen sowie zur Erfüllung rechtlicher und unternehmensspezifischer Anforderungen ist das Notfall- und Krisenmanagement unverzichtbar. Als Vorsorgemaßnahme wird nach der Identifikation und Bewertung der kritischen Geschäftsprozesse ein leistungsfähiges Notfall- und Krisenmanagement zur systematischen Vorbereitung auf die Bewältigung von Schadensereignissen sowie der Verhinderung des Übergreifens von Schäden auf andere Unternehmensteile beziehungsweise Unternehmen aufgebaut. Unternehmensspezifische Notfallpläne, die unter anderem auch die Grundlage für Planspiele und Notfallübungen bilden, werden erstellt.

Können für das Unternehmen besonders wichtige Prozesse in Notfällen nicht weiter aufrechterhalten werden, greifen brancheninterne Vereinbarungen, um den geregelten Geschäftsbetrieb kurzfristig wieder aufnehmen zu können. Zusätzlich sind in vielen Bereichen Absprachen auf der Grundlage bewährter Konzepte getroffen, die innerhalb der einzelnen Branchen erstellt und abgestimmt wurden, um bei Ausfall eines Betreibers die Verfügbarkeit der Dienstleistung auf Branchenebene aufrechtzuerhalten.

Empfehlungen:

- Alternativprozesse sollten für den Krisenfall einsatzbereit gehalten werden, um die Auswirkungen von Störungen kritischer Geschäftsprozesse zu reduzieren.
- Ausreichende Kapazitäten der jeweiligen Infrastrukturen sollten branchenintern für den Krisen- und Notfall vorgehalten werden (insbesondere Stromversorgung).
- Zusätzlich sollten Ausweichinfrastrukturen nutzbar sein.
- Branchenübergreifend sollten Notfall- und Krisenpläne zur Vorbereitung auf Krisen und als Grundlage für branchenübergreifende Übungen erstellt werden.
- Verantwortlichkeiten zur Bewältigung von Krisen- und Notfallsituationen sollten klar zugewiesen werden.
- Kriterien sowie Verantwortliche für die Feststellung einer Krise sollten definiert sein.
- Zuständigkeiten für die Inkraftsetzung der Notfall- und Krisenpläne sollten bestimmt sein.
- Betreiber Kritischer Infrastrukturen sollten bei Ressourcenknappheit in Krisen vorrangig versorgt werden, um ein effizientes Wiederanlaufen kritischer Geschäftsprozesse zu gewährleisten.

2.2.5 Realisierung der Sicherheitskonzepte

Die Sicherheitskonzepte der Betreiber Kritischer Infrastrukturen sind grundsätzlich nachvollziehbar und vollständig umgesetzt. Die Umsetzung wird regelmäßig überprüft. Zu den Standardanforderungen an die IT-Sicherheit im Bereich Verfügbarkeit, Integrität und Vertraulichkeit bei den Betreibern gehören zum Beispiel:

- Analyse der Infrastruktur unter Hochverfügbarkeitsaspekten, Umsetzung der entsprechenden technischen und organisatorischen Maßnahmen,
- Sicherheitseinstufung von Dokumenten und Klassifizierung von Informationen,
- Erstellung und Umsetzung von Konzepten zur kryptografischen Absicherung schützenswerter Informationen,
- Richtlinien zum Einsatz neuer Komponenten in bestehenden IT-Architekturen,
- erweiterte Regelungen und Kontrollen für den Zutritt zu IT-Systemen und den Zugriff auf Daten,
- Auswahl von nachgewiesen vertrauenswürdigen Unternehmen für IT-Sicherheitsdienstleistungen.

2.2.6 Sicherheit im gesamten Produktlebenszyklus

Betreiber Kritischer Infrastrukturen formulieren spezielle Anforderungen an die Sicherheit und Verlässlichkeit der eingesetzten Produkte. Diese umfassen nicht nur die Sicherheitsmerkmale selbst, sondern den gesamten Lebenszyklus. Sicherheit ist bereits bei der Definition der Anforderungen zur Beschaffung ein wesentlicher Aspekt. Dies gilt auch für Fehlerbehebung, Weiterentwicklung und Migration auf Nachfolgeprodukte oder Nachfolgeversionen. Die Einhaltung dieser Anforderungen ist unabhängig davon, ob es sich um Eigen- beziehungsweise Auftragsentwicklungen oder Standardprodukte handelt.

Um den erhöhten Sicherheitsanforderungen der Betreiber Kritischer Infrastrukturen zu genügen, sind Produkte und Komponenten mit entsprechenden Eigenschaften zu entwickeln und zu nutzen. Für hochkritische Komponenten werden bereits betreiberspezifische Lösungen entwickelt und eingesetzt.

Empfehlungen:

- Betreiber Kritischer Infrastrukturen sollten Sicherheitsanforderungen definieren und bei deren Überprüfung branchenweit kooperieren.
- Es sollten Produkte und Komponenten entwickelt werden, die den erhöhten Sicherheitsanforderungen der Betreiber Kritischer Infrastrukturen entsprechen.
- Die Branchenebene wie auch die branchenübergreifende Ebene sollten sich verstärkt für die Nutzung zertifizierter Software einsetzen.

2.2.7 Durchführen von Schulungen und Sensibilisierung durch zielgruppenspezifische Informationsangebote

Die Mitarbeiterinnen und Mitarbeiter werden aufgefordert, auf die Sicherheit ihres Betriebs zu achten und sicherheitsbewusst zu agieren. IT-Nutzer, IT-Verantwortliche, IT-Sicherheitsverantwortliche und Führungskräfte werden unternehmensintern mittels geeigneter Schulungskonzepte und -materialien aus- und weitergebildet, um die benötigte IT-Sicherheitskompetenz zu erlangen.

Um innerhalb der einzelnen KRITIS-Branchen einen möglichst hohen und homogenen Ausbildungsstand zu erhalten, werden branchenspezifisch Schulungsmaterialien und Konzepte entwickelt und eingesetzt. Darin sind auch die Kriterien zur Überprüfung des Schulungserfolges festgeschrieben. Neben den eigenen Mitarbeiterinnen und Mitarbeitern bilden Kunden und Partner ebenfalls eine Zielgruppe für Schulungsmaßnahmen. Weiterhin werden die Inhalte in Kooperation mit Schulen, Hochschulen und Universitäten gemeinsam erarbeitet.

Zur Verbesserung der IT-Sicherheitssensibilisierung arbeiten die Betreiber Kritischer Infrastrukturen branchenübergreifend mit der öffentlichen Verwaltung zusammen, zum Beispiel mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundeskriminalamt, der Bundesnetzagentur und den zuständigen Fachministerien. Es werden gemeinsame Übungen, wie etwa die „Länderübergreifende Krisenmanagement Exercise“ (LÜKEX), durchgeführt.

Die öffentliche Verwaltung stellt spezielle und verlässliche Informationen bereit, wie IT-Lageberichte, Reise- und Terrorwarnungen oder Epidemieinformationen. Kostenfreie und herstellerneutrale Hilfsmittel und Leitfäden werden angeboten.

Empfehlungen:

- In den Profilen von Stellenausschreibungen sollten IT-Sicherheitsqualifikationen zusätzlich definiert werden.
- Die Entwicklung branchenweiter Schulungskonzepte und Informationsangebote sollte intensiviert werden.
- Betreiber Kritischer Infrastrukturen sollten vermehrt zur Reduzierung ihrer Sicherheitsrisiken bei branchen- und bundesweiten sowie internationalen Sensibilisierungsinitiativen mitwirken.

2.2.8 IT-Sicherheitsrevision

Die Umsetzung der IT-Sicherheitskonzepte wird mit regelmäßigen internen Revisionen kontrolliert. Aufgabe einer Revision ist unter anderem die unabhängige Prüfung der Einhaltung gesetzlicher Vorgaben und darauf bezogener Umsetzungsbestimmungen. Die Aufgaben der Revision sind von der IT-(Sicherheits-)Abteilung getrennt. Die regelmäßige Durchführung von IT-Sicherheitsrevisionen und IT-Audits, die für die IT-gestützten kritischen Geschäftsprozesse von besonderer Bedeutung sind, erfolgt nachvollziehbar anhand von Prüfplänen. Die Revisionsergebnisse fließen in die stetige Verbesserung der IT-Sicherheitskonzepte und der daraus resultierenden Maßnahmen ein.

In einzelnen Branchen existieren spezifische Zulassungs- und Prüfvorschriften für IT-Systeme. Diese sichern unter anderem auch die Funktionsfähigkeit und Sicherheit unternehmensübergreifender Prozesse.

2.2.9 Notfall- und Krisenreaktionsübungen

Notfall- und Krisenreaktionsprozesse können nur schnell und wirkungsvoll greifen, wenn alle Beteiligten in die entsprechenden Handlungen eingewiesen sind und diese in Form von Übungen auf ihre Wirksamkeit geprüft wurden. Unternehmensintern werden diese wesentlichen Prozesse auf technischer und organisatorischer Ebene geübt.

Bei Übungen auf Branchenebene wird insbesondere erprobt,

- ob die verabredeten Kommunikationsbeziehungen aufgebaut und aufrechterhalten werden können und
- ob die verabredeten Maßnahmen zur gegenseitigen Unterstützung und Übernahme von Aufgaben wie geplant durchgeführt werden.

Die Auswertung der Ergebnisse erfolgt in Kooperation aller beteiligten Partner.

Empfehlungen:

- Auf Unternehmensebene sollten die Übungen mit umfassenderen Szenarien auch unter Einbeziehung externer Partner durchgeführt werden.
- Notfallübungen sollten mit wechselnden Zielsetzungen und Teilnehmern abgehalten werden.
- Regeln für die Zusammenarbeit mit unterschiedlichen Organisationen, wie zum Beispiel Polizeien, Feuerwehren, Rettungsdiensten, lokalen Katastrophenschutzbehörden und dem BSI, sowie Kunden und Zulieferern sollten ausgearbeitet beziehungsweise berücksichtigt werden.
- Auf Branchenebene und branchenübergreifender Ebene sollte die regelmäßige Durchführung von Planspielen und Notfallübungen mit allen relevanten Behörden, Organisationen sowie externen Partnern intensiviert werden, um branchenweiten und branchenübergreifenden Krisensituationen vorbereitet begegnen zu können. Diese Notfallübungen sollten von eigens aufgestellten Gremien entwickelt und ausgewertet werden. Hierdurch könnten gezielte Optimierungsprozesse angestoßen und bestehende branchen- und sektorübergreifende Abhängigkeiten sowie kritische Schwachstellen identifiziert und Vermeidungsstrategien entwickelt werden.
- Um Krisen effektiv bewältigen zu können, sollten insbesondere Themenstellungen aus der Telekommunikations- und Elektrizitätsbranche behandelt und relevante staatliche Einrichtungen in die Übungen einbezogen werden.
- Krisenszenarien sollten entwickelt werden, wie zum Beispiel der Stromausfall in einer Großstadt, um die branchenübergreifende Koordination zu verbessern, geeignete Strukturen zur Zusammenarbeit zu entwickeln und existierende Gefährdungen zu erkennen.

2.3 Reaktion

Störungen in Informationsinfrastrukturen erfordern schnelle und wirksame Reaktionen. Dazu gehören neben dem Sammeln und Analysieren von Informationen insbesondere die Alarmierung der Betroffenen sowie das Ergreifen von Maßnahmen zur Schadensminimierung und Wiederherstellung kritischer Geschäftsprozesse. Geeignete Mechanismen sind bei den Betreibern in weiten Teilen etabliert. Besonders hervorzuheben sind hierbei die IT-Notfallteams und CERT-Strukturen bei den Betreibern Kritischer Infrastrukturen. Krisen- und Notfallpläne sowie die Sicherstellung der durchgängigen Erreichbarkeit von Entscheidungsträgern und technischem Personal sind weitere wesentliche Bestandteile der Krisenreaktion. Liegen Störungen in den Informationsinfrastrukturen eines Betreibers vor, wird zuerst intern die Situation analysiert und geeignete Gegenmaßnahmen werden ergriffen. Bei möglichen externen Auswirkungen folgen im Rahmen des branchenspezifischen Krisenmanagements Schritte, um die Verfügbarkeit der Dienstleistungen und Waren aufrechtzuerhalten.

2.3.1 IT-Sicherheitslagefeststellung

Die Betreiber Kritischer Infrastrukturen haben Mechanismen zur Feststellung der IT-Sicherheitslage definiert und etabliert. Grundlage ist das unternehmensinterne Erkennen, Erfassen und Bewerten von Vorfällen nach festen Regeln unter Berücksichtigung der allgemeinen Sicherheitslage. Die Informationen werden zentral gesammelt und ausgewertet, um zu einer unternehmensinternen Lagebeurteilung zu kommen.

Bei Abweichungen vom Normalzustand wird unverzüglich eine geeignete Problembehandlung eingeleitet. Dieses Vorgehen – einschließlich der Definition von stufenspezifischen Rollen und Pflichten – ist dokumentiert und liegt den beteiligten Stellen des Betreibers vor. Die wesentlichen Rollen werden entsprechend ausgebildeten Mitarbeiterinnen und Mitarbeitern zugewiesen. Eine Vertretungsregelung ist festgelegt. Standardmäßig sind unternehmensinterne Mechanismen definiert, die Kriterien zur Eskalation sowie die Eskalationsstufen enthalten.

Neben der unternehmensinternen IT-Sicherheitslagefeststellung wird auch auf Branchenebene die übergeordnete IT-Sicherheitslage beobachtet, um frühzeitig potenzielle Bedrohungen zu erkennen. Nach Bewertung findet darüber ein Informationsaustausch mit anderen Betreibern innerhalb der Branche statt, wobei Kommunikationswege und Ansprechpartner definiert sind. So können rechtzeitig branchenweit geeignete Präventivmaßnahmen ergriffen werden.

Empfehlungen:

- Branchenübergreifend sollten unter Beteiligung der Bundesverwaltung alle notwendigen und wichtigen Informationen zur Feststellung der IT-Sicherheitslage identifiziert und in entsprechende Meldestrukturen eingebracht werden.
- Geeignete Strukturen für eine Zusammenarbeit aller Beteiligten, vor allem mit Blick auf ein unternehmensübergreifendes Lage- und Analysezentrum, sollten aufgebaut werden. Vorfälle könnten so übergreifend erfasst, bewertet und verarbeitet werden.
- Zur Lagebewertung sollte ein Stufensystem eingeführt werden, das die Schwere eines Vorfalles anhand von Abstufungen darstellt.

2.3.2 Mechanismen zur Warnung und Alarmierung

Bei sicherheitsrelevanten Vorkommnissen muss eine schnelle und angemessene Reaktion erfolgen. Dazu sind bei den Betreibern Kritischer Infrastrukturen geeignete Vorgehensweisen zur Warnung und Alarmierung festgelegt. Diese enthalten Bestimmungen über die zu warnenden beziehungsweise zu alarmierenden Stellen, abhängig vom erkannten Vorfall und von den Unterscheidungskriterien für Warnung und Alarmierung. Neben unternehmensinternen Adressaten werden externe Stellen je nach Abhängigkeit von Prozessen alarmiert.

Werden sicherheitsrelevante Vorkommnisse erkannt, die gravierenden Einfluss auf die gesamte Branche haben können, werden die potenziell Betroffenen über definierte Wege gewarnt beziehungsweise alarmiert.

Empfehlungen:

- Es sollten Mechanismen zur Beobachtung und Erfassung von Störfällen etabliert werden, um eine abgestufte Lagebewertung zu ermöglichen.
- Die Alarmierung sollte aus qualifizierten Informationen über Art und Umfang der Störung bestehen, um zielgerichtet Warnungen und Alarmierungen weiterleiten zu können.
- Die etablierten Prozesse sollten in drei Eskalationsstufen unterteilt werden (unternehmensinterne, brancheninterne sowie branchenübergreifende Alarmierung).

2.3.3 IT-Krisenreaktion

Betreiber Kritischer Infrastrukturen legen adäquate Reaktionen zur Bewältigung von IT-Krisen in Krisenreaktionsplänen fest. Diese umfassen auch die Kooperation mit internen und externen Stellen in Krisensituationen. Die Organisation des Krisenmanagements und die Verteilung der Kompetenzen sind eindeutig geregelt, sodass die erforderlichen Maßnahmen umgehend ausgelöst und umgesetzt werden können.

Zur Bewältigung branchenweiter Krisen sind in Teilbereichen geeignete Vorgehensweisen definiert. Sie regeln die Kooperation der Betreiber zur Krisenbewältigung. Darin beschrieben sind unter anderem das Vorgehen zur Koordination von Abwehrmaßnahmen und zur Aufrechterhaltung der wichtigen Dienstleistungen sowie Ansprechpartner und Kommunikationswege. Auch die Richtlinien zur Öffentlichkeitsarbeit im Krisenfall sind dort festgelegt.

Empfehlungen:

- Krisenreaktionsprozesse sollten auch branchenübergreifend etabliert werden. Dazu sollten Prozessabläufe definiert werden, die eine reibungslose Kooperation aller beteiligten Stellen sichern.
- Notfallkonzepte für branchenübergreifende IT-Krisen sollten erstellt und umgesetzt werden.
- In diesen Konzepten sollten zu kontaktierende Stellen in branchenübergreifenden Krisensituationen sowie Meldewege und Eskalationsstufen verankert werden.
- Branchenübergreifend sollte eine geregelte Koordination geeigneter Abwehrmaßnahmen durchgeführt werden.
- Im Rahmen von Übungen sollten bereits bestehende Konzepte auf ihre Tauglichkeit geprüft und fortgeschrieben werden.

2.3.4 Protokollierung und Monitoring

Betreiber Kritischer Infrastrukturen bereiten die gesammelten Informationen über Sicherheitsvorfälle und deren Behebung auf. Voraussetzung dazu ist die Protokollierung sicherheitsrelevanter Vorgänge. Besonders in kritischen Bereichen wird ein automatisierter Nachweis geführt, der festgelegte Aktionen zu Daten und Prozessen protokolliert (Monitoring). Diese Protokolle ermöglichen es, Unregelmäßigkeiten zu erkennen und Vorfälle im Nachhinein analysieren zu können. Sie dienen auch der Beweissicherung bei Störfällen. Das Monitoring ist unter besonderer Berücksichtigung der Mitbestimmungs- und Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter konzipiert.

2.4 Nachhaltigkeit

Um die nationalen Informationsinfrastrukturen langfristig schützen zu können, benötigt Deutschland neben dem politischen Willen und der Bereitschaft aller Verantwortlichen zur Stärkung der IT-Sicherheit Fachkompetenz sowie vertrauenswürdige IT-Dienstleistungen und IT-Sicherheitsprodukte. Die Betreiber leisten bereits jetzt wesentliche Beiträge zu diesem Ziel. Beispiele sind die Mitgestaltung der Aus- und Fortbildungsinhalte für Mitarbeiterinnen und Mitarbeiter und die Zusammenarbeit mit Forschung und Entwicklung zur Bereitstellung verlässlicherer IT-Systeme. Auf Branchenebene und branchenübergreifender Ebene arbeiten Betreiber Kritischer Infrastrukturen und andere Organisationen zusammen, um gemeinsame Interessen zur Verbesserung der IT-Sicherheit national und international durchzusetzen.

2.4.1 Ausbildung zur IT-Sicherheit

Durch bereits bestehende Kooperationen mit Schulen, Hochschulen und Universitäten zielen die Betreiber auf eine verstärkte Berücksichtigung der IT-Sicherheit in der Ausbildung.

In gemeinsamen Aktivitäten von Staat und Unternehmen werden Lehrinhalte für Schulen, Hochschulen und Universitäten vorgeschlagen, sodass zukünftige IT-Nutzer, IT-Verantwortliche, IT-Sicherheitsverantwortliche und Führungskräfte während ihrer Ausbildung das Themengebiet IT-Sicherheit vertieft behandeln.

Empfehlung:

- Branchenübergreifende Ausbildungsinitiativen zur IT-Sicherheit sollten ergriffen werden.

2.4.2 Zusammenarbeit in Forschung und Entwicklung

In einzelnen Themenfeldern arbeiten die Betreiber Kritischer Infrastrukturen mit Herstellern, Forschungsinstituten, Hochschulen und Universitäten zusammen. So wird die Entwicklung neuer Produkte und Lösungen unterstützt, die bedarfsgerecht die steigenden Bedürfnisse nach IT-Sicherheit erfüllen.

Die Industrie- und Wirtschaftsverbände der KRITIS-Branchen arbeiten mit Universitäten, Hochschulen und Unternehmen anderer Branchen zusammen, um die Entwicklung verlässlicherer IT-Lösungen zu fördern. Damit wird das große Potenzial an Wissen und Forschungskapazitäten an den Hochschulen und Universitäten für die IT-Sicherheit genutzt.

Empfehlungen:

- IT-Sicherheit sollte in allen Forschungs- und Entwicklungsprojekten als integraler Bestandteil verankert werden. Je nach Sicherheitsbedarf sollten Produkte oder Komponenten der nationalen Kryptoindustrie eingesetzt werden.
- IT-Sicherheit sollte bereits in der Planungsphase von Produkten berücksichtigt werden.
- Die Zusammenarbeit zwischen Betreibern Kritischer Infrastrukturen und dem Bereich „Forschung und Entwicklung“ sollte intensiviert werden, sodass neueste Erkenntnisse und innovative Produkte in den Einsatz überführt und vertrauenswürdige Sicherheitsprodukte bereitgestellt werden können.

2.4.3 Zusammenarbeit zur IT-Sicherheit

Innerhalb einiger Branchen finden sich Vertreter der Betreiber Kritischer Infrastrukturen in Arbeitskreisen zusammen, um Lösungen für gemeinsame Fragestellungen zu finden. Diese behandeln zum Beispiel konkrete Sicherheitsfragen, die mehrere Betreiber oder die ganze Branche betreffen, IT-Verfahren, Geschäftsprozesse und Standards.

Viele IT-Sicherheitsvorkehrungen werden unternehmensintern als Insellösungen realisiert. Durch unternehmensübergreifende Zusammenarbeit ist es jedoch möglich, einen Branchenstandard zu definieren. Speziell im Bereich der abgesicherten Kommunikation sind die Vorteile offensichtlich. Sogar bei Maßnahmen, die vollständig unternehmensintern zu realisieren sind, können Synergien genutzt werden. So werden etwa Sicherheitsvorgaben in Kooperation aller Beteiligten erstellt und fortgeschrieben, die Umsetzung erfolgt jedoch unternehmensspezifisch. Weiterhin haben sich zum informellen Austausch über spezifische Sicherheitsfragen Kooperationsplattformen gebildet.

Empfehlung:

- Die branchenübergreifende Zusammenarbeit zur IT-Sicherheit sollte verstärkt und auf eine breitere Basis gestellt werden.

2.4.4 Interessenwahrnehmung auf nationaler und internationaler Ebene

Betreiber Kritischer Infrastrukturen haben Kooperationen vereinbart, um auf nationaler und internationaler Ebene ihre Interessen zum Schutz Kritischer Infrastrukturen wahrzunehmen. Dazu gehört unter anderem die Mitwirkung in Normungs- und Standardisierungsgremien. Branchenverbände, Behörden und weitere Institutionen wirken mit.

Empfehlungen:

- Aktivitäten auf nationaler und internationaler Ebene sollten gebündelt und koordiniert werden, um Kritische Infrastrukturen sicher betreiben zu können.
- Betreiber Kritischer Infrastrukturen sollten ihre Zusammenarbeit zwecks nationaler und internationaler Gestaltung des politischen Willens branchenintern und branchenübergreifend intensivieren.
- Es sollte grenzüberschreitend zusammengearbeitet werden. Die rechtlichen, organisatorischen und technischen Rahmenbedingungen sollten erarbeitet und umgesetzt werden.
- Sicherheitsaspekte sollten unter Mitwirkung der Behörden direkt in den Produktstandards verankert werden.

2.5 Fazit

Auf Unternehmensebene sind die wesentlichen Maßnahmen zur Wahrung eines angemessenen IT-Sicherheitsniveaus umgesetzt. Übungen zum Notfall- und Krisenmanagement könnten in einzelnen Teilbereichen umfassender durchgeführt werden.

Die Zusammenarbeit der Betreiber Kritischer Infrastrukturen und der Verbände auf Branchenebene zur Prävention und insbesondere zur IT-Krisenreaktion ist unterschiedlich ausgeprägt. Beispielhaft sind Maßnahmen einzelner Branchen aufgeführt worden. Hier wird den anderen Branchen eine Umsetzung vergleichbarer Maßnahmen empfohlen.

Auf der branchenübergreifenden Ebene gibt es in einzelnen Bereichen bereits eine intensive Zusammenarbeit, die sich insbesondere bei der internationalen Interessenwahrung bewährt. Auf nationaler Ebene sollte im Bereich der IT-Krisenreaktion die Zusammenarbeit ebenfalls weiter verstärkt werden.

3. Kommunikation

3.1 Einführung

Der Ausbau der Kommunikation – insbesondere zur IT-Krisenprävention und schnellen Reaktion in IT-Krisenfällen – wird von den Beteiligten des Umsetzungsplans KRITIS als wesentlicher Baustein zur Verbesserung der IT-Sicherheit in Kritischen Infrastrukturen betrachtet.

>> Eine IT-Krise im Kontext des Umsetzungsplans 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.

Prävention und Krisenmanagement erfordern unterschiedliche Kommunikationsarten:

- Die **anlassbezogene Kommunikation zur Krisenfrüherkennung** wird von den Betreibern Kritischer Infrastrukturen genutzt, um besondere Vorkommnisse im Bereich der IT-Sicherheit zu melden, zu einer verbesserten Einschätzung der gesamten IT-Sicherheitslage zu gelangen und somit frühzeitig Schutzmaßnahmen ergreifen zu können.

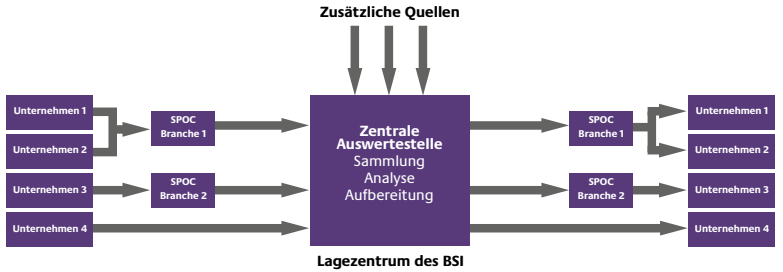
- Durch die **Kommunikation zur Alarmierung und Krisenbewältigung** wird ein Informationsaustausch zwischen den Betreibern Kritischer Infrastrukturen untereinander und mit den staatlichen Stellen bei IT-Sicherheitsvorfällen etabliert. Auswirkungen IT-sicherheitsrelevanter Ereignisse sollen minimiert, die Ausbreitung von IT-Krisen eingedämmt beziehungsweise zeitnah unternehmensübergreifende Gegenmaßnahmen koordiniert werden.

- Im Rahmen des regelmäßigen **Informationsaustausches und der Zusammenarbeit zur Krisenvermeidung** werden Arbeitsgruppen eingerichtet und Treffen durchgeführt. Durch Austausch von Erfahrungen und Informationen aus den einzelnen Branchen soll die IT-Sicherheit bei Betreibern Kritischer Infrastrukturen weiter verbessert werden. Auch sollen Verbesserungsvorschläge im Nachgang zu bereits eingetretenen IT-Sicherheitsvorfällen erarbeitet und anderen Betreibern zur Verfügung gestellt werden.

Für die beiden erstgenannten Kommunikationsarten soll ein gegenseitiger Informationsaustausch der Betreiber Kritischer Infrastrukturen über Single Points of Contact (SPOCs) mit dem BSI etabliert werden (siehe Abbildung 3). Über die SPOCs sind die Ansprechpartner in den Unternehmen der jeweiligen Branche erreichbar. Die SPOCs sollen auf Branchenebene den Informationsfluss bündeln und eine 24/7-Erreichbarkeit sicherstellen. Als Übergangslösung bis zur Einrichtung der SPOCs wird der direkte Kontakt zwischen den Betreibern Kritischer Infrastrukturen und dem BSI intensiviert.

Die gewonnenen Informationen werden vom BSI-Lagezentrum ergänzt und aufbereitet (zum Beispiel zu einem nationalen IT-Sicherheitslagebild). Diese Analysen werden den Betreibern zur Verfügung gestellt. Das BSI strebt an, die Bewertung der IT-Sicherheitslage durch die Gewinnung von zusätzlichen Informationen auf eine breitere Basis zu stellen.

Abbildung 3: Ablauf der Kommunikation



3.2 Informationsaustausch

Durch die gezielte Weitergabe von aktuellen Nachrichten über Bedrohungen der IT, IT-sicherheitsrelevante Vorfälle und notwendige Schutzmaßnahmen kann die Sicherheit der Betreiber Kritischer Infrastrukturen weiter gesteigert werden. Die Kommunikation zwischen Staat und Wirtschaft ist insbesondere bei der Krisenbewältigung von großer Bedeutung. Um diese Kooperation zu ermöglichen, müssen Maßnahmen zur Gewährleistung eines schnellen und sicheren Kommunikationsflusses getroffen werden.

Die Betreiber Kritischer Infrastrukturen sind bei Krisen in der unternehmensinternen Kommunikation bereits gut aufgestellt. Erste Kommunikationsstrukturen, die in einem IT-Krisenfall über die Grenzen des eigenen Unternehmens hinausführen, sind etabliert. In Teilbereichen bestehen bereits brancheninterne Eskalations- und Meldewege, welche auch die zuständigen Behörden und Polizeien einbeziehen. Eine branchenübergreifende Kommunikation zur IT-Krisenbewältigung ist zurzeit eher die Ausnahme. Bei der Ausweitung beziehungsweise Intensivierung der Kommunikation zwischen den Betreibern Kritischer Infrastrukturen sollten bereits vorhandene Kommunikationswege einbezogen werden.

Der Informationsaustausch erfolgt auf freiwilliger Basis. Dazu sind eindeutige Verhaltensregeln bezüglich Umgang, Weitergabe und Schutz der Informationen sowie insbesondere der Informationsquellen festzulegen.

3.2.1 Anlassbezogene Kommunikation zur IT-Krisenfrüherkennung

Erkenntnisse mit potenziellen Auswirkungen auf die IT-Sicherheitslage oder Anzeichen einer IT-Krise werden an das Lagezentrum des BSI übermittelt. Hierzu zählen unter anderem schwerwiegende IT-Angriffe auf Unternehmen oder bisher nicht kommunizierte Schwachstellen in kritischen IT-Anwendungen, soweit sie nicht im Rahmen der etablierten CERT-Strukturen kommuniziert werden.

Die anlassbezogene Kommunikation zur IT-Krisenfrüherkennung unterstützt und ergänzt die Erstellung eines nationalen IT-Sicherheitslagebildes durch das BSI. Durch dessen Verteilung an die SPOCs beziehungsweise Betreiber wird der sichere Betrieb der IT in Kritischen Infrastrukturen weiter verbessert. Die Betreiber Kritischer Infrastrukturen können sich früher auf mögliche IT-Krisen vorbereiten.

Bisher werden für die anlassbezogene Kommunikation zur Krisenfrüherkennung noch keine erhöhten Anforderungen an die Vertraulichkeit und Verfügbarkeit der Kommunikationsmittel (zum Beispiel Telefon, Fax, E-Mail) gestellt. Mittelfristig sollten geeignete Maßnahmen ergriffen werden, um auch sensible Daten übertragen zu können. Daher kommt dem Auf- beziehungsweise Ausbau geeigneter Kommunikationsstrukturen und den hierzu einsetzbaren Techniken und Mechanismen eine besondere Bedeutung zu. Diese sollen gemeinsam festgelegt und ausgebaut werden. Langfristig wird eine Beteiligung der Betreiber am IT-Frühwarnsystem des BSI angestrebt.

3.2.2 Kommunikation zur Alarmierung und Krisenbewältigung

In einer IT-Krise ist eine schnelle und abgestimmte Kommunikation wichtig, um eine rechtzeitige Reaktion zu ermöglichen und Schäden einzugrenzen. Informationen über Ausdehnung, Dauer, Grund beziehungsweise Auslöser der Störung sowie Angaben zu potenziellen Auswirkungen auf andere Unternehmen sollten kommuniziert werden. Solche Informationen erlauben es den vorerst nicht betroffenen Unternehmen, sich entsprechend vorzubereiten.

Die Mechanismen der anlassbezogenen Kommunikation zur IT-Krisenfrüherkennung eignen sich nur bedingt für die Kommunikation zur Alarmierung und Krisenbewältigung. Im Rahmen dieser Kommunikation müssen insbesondere zeitkritische Informationen verarbeitet werden. Die Mechanismen und Kommunikationsmittel müssen insbesondere im Hinblick auf die Verfügbarkeit der Kommunikationsmöglichkeiten in besonderen Krisenlagen erweitert werden. Die bei der Einrichtung der SPOCs festgelegten Verfahren sollen genutzt beziehungsweise ausgebaut werden. Die Ansprechpartner der Unternehmen sollten in geeignete IT-Krisenreaktionsprozesse eingewiesen sein und über entsprechende Kompetenzen verfügen.

3.2.3 Informationsaustausch und Zusammenarbeit zur Krisenvermeidung

Damit IT-Krisen möglichst vermieden werden und eine bessere Vorbereitung auf künftige Ereignisse gewährleistet werden kann, sind ein kontinuierlicher Informationsaustausch und eine Zusammenarbeit im Rahmen von Workshops und Arbeitsgruppen zwischen den Betreibern Kritischer Infrastrukturen und staatlichen Stellen notwendig. Aktuelle und akute IT-Sicherheitsfragen können hier diskutiert werden. Im Nachgang zu IT-Krisen werden Vorfälle analysiert, Erfahrungen ausgetauscht und Verbesserungsmöglichkeiten erarbeitet. Die erzielten Lerneffekte können einen wichtigen Beitrag zur nachhaltigen Sicherung der Informationsinfrastrukturen der Betreiber Kritischer Infrastrukturen leisten.

3.3 Bilanz und Perspektiven der Zusammenarbeit

Die Analyse der existierenden Kommunikationsformen zeigt, dass sowohl bei der anlassbezogenen Kommunikation zur Krisenfrüherkennung als auch bei der Kommunikation zur Alarmierung und Krisenbewältigung unternehmens- und teilweise auch branchenweit Strukturen für den Informationsaustausch zwischen den Betreibern Kritischer Infrastrukturen bereits vorhanden sind. Jedoch existieren für den Informationsaustausch und die Zusammenarbeit zur Krisenvermeidung auf branchenübergreifender Ebene noch keine Kommunikationsstrukturen.

Die Betreiber Kritischer Infrastrukturen befürworten eine Intensivierung der Kommunikation, insbesondere auf branchenübergreifender Ebene, um der wachsenden gegenseitigen Abhängigkeit Rechnung zu tragen. Mittelfristig ist der Aus- beziehungsweise Aufbau von SPOCs als zentrale Kommunikationsknoten in den einzelnen Branchen geplant.

Weitere gemeinsame Arbeiten aller Beteiligten werden als notwendig und wichtig erachtet. So sollen in einem ersten Schritt unter anderem die Prozesse und Technologien zur Kommunikation weiter spezifiziert werden. Durch einen Austausch zu aktuellen IT-Sicherheitsthemen und zur Aufarbeitung von IT-Krisen soll eine weitere Verbesserung der IT-Sicherheit in Kritischen Infrastrukturen erreicht werden. Die dabei etablierten Prozesse sollen regelmäßig geübt und schrittweise weiter ausgebaut werden.

4. Roadmap zum weiteren Vorgehen

Die Empfehlungen zur Aufrechterhaltung und weiteren Verbesserung der IT-Sicherheit und zur Etablierung von Kommunikationsstrukturen, die in den vorangegangenen Kapiteln beschrieben sind, haben die an der Erstellung des Umsetzungsplans KRITIS Beteiligten aufgegriffen und eine Roadmap zum weiteren Vorgehen beschlossen.

Mit dieser Roadmap werden vier Hauptthemen aufgegriffen:

1. Notfall- und Krisenübungen
2. Krisenreaktion und -bewältigung
3. Aufrechterhaltung kritischer Infrastrukturdienstleistungen
4. Nationale und internationale Zusammenarbeit

Die Gründung entsprechender Arbeitsgruppen ist im April 2007 unter Federführung des Bundesministeriums des Innern erfolgt. Die kooperative Zusammenarbeit zwischen Staat und Wirtschaft wird damit fortgeführt und die Empfehlungen werden anhand eines konkreten Zeitrahmens umgesetzt.

Für jede Arbeitsgruppe hat sich ein an der Erstellung des Umsetzungsplans KRITIS Beteiligter bereit erklärt, die Leitung und Gestaltung zu übernehmen. Die Arbeitsgruppen sollen auch durch bisher nicht an der Erstellung des Umsetzungsplans KRITIS beteiligte Unternehmen, Verbände und Behörden erweitert werden.

In der zeitlichen Abfolge werden zunächst die Themenfelder „Notfall- und Krisenübungen“ sowie „Krisenreaktion und -bewältigung“ vertiefend bearbeitet.

Hier werden erste Ergebnisse und Umsetzungen bis 2008 erarbeitet werden. Die dort gewonnenen Erkenntnisse werden als Grundlage für die folgende Arbeitsgruppe des Themenbereichs „Aufrechterhaltung kritischer Infrastrukturdienstleistungen“ genutzt und in die „Nationale und internationale Zusammenarbeit“ eingebracht.

Die Arbeitsgruppen werden durch das BSI unterstützend begleitet. Neben fachlicher Mitwirkung wird dort die Funktion der Geschäftsstelle eingerichtet.

Durch diesen in Deutschland erstmalig angewendeten branchenübergreifenden Arbeitsgruppenansatz wird ein wesentlicher Beitrag zur nachhaltigen Gewährleistung der IT-Sicherheit in Kritischen Infrastrukturen erbracht.

4.1 Notfall- und Krisenübungen

Notfall- und Krisenreaktionsprozesse können nur schnell und wirkungsvoll ablaufen, wenn alle Beteiligten in die entsprechenden Handlungen eingewiesen sind und die Prozesse in Form von Übungen auf ihre Wirksamkeit überprüft wurden. Unternehmensintern werden diese wesentlichen Prozesse auf technischer und organisatorischer Ebene bereits geübt, auf Branchenebene und branchenübergreifender Ebene sind jedoch weitere Schritte erforderlich.

Um die Empfehlungen dieses Themenbereichs umzusetzen, wurde im April 2007 die Arbeitsgruppe „Notfall- und Krisenübungen“ gegründet.

Der Schwerpunkt der Tätigkeiten dieser Arbeitsgruppe liegt in der Ausarbeitung und Umsetzung sämtlicher für die Planung, Durchführung und Auswertung von Notfall- und Krisenübungen erforderlichen Rahmenbedingungen. Es werden branchenübergreifende IT-Krisenszenarien entwickelt, anhand derer regelmäßige Übungen durchgeführt werden. Bereits bestehende Übungsreihen werden dabei berücksichtigt, mögliche Synergieeffekte werden identifiziert und genutzt. So können die erarbeiteten Szenarien beispielsweise als Vorlage in die Planung von LÜKEX-Übungen (Länderübergreifende Krisenmanagement Exercise) eingebracht werden. Dabei kann dann auch die Landes- und Kommunalebene einbezogen werden.

Die wechselnden Teilnehmer der Notfall- und Krisenübungen setzen sich aus den verschiedenen Branchen Kritischer Infrastrukturen sowie den relevanten staatlichen und privatwirtschaftlichen Organisationen zusammen.

Gemeinsame Ziele aller Beteiligten sind die Identifikation branchen- beziehungsweise sektorübergreifender Abhängigkeiten und kritischer Schwachstellen, die Optimierung von Krisenreaktionsprozessen sowie eine Verbesserung der branchenübergreifenden Koordination durch den Aufbau geeigneter Strukturen.

Hierdurch wird unter anderem die Grundlage für die weitere Arbeit im Rahmen der Arbeitsgruppe „Krisenreaktion und -bewältigung“ geschaffen.

Die Arbeitsgruppe wird sich, auch unter der Einbeziehung weiterer Teilnehmer (neben dem BSI zum Beispiel auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe mit der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz) bis Mitte 2008 mit den Vorbereitungen der turnusmäßigen Übungen und der damit verbundenen Schaffung geeigneter Rahmenbedingungen befassen. Ab Ende 2008 werden die entwickelten Notfall- und Krisenübungen mit wechselnden Zielsetzungen und Teilnehmern durchgeführt. Diese Arbeitsgruppe setzt sich zunächst aus Vertretern der Arcor AG & Co. KG, der Bayerischen Hypo- und Vereinsbank AG, der Commerzbank AG, der DB Sicherheit GmbH, der Deutschen Bank AG, der Deutschen Bundesbank, der Deutschen Telekom AG, der Deutschen Postbank AG, der Dresdner Bank AG, des Deutschen Sparkassen- und Giroverbandes e. V., der E-Plus Mobilfunk GmbH & Co KG, der O_2 (Germany) GmbH & Co. OHG, des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V., des Mineralölwirtschaftsverbandes e. V., der RWE Energy AG, der T-Mobile Deutschland GmbH sowie des Bundesministeriums für Wirtschaft und Technologie und der Bundesanstalt für Finanzdienstleistungsaufsicht zusammen.

4.2 Krisenreaktion und -bewältigung

Bei sicherheitsrelevanten Vorkommnissen muss eine schnelle und angemessene Reaktion erfolgen. In Krisenreaktionsplänen haben die Betreiber Kritischer Infrastrukturen für ihren Bereich adäquate Vorgehensweisen festgelegt. Branchenweite oder branchenübergreifende Absprachen zur Krisenreaktion sind zu verbessern.

Die Arbeitsgruppe „Krisenreaktion und -bewältigung“ hat ihre Tätigkeit im April 2007 aufgenommen und widmet sich der branchenübergreifenden Etablierung geeigneter Krisenreaktionsprozesse, von der IT-Lageanalyse über Warnung und Alarmierung bis hin zur koordinierten Krisenbewältigung.

Dazu werden Aspekte der Erfassung und Bewertung der IT-Sicherheitslage sowie der daraus abzuleitenden Strukturen für die Zusammenarbeit mit einem nationalen IT-Lage- und -Analysezentrum betrachtet.

Es werden Prozesse und technische Realisierungen zur Warnung und Alarmierung bei schwerwiegenden IT-Vorfällen definiert und gemeinschaftlich zwischen BSI

und den KRITIS-Unternehmen umgesetzt. Dabei sind die Etablierung von Single Points of Contact auf Branchenebene sowie die zugehörige Definition von Meldestrukturen ein wesentlicher Meilenstein.

Zur gemeinschaftlichen Krisenbewältigung werden die notwendigen Prozesse identifiziert und in branchenübergreifend abgestimmte Krisenreaktionskonzepte eingebracht. Insbesondere die geregelte und vorbereitete Kommunikation zwischen allen Beteiligten ist für eine koordinierte Krisenbewältigung von großer Bedeutung.

Die Arbeitsgruppe wird Konzepte zur branchenübergreifenden Krisenreaktion und -bewältigung bis Mitte 2008 erstellen. In dieser Arbeitsgruppe sind zunächst die Allianz SE, die Bundesanstalt für Finanzdienstleistungsaufsicht, die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, der Bundesverband deutscher Banken e. V., die Commerzbank AG, die Deutsche Bahn AG, die Deutsche Bank AG, die Deutsche Bundesbank, die Deutsche Flugsicherung GmbH, die DZ BANK AG Deutsche Zentral-Genossenschaftsbank Frankfurt am Main, der Deutsche Sparkassen- und Giroverband e. V., die Europäische Zentralbank, die E-Plus Mobilfunk GmbH & Co KG, der Gesamtverband der Deutschen Versicherungswirtschaft e. V., die O_2 (Germany) GmbH & Co. OHG, die RWE Energy AG, die T-Mobile Deutschland GmbH und die Vodafone D2 GmbH vertreten.

4.3 Aufrechterhaltung kritischer Infrastrukturdienstleistungen

Für das Gemeinwohl kritische Infrastrukturdienstleistungen müssen durch Präventivmaßnahmen so abgesichert werden, dass diese selbst in kritischen Situationen und in Notfällen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz des Unternehmens sichergestellt bleibt. Gravierende Auswirkungen auf das Gemeinwesen sind zu vermeiden.

Dazu werden im Rahmen einer Arbeitsgruppe kritische Prozesse identifiziert und bei Bedarf weiterführende Schutzkonzepte und Maßnahmen erarbeitet. Diese Arbeitsgruppe wird sich, nachdem erste Ergebnisse der Arbeitsgruppe „Krisenreaktion und -bewältigung“ vorliegen, im Jahr 2008 konstituieren und ihre Tätigkeit aufnehmen.

Im Rahmen der Erstellung der Schutzkonzepte werden auch Überlegungen zur vorrangigen Versorgung der Betreiber Kritischer Infrastrukturen bei krisenbedingter Ressourcenknappheit angestellt, um die Aufrechterhaltung beziehungsweise den schnellen Wiederanlauf kritischer Prozesse zu gewährleisten.

4.4 Nationale und internationale Zusammenarbeit

Der Schutz Kritischer Infrastrukturen und das Themengebiet IT-Sicherheit können nur in enger internationaler Zusammenarbeit nachhaltig vorangetrieben werden. Dazu ist bereits eine Vielzahl von Gremien und staatenübergreifender Zusammenarbeiten etabliert, in denen Normen und Standards sowie übergreifende Schutzstrategien erstellt werden.

Durch die Tätigkeit der im April 2007 gegründeten Arbeitsgruppe soll eine verstärkte Koordination und Abstimmung zwischen den am Umsetzungsplan KRITIS beteiligten Parteien erreicht werden. Dazu werden zunächst Informationen über die internationalen KRITIS-Aktivitäten der einzelnen Beteiligten ausgetauscht. Bewährte Methoden und Vorgehensweisen werden diskutiert und gemeinsame strategische Ziele abgestimmt. Es sollen Kooperationen vereinbart werden, um auf nationaler und internationaler Ebene die Interessen zum Schutz Kritischer Infrastrukturen besser wahrnehmen zu können.

Ziel der Arbeitsgruppe ist es, einen Beitrag zur Etablierung eines vergleichbaren Mindestniveaus der IT-Sicherheit in Kritischen Infrastrukturen auf internationaler Ebene, beginnend im europäischen Raum, zu schaffen.

Die Arbeitsgruppe wird zunächst die Möglichkeiten für eine gemeinsame Diskussionsplattform zum Informationsaustausch prüfen und entsprechende Strukturen aufbauen. Anlassbezogen werden zur Abstimmung von Spezialthemen Arbeitsgruppensitzungen einberufen beziehungsweise bei langfristigen Vorhaben Unterarbeitsgruppen gegründet.

5. Zusammenfassung und Ausblick

Kritische Infrastrukturen sind die Lebensadern unserer Gesellschaft, ihr Schutz ist eine gesamtgesellschaftliche Aufgabe. Ein Großteil dieser Infrastrukturen wird von der privaten Wirtschaft betrieben. Keine dieser Kritischen Infrastrukturen kann ohne angemessen geschützte Informationsinfrastrukturen ihre Dienstleistungen erbringen. Dies ist den Betreibern Kritischer Infrastrukturen bewusst. Sie haben deshalb in den jeweiligen Unternehmen bereits ein hohes Maß an IT-Sicherheit etabliert. Ein angemessener Schutz der Informationsinfrastrukturen ist aber nicht allein durch Maßnahmen in den einzelnen Unternehmen und Organisationen zu erreichen. Begleitende branchenweite und branchenübergreifende Maßnahmen auf nationaler und internationaler Ebene sind erforderlich.

Deshalb haben sich Betreiber Kritischer Infrastrukturen mit dem Bundesministerium des Innern zusammengefunden, um auf der Grundlage der im NPSI definierten strategischen Ziele Prävention, Reaktion und Nachhaltigkeit notwendige Maßnahmen zum Schutz der Informationsinfrastrukturen zu ermitteln und im vorliegenden Umsetzungsplan KRITIS zusammenzufassen. Diese Zusammenarbeit ist Ausdruck der gemeinsamen Verantwortung von Staat und Wirtschaft. Sie soll das Know-how der Betreiber bündeln und die IT-Sicherheit der Kritischen Infrastrukturen in Deutschland auch in Zukunft nachhaltig stärken.

Der Umsetzungsplan KRITIS ist Leitbild für die Betreiber Kritischer Infrastrukturen zur IT-Sicherheit. Er ist ein Beitrag zur politischen Willensbildung sowie zur nationalen und internationalen Zusammenarbeit. Er wird anderen Unternehmen als Richtschnur empfohlen, um auch dort ein angemessenes IT-Sicherheitsniveau zu realisieren.

Der in diesem Umsetzungsplan beschriebene Sachstand spiegelt die heute gelebte Praxis von Betreibern Kritischer Infrastrukturen im Bereich der IT-Sicherheit wider. Diese reicht von einer durchgängigen IT-Sicherheitsorganisation in den einzelnen Unternehmen über Maßnahmen zum besonderen Schutz der kritischen Geschäftsprozesse bis zur Durchführung von Sensibilisierungsmaßnahmen für die einzelnen Mitarbeiterinnen und Mitarbeiter.

Die Grundlagen für auch zukünftig verlässliche Infrastrukturdienstleistungen sollen weiter gefestigt werden. Die mit dem Umsetzungsplan beschlossene Roadmap soll gemeinsam von den Betreibern Kritischer Infrastrukturen und staatlichen Stellen umgesetzt und fortgeschrieben werden, um auch in Zukunft den steigenden Anforderungen gerecht zu werden.

Die in einzelnen Branchen bereits bestehende vertrauensvolle und konstruktive Zusammenarbeit bei der Abstimmung in Krisensituationen soll weiter ausgebaut werden.

Die Partnerschaft zwischen Betreibern Kritischer Infrastrukturen und der Bundesverwaltung hat sich bewährt und wird mit dem Umsetzungsplan KRITIS auf eine breitere Basis gestellt.

In gemeinsamen Arbeitsgruppen werden dazu die Themenfelder „Notfall- und Krisenübungen“, „Krisenreaktion und -bewältigung“, „Aufrechterhaltung kritischer Infrastrukturdienstleistungen“ und „Nationale und internationale Zusammenarbeit“ behandelt.

Der Umsetzungsplan KRITIS wird aufgrund der stetigen Weiterentwicklung der IT-Landschaft fortgeschrieben. Erkenntnisse, die sich aus den Aktivitäten der Arbeitsgruppen sowie der Umsetzung der Maßnahmen und Empfehlungen ergeben, fließen in die Aktualisierung des Umsetzungsplans KRITIS ein.

Die Überprüfung der Maßnahmen und Empfehlungen auf ihre Aktualität und die sich daraus ergebenden Anpassungen werden wieder in enger Kooperation von Behörden und Betreibern Kritischer Infrastrukturen erarbeitet. Dabei ist der Kreis der Beteiligten nicht auf die bisherigen Verfasser beschränkt, vielmehr ist eine Mitwirkung weiterer Betreiber erwünscht.

Kommentierungen und Anregungen zum vorliegenden Umsetzungsplan KRITIS sind jederzeit erwünscht. Nutzen Sie bitte dazu folgende Adresse:

Bundesministerium des Innern, Referat IT 3
Alt-Moabit 101 D
10559 Berlin
Telefon: (030) 1 86 81-0
E-Mail: it3@bmi.bund.de

Abkürzungen

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management
BKA	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
EPSKI	Europäisches Programm für den Schutz Kritischer Infrastrukturen
IT	Informationstechnik
KRITIS	Kritische Infrastrukturen
LÜKEX	Länderübergreifende Krisenmanagement Exercise
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
SPOC	Single Point of Contact
UP KRITIS	Umsetzungsplan KRITIS

Glossar

Bundesverwaltung	Bundesressorts und deren Geschäftsbereichsbehörden wie zum Beispiel BSI, BKA, BBK, BNetzA (vgl. Artikel 86 Grundgesetz).
Informationsinfrastruktur	Die Gesamtheit der IT-Anteile einer Infrastruktur wird als deren Informationsinfrastruktur bezeichnet.
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 geschützt sind.
Betreiber Kritischer Infrastrukturen	Betreiber Kritischer Infrastrukturen sind privatwirtschaftliche Unternehmen oder Behörden, die Dienstleistungen in den Kritischen Infrastrukturen erbringen.

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 einträten.

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 (Telekommunikation, Informationstechnologie)
- 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)

IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie wird hier als Sammelbegriff für die ebenfalls bei Betreibern Kritischer Infrastrukturen verwendeten Bezeichnungen Information Security Policy, IT-Sicherheitspolitik, IT-Sicherheitsstrategie, IT-Sicherheitsgrundsätze und IT-Sicherheitsrichtlinien verstanden.

Literaturverzeichnis

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

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

Notizen

Notizen

Impressum

Herausgeber und Redaktion:
Bundesministerium des Innern
Referat Öffentlichkeitsarbeit
Alt-Moabit 101 D, 10559 Berlin
www.bmi.bund.de

Gesamtgestaltung und Redaktion:
MEDIA CONSULTA Deutschland GmbH
Anita Drbohlav (Kreation), Dörte Hansen und
Petra Grampe (Redaktion), Patrick Pabst (Produktion)

Bildnachweis:
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Druck:
***

Die Broschüre kann kostenlos bestellt werden beim:
Publikationsversand der Bundesregierung
Postfach 481009, 18132 Rostock
Tel.: 0 18 05-77 80 90
Fax: 0 18 05-77 80 94
E-Mail: publikationen@bundesregierung.de
Internet: www.bmi.bund.de
Artikelnummer: BMI07310

Ihre zum Versand der Publikationen angegebenen personenbezogenen Daten werden nach erfolgter Lieferung gelöscht.