



Bundesministerium  
des Innern

**Nationaler Plan**

zum Schutz der  
Informationsinfrastrukturen  
Umsetzungsplan KRITIS



# IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen

Umsetzungsplan KRITIS  
Arbeitsgruppe 1  
„Notfall- und Krisenübungen“

[www.bmi.bund.de](http://www.bmi.bund.de)



# Vorwort

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

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

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

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

der Veröffentlichung des Plans im September 2007 fingen die Arbeiten der praktischen Auskleidung des theoretischen Umsetzungsplans an, deren Ergebnis bezüglich IT-Notfall- und Krisenübungen mit dem vorliegenden Dokument vorgestellt wird.

# Inhalt

<b>1</b>	<b>Einleitung und Motivation</b>	<b>5</b>
<b>2</b>	<b>Anwenderkreis</b>	<b>9</b>
<b>3</b>	<b>Abgrenzungen</b>	<b>10</b>
<b>4</b>	<b>Übungsarten</b>	<b>11</b>
<b>5</b>	<b>Übungsszenarien</b>	<b>15</b>
<b>6</b>	<b>Übungsplan</b>	<b>18</b>
	6.1 Aufbau- und Erhaltungsphase	18
	6.2 Strategischer KRITIS-Übungsplan	18
<b>7</b>	<b>Ausblick und nächste Schritte</b>	<b>23</b>
	<b>Anhang</b>	<b>24</b>
	<b>Abkürzungen</b>	<b>25</b>
	<b>Glossar</b>	<b>26</b>
	<b>Literaturverzeichnis</b>	<b>33</b>
	<b>Beteiligte UP-KRITIS-Partner</b>	<b>34</b>

# Abbildungen

<b>Abbildung 1:</b>	Übungsplan Aufbauphase	19
<b>Abbildung 2:</b>	Übungsplan Erhaltungsphase	20

# Tabellen

<b>Tabelle 1:</b>	Übungs- und Planungsaufwand für die Übungsarten	13
<b>Tabelle 2:</b>	Übungs- und Planungsdauer für die Übungsarten	14
<b>Tabelle 3:</b>	Häufigkeit der Übungsarten in der Aufbauphase	19
<b>Tabelle 4:</b>	Häufigkeit der Übungsarten in der Erhaltungsphase	20

# 1 Einleitung und Motivation

Kritische Infrastrukturen (KRITIS) sind im Rahmen des Nationalen Plans zum Schutz der Informationsinfrastrukturen (NPSI) Organisationen und Einrichtungen mit herausragender Bedeutung für das deutsche Gemeinwesen. Bereits bei Teilausfällen oder gravierenden Funktionsbeeinträchtigungen dieser Strukturen muss in Deutschland mit nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen einschneidenden Auswirkungen gerechnet werden. Dabei ist auch zu berücksichtigen, dass unterschiedliche Sektoren, die den Kritischen Infrastrukturen zugerechnet werden, zum Teil stark aufeinander angewiesen sind. Betreiber der Kritischen Infrastrukturen sind staatliche Organe, Wirtschaftsunternehmen und andere Institutionen. Diese sind sich einig, dass der Schutz der Kritischen Infrastrukturen eine wichtige nationale Aufgabe ist, die in gemeinsamer Arbeit angegangen werden muss. Ein besonderer Schwerpunkt liegt dabei auf der Absicherung der Informationsinfrastrukturen, die zu deren Betrieb unabdingbar sind.

In diesem Rahmen wurde unter der Federführung des Bundesministeriums des Innern der Umsetzungsplan KRITIS (UP KRITIS) erarbeitet, der Teil des Nationalen Plans zum Schutz der Informationsinfrastrukturen ist. Der UP KRITIS enthält ein Leitbild. In diesem heben die an der Erarbeitung des Plans beteiligten Partner die Notwendigkeit einer langfristigen Zusammenarbeit hervor und stellen fest, dass konkrete Maßnahmen zur Gewährleistung eines angemessenen hohen Schutzes der Kritischen Infrastrukturen umgesetzt werden sollen.

Eine wesentliche Maßnahme ist die Durchführung von IT-Notfall- und Krisenübungen, bei denen der Umgang mit akuten Bedrohungen und kritischen Beeinträchtigungen, welche die Informationsinfrastrukturen betreffen, geprobt wird. Diese Übungen ermöglichen es, gegenseitige Abhängigkeiten der UP-KRITIS-Partner bewusst zu machen, geeignete gemeinsame Konzepte und Maßnahmen zur IT-Notfall- und Krisenbewältigung zu entwickeln und diese anschließend regelmäßig zu überprüfen. Der Fokus der Übungen liegt dabei naturgemäß nicht auf der individuellen IT-Notfall- und Krisenbewältigung, sondern in der branchenübergreifenden Zusammenarbeit und der Zusammenarbeit mit den staatlichen Stellen. Unter Berücksichtigung der Zuständigkeiten von Bund und Ländern wird die Zusammenarbeit mit allen potenziell Beteiligten bis hin zur kommunalen Ebene als erforderlich erachtet. Die dazu notwendigen

Strukturen und Abläufe sind im Rahmen des UP KRITIS im Konzept zur „Früherkennung und Bewältigung von IT-Krisen“ beschrieben.

Das vorliegende Konzept enthält:

- Beschreibungen infrage kommender Übungsarten
- Empfehlungen zur regelmäßigen Abhaltung von Übungen

Die Teilnahme an KRITIS-Übungen ist freiwillig. Die UP-KRITIS-Partner entscheiden bei jeder geplanten Übung selbst, ob und in welchem Rahmen sie sich beteiligen. Ziel ist es, mit minimalem Aufwand maximalen Nutzen für die Teilnehmer zu erreichen.

Weiterführende Anlagen zum Konzept, die konkrete Hilfen zur Planung und Durchführung von KRITIS-Übungen sowie ausführliche Erläuterungen der Übungsarten enthalten, sind als ein separates Dokument mit dem Titel „Anlagen zum Konzept für IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen“ verfügbar.

Das vorliegende Dokument beschreibt IT-Notfall- und Krisenübungen, bei denen die Zusammenarbeit bei und der Umgang mit akuten Bedrohungen und kritischen Beeinträchtigungen, welche die Informationsinfrastrukturen betreffen können, geprobt wird. Es dient folgenden Zielen:

- Festlegung und Beschreibung von möglichen Übungsarten
- Empfehlung von Zyklen, in denen Übungen durchgeführt werden sollen
- Beschreibung der Planung, Vorbereitung, Durchführung, Auswertung und Nachbereitung von Übungen inklusive konkreter Hilfsmittel
- Optimierung des Übungsaufwands durch die Berücksichtigung von Integrationsmöglichkeiten in andere übergreifende und ergänzende Krisenübungen wie zum Beispiel LÜKEX
- Förderung der Zusammenarbeit der Arbeitsgruppenteilnehmer bei der konkreten Planung der Übungen
- Gewinnung weiterer KRITIS-Unternehmen<sup>1</sup>, Behörden und Institutionen für die Mitarbeit am UP KRITIS

<sup>1</sup> Die Einbeziehung und Mitarbeit von Wirtschaftsunternehmen, die nicht den KRITIS-Sektoren zugerechnet werden, ist nicht ausgeschlossen.

## Ziele der Übungen

Mit dem Durchspielen von Reaktionen auf IT-Notfälle und -Krisen sowie der Funktionsüberprüfung der dazu vorgesehenen Einrichtungen, ohne dass ein realer Ernstfall vorliegt, werden das Krisenmanagement und die Krisenreaktion geübt und auf der Grundlage der gewonnenen Erfahrungen verbessert.

Die UP-KRITIS-Partner verfügen bereits über umfangreiche Konzepte und Maßnahmen zur individuellen IT-Krisen- und Notfallbewältigung, die auch regelmäßig geübt werden. Dies gilt aber nicht in gleichem Maße für die sektoren- und branchenübergreifende Zusammenarbeit bei Notfällen und Krisen mit IT-Bezug, die Kritische Infrastrukturen gefährden, sowie für die Zusammenarbeit mit den zuständigen staatlichen Stellen. Die bisherige Arbeit im Rahmen des UP KRITIS macht aber deutlich, dass eine solche Zusammenarbeit aufgrund der vielfältigen Schnittstellen und Abhängigkeiten zwischen den UP-KRITIS-Partnern sinnvoll ist und für alle Beteiligten einen erheblichen Mehrwert bietet. Übungen bieten die Chance, in einer sicheren Umgebung, ohne die Konsequenzen eines Ernstfalls, Handlungsbedarf aufzudecken und auf diesem Wege eine Verbesserung der IT-Notfall- und Krisenreaktion zu erreichen und zu erhalten. Bei Übungen dürfen Fehler auftreten. Die korrekte Aufarbeitung dieser Fehler kann zur Optimierung der Reaktionsprozesse beitragen.

Durch Übungen können im Einzelnen folgende Ziele erreicht werden:

- Vorhandene Konzepte, Strukturen, Maßnahmen und Kommunikationsmittel werden regelmäßig auf Funktionsfähigkeit überprüft. Es besteht eine hohe Wahrscheinlichkeit, dass diese auch bei sorgfältiger Ausarbeitung im Ernstfall nicht wie gewünscht funktionieren, wenn sie nicht zuvor geübt wurden. Dies liegt unter anderem daran, dass sie außerhalb von IT-Krisen und Notfällen nie oder fast nie zum Einsatz kommen.
- Die Fähigkeiten aller Beteiligten werden ausgebaut und ihre Handlungssicherheit wird im Ernstfall verbessert. Gut geübtes und eingespieltes Personal beherrscht auch Lagen besser, die zuvor nicht geübt wurden.
- Zwischen den UP-KRITIS-Partnern wird eine vertrauensvolle Kommunikation aufgebaut und es werden wertvolle Kontakte ermöglicht und gefestigt.

- Bei den UP-KRITIS-Partnern wird zusätzliches Bewusstsein für die Notwendigkeit einer übergreifenden Zusammenarbeit, die gegenseitigen Abhängigkeiten und die Notwendigkeit von Übungen geschaffen.
- Die gegenseitigen Erwartungen der UP-KRITIS-Partner bei der IT-Notfall- und Krisenbewältigung werden offengelegt. Zeigt sich in der Übung, dass Erwartungen nicht entsprochen werden, können daraus folgende Schwachstellen bei der IT-Notfall- und Krisenbewältigung identifiziert werden.
- Es wird herausgefunden, wo und zu welchem Zeitpunkt eine Zusammenarbeit bei IT-Notfällen und Krisen sinnvoll und notwendig ist.
- Branchen- beziehungsweise sektorübergreifende gegenseitige Abhängigkeiten von Kritischen Infrastrukturen werden verdeutlicht. Zuvor nicht identifizierte Abhängigkeiten können ebenfalls auf bestehende Schwachstellen bei der IT-Notfall- und Krisenbewältigung hinweisen.
- Es werden Erfahrungen in der Zusammenarbeit mit dem IT-Lage- und Krisenreaktionszentrum des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gesammelt.
- Es werden der UP-KRITIS-Arbeitsgruppe „Krisenreaktion und -bewältigung“ Anregungen gegeben, um geeignete Strukturen, Konzepte und Maßnahmen zur gemeinsamen IT-Notfall- und Krisenbewältigung zu entwickeln.

Zusammenfassend ist festzustellen, dass IT-Notfall- und Krisenübungen eine wesentliche Voraussetzung sind, um angemessene, optimale Reaktionsprozesse zu erreichen. Es wird jedoch ausdrücklich betont, dass die Teilnahme an Übungen auf freiwilliger Basis erfolgt. Die UP-KRITIS-Partner entscheiden bei jeder geplanten Übung selbst, ob und in welchem Rahmen sie sich beteiligen. Auch nachdem ein Partner seine Teilnahme an einer bestimmten Übung erklärt hat, kann er ohne Angabe von Gründen in jeder Phase der Übungsvorbereitung und -durchführung seine Teilnahme beenden, wenn dies die Umstände für ihn erfordern.

## 2 Anwenderkreis

Das vorliegende Dokument wendet sich in erster Linie an folgende Anwender:

- Mitglieder der UP-KRITIS-Arbeitsgruppen: Ihre Aufgabe ist es, das Übungskonzept in den Institutionen und Unternehmen, denen sie angehören, bekannt zu machen, Rahmenbedingungen für Übungen zu beschließen, an der konkreten Planung von Übungen mitzuarbeiten und die Bereitstellung der für die Übungen notwendigen Ressourcen in ihren Institutionen und Unternehmen zu ermöglichen.
- KRITIS-Ansprechpartner der Branchen (SPOCs): Diese sind aufgrund ihrer Funktion in viele Übungen involviert (Beispiel Alarmübung) und müssen die Übungen daher verstehen und kennen.
- Die Leitungsebene in Behörden und Unternehmen, die Kritische Infrastrukturen betreiben, mit diesen zusammenarbeiten oder in deren Schutz involviert sind: Dieser Anwenderkreis sollte eine summarische Kenntnis der Gründe für und der Ziele von IT-Notfall- und Krisenübungen im Rahmen des UP KRITIS erhalten. Diese Kenntnis ist erforderlich, da die Übungen Kosten und Aufwand verursachen und deshalb mit der Leitungsebene abgestimmt werden müssen.
- Alle Krisenstabsleiter und -mitglieder und weitere potenziell Verantwortliche sollten, soweit sie betroffen sein können, rechtzeitig im Vorfeld Kenntnis dieses Konzepts haben. Dies ist auch sachdienlich im Hinblick auf mögliche Verzahnungen von KRITIS- und unternehmensinternen Übungen und der Verknüpfung mit bestehenden Übungsreihen wie LÜKEX.
- Mitarbeiter im Bundesministerium des Innern und in zugeordneten Geschäftsbereichen (besonders im BSI und BBK), die mit Aufgaben im Rahmen des KRITIS-Schutzes betraut sind.
- Mitarbeiter von Aufsichts- und Regulierungsbehörden für Betreiber Kritischer Infrastrukturen (zum Beispiel BaFin und Bundesnetzagentur): Die Übungen sind ein Beitrag zum oftmals gesetzlich geforderten Risikomanagement für Unternehmen.
- Vertreter von Interessenverbänden von Wirtschaftszweigen, die den Kritischen Infrastrukturen zuzurechnen sind.

# 3 Abgrenzungen

Die im vorliegenden Konzept vorgestellten Übungen ergänzen die bereits in Deutschland durchgeführten Katastrophenschutz- und Notfallübungen. Während bei Katastrophenschutz- und Notfallübungen die Wiederherstellung physischer Infrastrukturen und der Umgang mit Personenschäden im Vordergrund stehen, liegt der Fokus der hier beschriebenen Übungsszenarien auf den Informationsinfrastrukturen, die zum Betrieb der Kritischen Infrastrukturen notwendig sind. Es wird als notwendig erachtet, KRITIS-Übungen auch in staatliche Katastrophenschutz- und Notfallübungen wie zum Beispiel LÜKEX zu integrieren. Diese angestrebte Integration wird durch das vorliegende Konzept unterstützt.

Ebenso gibt es eine Abgrenzung zu individuellen Einzelübungen von Betreibern Kritischer Infrastrukturen. Die Einzelübungen konzentrieren sich in der Regel auf die interne Bewältigung von IT-Krisen und Notfällen. Gegenstand der hier vorgestellten Übungen ist dagegen die übergreifende Zusammenarbeit von KRITIS-Unternehmen und betroffenen staatlichen Stellen. Eine Verknüpfung von KRITIS-Übungen mit internen Übungen kann für UP-KRITIS-Partner sinnvoll sein, ist aber keine Voraussetzung für die Durchführung der KRITIS-Übungen. Die Entscheidung über eine mögliche Verknüpfung wird daher von jedem UP-KRITIS-Partner im Einzelfall getroffen.

## 4 Übungsarten

Je nach dem Zweck einer Übung können Inhalte und Form sehr unterschiedlich sein. In einem ersten Ansatz kann danach differenziert werden, was in der Übung geschieht:

- Diskussionsorientierte Übungen behandeln auf theoretischer Ebene mögliche Verfahren, Planungen oder Konzepte für den IT-Krisenfall. Dabei werden Abläufe und Lösungsmöglichkeiten vorgestellt und diskutiert. Sie dienen also eher der Neuentwicklung von geeigneten IT-Notfall- und Krisenreaktionen als der Überprüfung. Sie eignen sich für einen Einstieg in ein neues Thema.
- Handlungsorientierte Übungen dienen dem realitätsnahen „Ausprobieren“, Einüben und Überprüfen von Verfahren, Plänen, Konzepten, Absprachen etc. Sie können einerseits den Beteiligten wertvolle Erfahrungen vermitteln und andererseits Planungsfehler, Lücken, Ressourcenmängel, fehlende Verantwortlichkeiten etc. aufdecken. So kann die Leistungsfähigkeit der Übenden erhöht und gleichzeitig die Aktualität des Geübten sichergestellt werden.

Eine weitere Unterscheidung ist im Hinblick auf die Zielgruppen der Übungen sinnvoll. Hier sind drei Ebenen zu nennen:

- In operativen Übungen wird das konkrete Arbeiten und Vorgehen der Umsetzungsebene geübt. Für solche Übungen eignen sich Verfahren, die klar organisiert und gegebenenfalls technisch unterstützt sind. Teilnehmer sind Mitarbeiter aus dem operativen Betrieb oder von Notfallteams der übenden Organisationen.
- Bei taktischen Übungen steht das Koordinieren, Zusammenarbeiten und Entscheiden im Vordergrund, gerade auch zwischen unterschiedlichen Organisationen. Hier liegt der Hauptfokus des vorliegenden Konzepts. Zielgruppe sind die für den IT-Krisenfall vorgesehenen Koordinationsstrukturen.
- Die strategischen Übungen richten sich an die Führungsebene. Hier geht es um die generelle Art des Zusammenwirkens der beteiligten Organisationen und damit verbundene komplexe Entscheidungen.

## Übungsarten im Rahmen des UP KRITIS

Auch für die Zwecke dieses Konzepts ist es sinnvoll, unterschiedliche Ansätze in Bezug auf die Übungsziele, den Übungsaufwand und die Übungsteilnehmer zu mischen. Im Rahmen des UP KRITIS sollen folgende Übungsarten zum Einsatz kommen:

- Eine Planbesprechung/Planübung ist die einzige diskussionsorientierte Übung. Sie ist sowohl für die taktische als auch für die strategische Ebene tauglich und kann als Allzweckmittel zur Übung beliebiger Inhalte verwendet werden. Es handelt sich um eine Besprechung des Ablaufs einer IT-Notfall-/Krisenreaktion auf festgelegte Szenarien mit Fachleuten und Führungskräften am „grünen Tisch“ als gemeinsame konstruktive Diskussion mit Moderation und Leitfaden, gegebenenfalls auch mit Fachvortrag zum geübten Thema.
- Eine Kommunikationsübung ist eine Übung auf allen Ebenen. Sie dient zur Überprüfung von Erreichbarkeiten und Abläufen bei der Alarmierung sowie zur Überprüfung der Funktionsfähigkeit der Kommunikationsmittel und -verfahren, die im IT-Not- bzw. Krisenfall (oder zur Diskussion von komplexen Lagen, die Krisenpotenzial haben) zum Einsatz kommen sollen.
- Eine Koordinationsübung findet auf der operativen und taktischen Ebene statt. Dabei üben die Leitungs- und Stabsstrukturen sowie die Lage- und Krisenreaktionszentren der beteiligten Organisationen die Reaktion auf ein festgelegtes Szenario, ohne dass eine tatsächliche Umsetzung der Ereignisse und Maßnahmen erfolgt. Zugleich werden auch die infrastrukturellen und technischen Voraussetzungen der zentralen Krisenreaktionsorganisation überprüft.
- Die erweiterte Koordinationsübung bezieht zusätzliche Ebenen mit ein. Es geht um das Durchspielen der IT-Krisenreaktion auf ein festgelegtes Szenario unter möglichst realistischen Bedingungen mit allen Beteiligten. Nach Möglichkeit werden dabei Ereignisse real nachgestellt und beschlossene Maßnahmen tatsächlich durchgeführt.

Für die Durchführung aller genannten Übungsarten mit Ausnahme der Planbesprechung/Planübung ist das Vorhandensein geeigneter organisatorischer und technischer Grundstrukturen zur Krisenkommunikation und -bewältigung<sup>2</sup> eine notwendige Voraussetzung. Planbesprechungen und -übungen können dagegen ohne diese Voraussetzungen durchge-

<sup>2</sup> Das Konzept „Früherkennung und Bewältigung von IT-Krisen“ enthält die Beschreibung der Grundstrukturen.

führt werden. Eine ausführliche Beschreibung der einzelnen Übungsarten findet sich in dem separaten Anlagendokument zum vorliegenden Konzept.

## Aufwand und Dauer

In den nachfolgenden Übersichtstabellen 1 und 2 werden die einzelnen Übungsarten bezüglich ihres Aufwands und ihrer Dauer gegenübergestellt. Bei der Planung wird der meiste Aufwand typischerweise durch ein Team von wenigen Personen geleistet. Der Übungsaufwand selbst wird dagegen eher durch die im Normalfall große Anzahl von Übungsbeteiligten hervorgerufen. Der Planungsaufwand für eine einzelne Übung reduziert sich, wenn Übungsserien in immer gleicher Weise (zum Beispiel Alarmauslösung) durchgeführt werden.

**Tabelle 1: Übungs- und Planungsaufwand für die Übungsarten**

Übungsart	Planungsaufwand	Übungsaufwand
Planbesprechung/Planübung	gering	gering
Kommunikationsübung	mittel	gering bis mittel
Koordinationsübung	hoch bis sehr hoch	mittel bis sehr hoch
Erweiterte Koordinationsübung	hoch bis sehr hoch	sehr hoch

Erläuterung des Aufwands:

gering: Personenwoche

mittel: mehrere Personenwochen

hoch: mehrere Personenmonate

sehr hoch: Personenjahre

Die Planungsdauer für komplexe Übungen mit vielen Teilnehmern kann mehr als ein Jahr betragen. Es ist daher auf einen rechtzeitigen Beginn bezüglich eines angestrebten Übungstermins zu achten. Demgegenüber ist die Dauer der eigentlichen Übung kurz, um zu vermeiden, dass bei den beteiligten UP-KRITIS-Partnern Produktions- und Verwaltungsprozesse durch für die Übung abgezogenes Personal beeinträchtigt werden. Als Maximaldauer für eine KRITIS-Übung sind mehrere Tage denkbar, wenn komplexe IT-Krisensituationen eventuell auch im internationalen Verbund geübt werden sollen.

**Tabelle 2: Übungs- und Planungsdauer für die Übungsarten**

Übungsart	Planungsdauer	maximale Übungsdauer
Planbesprechung/Planübung	mittel	sehr kurz
Kommunikationsübung	mittel	kurz
Koordinationsübung	lang	kurz
Erweiterte Koordinationsübung	lang	kurz

Erläuterung der Dauer:

sehr kurz: bis zu einem Tag

kurz: mehr als ein Tag bis zu einer Woche

mittel: mehrere Wochen

lang: mehrere Monate und länger

# 5 Übungsszenarien

Ein Szenario umfasst eine Ausgangssituation und in der Regel eine Abfolge von Ereignissen, auf die durch den Übenden reagiert werden muss (Was wäre, wenn ...). Das Szenario kann fiktive realitätsnahe oder reale Vorfälle enthalten und liefert die für die Übung relevanten Grundinformationen oder Annahmen. Detailliert wird das Szenario durch eine Lage, die konkret die Übungsumgebung zur Ausgangssituation beschreibt.

Einspielungen von kleineren detaillierten Einlagen (zum Beispiel eine Beobachtung, eine eingehende Meldung, ein Pressebericht) in der Folge ergänzen, erweitern oder verändern das Szenario so, dass die Teilnehmer zum Reagieren und Handeln gebracht werden, weitere Informationen erhalten und die Anpassungsfähigkeit und Belastbarkeit der IT-Notfall- bzw. Krisenreaktion geprüft wird.

Zusätzliche Annahmen und sogenannte Übungskünstlichkeiten sind ggf. in die Szenarien einzubeziehen, da nicht alles real gespielt werden kann oder soll, was bei IT-Krisen- und Notfällen passiert (zum Beispiel Annahme des Ausfalls der Telefonanlage, obwohl alle Apparate funktionieren, oder Darstellung aller externen Kontakte durch die Übungsleitung).

Bei Szenarien wird außerdem generell zwischen Ursachen- und Wirkungsszenarien unterschieden:

- Ein Ursachenszenario beinhaltet die zugrundeliegenden Ursachen (Stromausfall, Virenbefall, Hackereinbruch usw.).
- Ein Wirkungsszenario geht von definierten Ausfällen/Beeinträchtigungen aus (zum Beispiel Ausfall eines Rechenzentrums), ohne die Ursachen zu berücksichtigen.

Je nach Übungsart und -ziel ist zu entscheiden, welcher der beiden Szenariotypen besser geeignet ist. Ursachenszenarien bieten sich an, wenn Ursachenerforschung, Problembehebungsvorgänge oder ursachenabhängige Schadensbegrenzungsprozesse geübt werden sollen. Wirkungsszenarien werden verwendet, wenn ursachenunabhängige Reaktionsprozesse im Fokus stehen oder gegenseitige Abhängigkeiten Kritischer Infrastrukturen erforscht werden sollen.

Im Kontext des vorliegenden Konzepts müssen die Szenarien zudem so beschaffen sein, dass sie

- sowohl die Verfügbarkeit der IT, die zum Betrieb der Kritischen Infrastrukturen notwendig ist, schwerwiegend beeinträchtigen
- als auch das Potenzial zu einer gravierenden und nach Möglichkeit sektorübergreifenden Beeinträchtigung Kritischer Infrastrukturen besitzen.

In vielen Fällen ist ein Einzelereignis nicht ausreichend, um die vorgeannten Bedingungen zu erfüllen. Es sollen daher auch Szenarien in Betracht gezogen werden, die aus mehreren (gegebenenfalls auch unabhängigen) Ereignissen bestehen, die gleichzeitig oder in enger zeitlicher Abfolge an mehreren Stellen auftreten (verteilte Ereignisse).

Es ist hilfreich, zuerst die Kommunikationswege und -schnittstellen zu üben und dann die Szenarien zu üben, denen die höchste Eintrittswahrscheinlichkeit zugebilligt wird. Es ist dabei aber festzuhalten, dass eine exakte Wahrscheinlichkeitsbestimmung oft sehr schwierig ist.

Weitere zu betrachtende Aspekte bei der Festlegung von Szenarien sind:

- die genaue Festlegung der beeinträchtigten Ressourcen und die Art und der Umfang der Beeinträchtigung
- Hintergründe und Ziele von Ursachenszenarien, die vorsätzlich durch Personen ausgelöst werden
- die zeitliche Abfolge und räumliche Verteilung (bei verteilten Ereignissen)

## Übungsgrundszzenarien

Im Rahmen des UP KRITIS hat man sich auf mehrere Grundszzenarien verständigt, die im KRITIS-Umfeld besonders geeignet erscheinen und daher primär geübt werden sollen:

- der Ausfall von Versorgungsleistungen, die für den IT-Betrieb wichtig sind, z. B.:
  - ein großflächiger Ausfall der Energieversorgung
  - der Ausfall der Klimaversorgung von Rechenzentren durch extreme klimatische Bedingungen
  - der Ausfall zentraler Leitstände
  - der Ausfall von zentralen Kommunikationssystemen, zum Beispiel Kernnetze, über die diverse Services (Internet, Telefonie, Datentransfer, ...) abgewickelt werden
  - umfassender Ausfall des Betreiberpersonals
- physische Angriffe mit dem Ziel, die IT-Infrastruktur zu übernehmen oder außer Betrieb zu setzen, z. B.:
  - auf Rechenzentren
  - auf zentrale Netzknoten
  - auf zentrale Netzwerkverbindungen
- logische Angriffe mit offensichtlich umfassenden finanziellen Mitteln und technischem Wissen, zum Beispiel:
  - Angriff auf zentrale Netzknoten
  - großflächiger Malware-Befall
  - Denial-of-Service-Angriffe auf kritische IT-Systeme
  - gezielter unbefugter Zugang zu kritischen IT-Systemen und Missbrauch der Systeme

# 6 Übungsplan

Die UP-KRITIS-Partner sind sich darüber einig, dass die Vorkehrungen für eine optimale IT-Notfall- und Krisenreaktion kontinuierlich aktualisiert und erhalten werden müssen. Ein geeigneter strategischer Übungsplan trägt dazu wesentlich bei.

## 6.1 Aufbau- und Erhaltungsphase

Der Übungsplan untergliedert sich in eine Aufbauphase und eine Erhaltungsphase. In der Aufbauphase geht es darum, durch Übungen mit aufeinander aufbauendem Schwierigkeitsgrad

- Handlungsbedarf aufzudecken,
- Grundlagen für die Arbeit im UP KRITIS zur Krisenreaktion und -bewältigung zu liefern,
- neue Verfahren und Techniken zu erproben, die durch die vorgenannte Arbeitsgruppe zur Verfügung gestellt werden,
- am Ende erstmalig die erforderliche Reaktionsfähigkeit bezüglich der betrachteten Szenarien nachgewiesen zu haben.

Die Aufbauphase soll innerhalb von drei Jahren abgeschlossen werden.

Ziel der darauf folgenden Erhaltungsphase ist es, die erforderliche Reaktionsfähigkeit auch für die Zukunft zu gewährleisten und zu verfestigen. Die Dauer der Erhaltungsphase ist nicht begrenzt. Weitreichende Änderungen der Kommunikationsstruktur, der Übungsteilnehmer oder anderer Ressourcen können es jedoch erforderlich machen, mit einer neuerlichen Aufbauphase zu beginnen.

## 6.2 Strategischer KRITIS-Übungsplan

Um die in den vorangegangenen Kapiteln genannten Ziele zu erreichen, haben sich die UP-KRITIS-Partner auf einen strategischen Übungsplan für die Aufbau- und die Erhaltungsphase geeinigt.

Der Übungsplan für die Aufbauphase ist in Abbildung 1 als Übersichtsgrafik und nachfolgend in Tabelle 3 mit zusätzlichen Erläuterungen dargestellt:

**Abbildung 1: Übungsplan Aufbauphase**

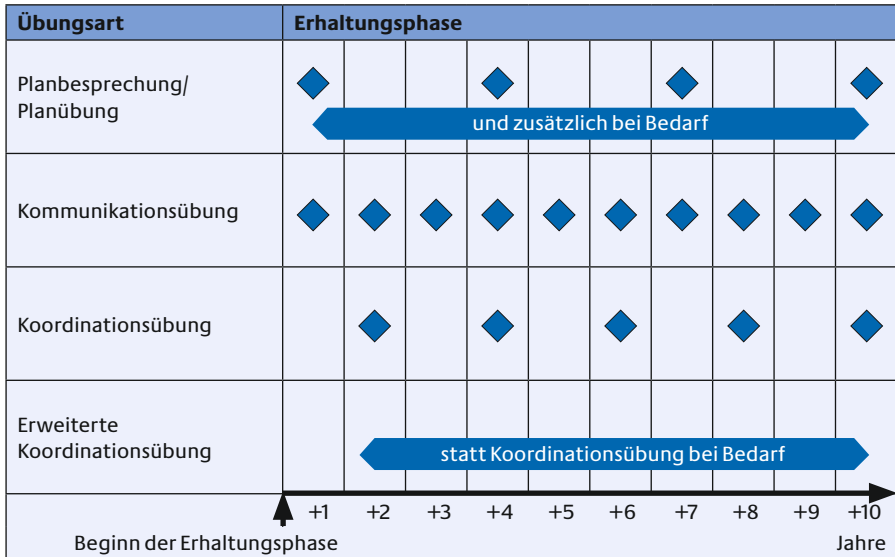
Übungsart	Aufbauphase		
Planbesprechung/ Planübung	◆ ◆	◆	◆
Kommunikationsübung		◆	◆
Koordinationsübung			◆

**Tabelle 3: Häufigkeit der Übungsarten in der Aufbauphase**

Übungsart	Häufigkeit in der Aufbauphase	Anmerkungen
Planbesprechung/ Planübung	4 x	Hauptfokus ist das Herausarbeiten von Anforderungen für die Arbeitsgruppe „Krisenreaktion und -bewältigung“, vorgeschlagene Szenarien sind zum Beispiel ein Stromausfall und logische Angriffe auf die IT.
Kommunikations- übung	3 x	Durchführung erst möglich nach Festlegung und nach Implementierung der durch die Arbeitsgruppe „Krisenreaktion und -bewältigung“ vorgeschlagenen notwendigen Kommunikationsstruktur.
Koordinationsübung	2 x	Durchführung erst möglich nach Festlegung und nach Implementierung der durch die Arbeitsgruppe „Krisenreaktion und -bewältigung“ vorgeschlagenen notwendigen Kommunikationsstruktur, nach Möglichkeit Anbindung an die LÜKEX 2009 und eventuell Cyber Storm 2010.

Der Übungsplan für die Erhaltungsphase ist in gleicher Form nachfolgend in Abbildung 2 und in Tabelle 4 dargestellt.

**Abbildung 2: Übungsplan Erhaltungsphase**



**Tabelle 4: Häufigkeit der Übungsarten in der Erhaltungsphase**

Übungsart	Häufigkeit in der Erhaltungsphase	Anmerkungen
Planbesprechung/ Planübung	Alle 3 Jahre und zusätzlich bei Bedarf	Bedarfsweise, zum Beispiel beim Auftauchen neuartiger, zu berücksichtigender IT-Krisenszenarien, auf die durch vorhandene Vorkehrungen nicht ausreichend reagiert werden kann
Kommunikationsübung	Jährlich	Eine funktionstüchtige Alarmierung und anforderungsgerecht funktionierende Kommunikationsmittel sind grundlegende Voraussetzungen für jede IT-Notfall- und Krisenreaktion
Koordinationsübung	Alle 2 Jahre	Möglichst kombiniert mit anderen nationalen oder internationalen Übungen wie zum Beispiel LÜKEX oder Cyber Storm
Erweiterte Koordinationsübung	Nach Bedarf statt einer Koordinationsübung	Möglichst kombiniert mit anderen nationalen oder internationalen Übungen wie zum Beispiel LÜKEX oder Cyber Storm

## Detailplanung

Der strategische Übungsplan bedarf weiterer Detaillierung in Form einer konkreten Übungsplanung (siehe separates Anlagendokument zum vorliegenden Konzept) für jede der aufgeführten Übungen. Dazu ist vorgesehen, dass die UP-KRITIS-Partner in Zukunft anlässlich regelmäßiger Treffen Rahmenbedingungen für anstehende Übungen beschließen, ihre grundsätzliche Teilnahmebereitschaft erklären und Mitglieder der Arbeitsgruppe und/oder externe Stellen mit der weiteren Detailplanung beauftragen. Es ist darauf zu achten, dass genügend Zeitvorlauf eingeplant wird, um eine gründliche Übungsplanung zu ermöglichen (siehe Tabelle 1 in Kapitel 4). Das beauftragte und dem Übungsaufwand angemessene Planungsteam berichtet den Stand seiner Arbeit an die UP-KRITIS-Partner und lässt sich Abnahmen erteilen.

Zu beschließende Rahmenbedingungen, die eine Grundlage für eine erste Beteiligungsentscheidung für jede durchzuführende Übung darstellen, sind:

- die Ziele und der Nutzen der Übung (WAS soll erreicht werden?)
- das Szenario (Von WELCHER Situation wird ausgegangen?)
- der Teilnehmerkreis (WER?)
- der Zeitpunkt der Durchführung und die beabsichtigte Dauer (WANN?, WIE LANGE?)
- die Durchführung als angekündigte oder unangekündigte Übung (WIE ÜBERRASCHEND?)
- das Risiko (WIE RISIKOREICH?)
- die Vertraulichkeitsanforderungen (WIE HEIKEL?)

Um die weitere Planung zu ermöglichen, sind außerdem zu fixieren und im Nachgang weiter zu detaillieren:

- die Besetzung des Planungsteams für die Übung, der Übungsleitung und des Auswertungsteams, gegebenenfalls mit externer Unterstützung (MIT WEM?)
- die erforderlichen Abnahmen von Zwischen- und Endergebnissen wie zum Beispiel dem Übungsplan durch die UP-KRITIS-Partner (WELCHE KONTROLLE?)

- eine Grobschätzung des notwendigen Finanz- und Personalbudgets für Vorbereitung, Durchführung und Nachbereitung der Übung sowie die Kosten- und Aufwandsübernahme (WER WIEVIEL?)

Bezüglich der Kosten- und Aufwandsübernahme gilt generell:

- BMI und BSI unterstützen die Übungsvorbereitung und -nachbereitung in wesentlichen Teilen. Kosten und Aufwand für notwendige Zulieferungen zur Übungsvorbereitung und -nachbereitung der teilnehmenden UP-KRITIS-Partner sowie für interne Übungsvorbereitungen verbleiben jedoch bei den einzelnen Partnern.
- Bezüglich der Übungsdurchführung übernimmt jeder der teilnehmenden UP-KRITIS-Partner seinen anfallenden Aufwand und die Kosten selbst.

Weiterführende Erläuterungen zu den Rahmenbedingungen sind im separaten Anlagendokument zum vorliegenden Konzept aufgeführt.

## **Integration neuer Partner**

Für neu hinzukommende UP-KRITIS-Partner besteht die Möglichkeit, auch nachträglich in den strategischen Übungsplan einzusteigen. Erforderliche Hilfestellungen werden angeboten. Die Teilnahme an Planbesprechungen und -übungen ist jederzeit ohne weitere Voraussetzungen möglich. Für andere Übungsarten sind die Integration in das Konzept zur Früherkennung und Bewältigung von IT-Krisen und eine bezüglich des Planungsstands rechtzeitige Beteiligungsentscheidung Mindestvoraussetzung. Gegebenenfalls sollte neuen UP-KRITIS-Partnern, die das erste Mal an einer komplexen Koordinationsübung teilnehmen, auch die Möglichkeit gegeben werden, nur solche Teile der Übung mitzuspielen (zum Beispiel die Alarmierung), die ihrem jeweiligen UP-KRITIS-Integrationsstand entsprechen.

## 7 Ausblick und nächste Schritte

Die Übungen sollen dazu beitragen, möglichst schnell belastungsfähige, branchenübergreifende Reaktionen auf IT-Krisen innerhalb der Kritischen Infrastrukturen zu ermöglichen. Dabei wird zunächst kurzfristig mit einfachen Basisübungen begonnen und der Schwierigkeits- und Realitätsgrad nach und nach gesteigert. Eine der ersten Übungen sollte der Verifikation der Kommunikationswege und Kontaktstellen dienen. Durch das Vernetzen relevanter Bereiche aus der Wirtschaft und der Verwaltung von Bund und Ländern wird ein großer Mehrwert in der Behandlung kritischer Ereignisse erzielt. Das vorliegende Dokument ist die gemeinsame Grundlage für die Erstellung künftiger Übungsplanungen und der darauf folgenden Aktivitäten.

# Anhang

# Abkürzungen

<b>BaFin</b>	Bundesanstalt für Finanzdienstleistungsaufsicht
<b>BBK</b>	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
<b>BMI</b>	Bundesministerium des Innern
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik
<b>IKT</b>	Informations- und Kommunikationstechnik
<b>IT</b>	Informationstechnik
<b>KRITIS</b>	Kritische Infrastrukturen
<b>NPSI</b>	Nationaler Plan zum Schutz der Informationsinfrastrukturen
<b>SPOC</b>	Single Point of Contact
<b>UP</b>	Umsetzungsplan
<b>UP KRITIS</b>	Umsetzungsplan KRITIS

# Glossar

## **Akteure**

Die Hauptaufgabe von Akteuren ist es, Übende vor dem Übungsbeginn in das Ausgangsszenario einzuweisen und im Übungsverlauf weitere Ereignisse einzuspielen. Daneben haben sie folgende Aufgaben:

- Protokollierung von unmittelbaren Reaktionen der Übenden, zum Beispiel am Telefon
- gegebenenfalls Abhalten von Fachvorträgen, die in die Übung eingeschoben werden

## **Betreiber Kritischer Infrastrukturen**

Betreiber Kritischer Infrastrukturen sind privatwirtschaftliche Unternehmen oder Behörden, die Dienstleistungen in den Kritischen Infrastrukturen erbringen.

## **Einspielung**

Einspielungen sind Ereignisse (zum Beispiel eine Beobachtung, eine eingehende Meldung, ein Pressebericht), die in Übungen Ausgangsszenarien in der Folge ergänzen, erweitern oder so verändern, dass die Teilnehmer zum Reagieren und Handeln gebracht werden, weitere Informationen erhalten und die Anpassungsfähigkeit und Belastbarkeit der Notfall-beziehungsweise Krisenreaktion geprüft wird.

## **Informationsinfrastruktur**

Die Gesamtheit der IT-Anteile einer Infrastruktur wird als deren Informationsinfrastruktur bezeichnet.

## **Informationstechnik**

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 und die Ausgabe von Informationen.

<b>IT-Krise</b>	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.
<b>IT-Sicherheit</b>	IT-Sicherheit ist der Zustand, in dem Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.
<b>Katastrophe</b>	(Groß-)Schadensereignis natürlichen Ursprungs (Erdbeben, Sturmfluten, Vulkanausbruch etc.) oder durch menschliche Aktivitäten verursacht (Chemieunfall, Flugzeugabsturz, Anschlag etc.), das zu einer gegenwärtigen Gefahr für das Leben oder die Gesundheit einer Vielzahl von Menschen, für die Umwelt oder für sonstige bedeutsame Rechtsgüter führen und von den für die Gefahrenabwehr zuständigen Behörden mit eigenen Kräften und Mitteln nicht angemessen bewältigt werden kann.
<b>Krise</b>	Eine vom Normalzustand abweichende, sich plötzlich oder schleichend entwickelnde Lage, die durch ein Risikopotenzial gekennzeichnet ist, das Gefahren und Schäden für Leib und Leben von Menschen, bedeutende Sachwerte, schwerwiegende Gefährdungen des politischen, sozialen oder wirtschaftlichen Systems in sich birgt und der Entscheidung – oftmals unter Unsicherheit und unvollständiger Information – bedarf.

## **Krisenbewältigung**

Die Durchführung von Maßnahmen mit dem Ziel der schnellstmöglichen Zurückführung einer akuten Krisensituation in den Normalzustand und der Minimierung ihrer Auswirkungen.

## **Krisenmanagement**

Schaffung von konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen, die eine schnellstmögliche Zurückführung der eingetretenen außergewöhnlichen Situation in den Normalzustand unterstützen.

## **Kritische Infrastruktur**

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

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

<b>Nachbereitungsteam</b>	Das Nachbereitungsteam ist dafür zuständig, den Übungsverlauf auszuwerten und darüber Berichte zu erstellen. Es greift dabei auf Auswertungsfragebogen und die erstellten Übungsprotokolle zu.
<b>Planungsteam</b>	Das Planungsteam ist dafür zuständig, eine Übung im Vorfeld detailliert auszuarbeiten. Es erstellt dabei den Grob- und den Feinplan für die Übung.
<b>SPOC</b>	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.
<b>Szenario</b>	<p>Ein Szenario ist eine Situation beziehungsweise eine Abfolge von Ereignissen, auf die durch den Übenden reagiert werden muss (Was wäre, wenn...).</p> <p>Es wird dabei zwischen Ursachen- und Wirkungsszenarien unterschieden:</p> <ul style="list-style-type: none"> <li>■ Ein Wirkungsszenario geht von definierten Ausfällen/Beeinträchtigungen aus (zum Beispiel Ausfall eines Rechenzentrums), ohne die Ursachen zu berücksichtigen.</li> <li>■ Ein Ursachenszenario beinhaltet zusätzlich die zugrundeliegenden Ursachen (Stromausfall, Virenbefall, Hackereinbruch usw.).</li> </ul> <p>Je nach Übungsart und -ziel ist zu entscheiden, welcher der beiden Szenariotypen besser geeignet ist. Ursachenszenarien bieten sich an, wenn Ursachenerforschung, Problembehebungsvorgänge oder ursachenabhängige Schadensbegrenzungsprozesse geübt werden sollen. Wirkungsszenarien werden verwendet, wenn ursachenunabhängige Reaktionsprozesse im Fokus stehen oder gegenseitige Abhängigkeiten Kritischer Infrastrukturen erforscht werden sollen.</p>

<b>Übende</b>	<p>Übende spielen bei einer Übung Aufgaben nach, in die sie auch im Ernstfall als Teil der Notfall- bzw. Krisenreaktion involviert sind. Zusätzliche Tätigkeiten bestehen darin,</p> <ul style="list-style-type: none"> <li>■ an der Übungseinweisung teilzunehmen, bevor mit den eigentlichen Notfall- und Krisenaktivitäten begonnen wird,</li> <li>■ ggf. an Fachvorträgen teilzunehmen, die in den Übungsverlauf eingebaut werden, um die Übenden mit nötigem Hintergrundwissen zu versorgen,</li> <li>■ ggf. regelmäßig oder auf Anforderung Statusberichte an die Übungsleitung zu liefern,</li> <li>■ ggf. Auswertungsfragebögen nach dem Ende der Übung auszufüllen und an die Übungsleitung zu übergeben.</li> </ul>
<b>Übung</b>	<p>Unter dem Begriff Übung wird das Durchspielen von Reaktionen auf Notfälle und Krisen sowie die Funktionsüberprüfung von Einrichtungen zur Notfall- und Krisenreaktion verstanden, ohne dass ein realer Ernstfall vorliegt.</p>
<b>Übungsbeobachter</b>	<p>Übungsbeobachter protokollieren während der Übungsdurchführung die von den Übenden ausgeführten Aktivitäten. Dabei werden zum Beispiel auch erreichte Zeiten und bemerkenswerte Entdeckungen wie unerwartete Schwierigkeiten oder Verbesserungspotenzial erfasst.</p>
<b>Übungsbestimmungen</b>	<p>Es handelt sich dabei um im Übungsvorlauf definierte Regelungen, die von den Übenden während des Übungsablaufs einzuhalten sind.</p>

- Übungsdrehbuch** Bei komplexen Übungen erweist es sich als sinnvoll, ähnlich wie beim Film den geplanten Verlauf in Form eines detaillierten Drehbuchs zu dokumentieren. Das Drehbuch enthält alle dem Gesamtzenario der Übung zugehörigen Ereignisse und zugehörige Informationen wie die Art der Benachrichtigung und erwartete Reaktionen.
- Übungskünstlichkeiten** In einer Übung kann und soll nicht alles real nachvollzogen werden, was bei Krisen und Notfällen passiert (zum Beispiel Feuer, Ausfall von IKT-Systemen, Datenverlust, Kontakt zu Medienvertretern). Man arbeitet in diesem Fall mit Annahmen oder Simulationen. Diese bezeichnet man als Übungskünstlichkeiten.
- Übungsleiter** Ein Übungsleiter ist für die Durchführung jeder Übung notwendig. Er koordiniert den gesamten Übungsverlauf inklusive des Auf- und Abbaus der Übungsumgebung. Dies umfasst typischerweise folgende Aufgaben:
- Start und Beendigung der Übung
  - Zentrale Anlaufstelle für Fragen und Probleme, die im Übungsverlauf entstehen
  - Anweisung von Ad-hoc-Änderungen im vorgesehenen Übungsablauf oder vorzeitiger Abbruch bei schwerwiegenden, nicht behebbaren Komplikationen
  - Moderation von Planbesprechungen und -übungen
  - Koordination der Versorgung (zum Beispiel Verpflegung) der Übungsbeteiligten
- Übungsleitgruppe** Bei komplexen Übungen ist es gegebenenfalls notwendig, dem Übungsleiter unterstützende Mitarbeiter an die Hand zu geben. Diese werden als Übungsleitgruppe bezeichnet.

**UP-KRITIS-  
Partner**

Alle Behörden, Interessenverbände, Unternehmen usw., die im Rahmen des Umsetzungsplans Kritische Infrastrukturen zusammenarbeiten (zum Beispiel in Arbeitsgruppen) und an Übungen teilnehmen.

# Literaturverzeichnis

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

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

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

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

Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Berlin, 2008.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): COMCHECK und ALEX – Beschreibungen, Checkliste und Hilfen für Kommunikationsüberprüfungen und Übungen. Bonn, 2006.

# Beteiligte UP-KRITIS-Partner

Allianz Deutschland AG  
Arcor AG & Co. KG  
Bundesamt für Sicherheit in der Informationstechnik (BSI)  
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)  
Bundesverband deutscher Banken  
Commerzbank AG  
Deutsche Bank AG  
Deutsche Börse Group  
Deutsche Bundesbank  
Deutsche Postbank AG  
Deutsche Telekom AG  
DFS Deutsche Flugsicherung GmbH  
Dresdner Bank AG  
eco e. V. – Verband der Deutschen Internetwirtschaft  
(E-Plus Gruppe) E-Plus Mobilfunk GmbH & Co. KG  
Europäische Zentralbank  
Gesamtverband der Deutschen Versicherungswirtschaft e. V.  
HUK-COBURG  
Mineralölwirtschaftsverband  
RWE Aktiengesellschaft  
RWE Energy Aktiengesellschaft  
SIZ Informatikzentrum der Sparkassenorganisation GmbH  
Telefónica O<sub>2</sub> Germany GmbH & Co. OHG  
Vodafone D2 GmbH

# Notizen





## **Impressum**

### **Herausgeber:**

Bundesministerium des Innern  
Alt-Moabit 101 D, 10559 Berlin  
[www.bmi.bund.de](http://www.bmi.bund.de)

### **Redaktion:**

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

### **Gestaltung und Produktion:**

MEDIA CONSULTA Deutschland GmbH

### **Druck:**

Silber Druck oHG

### **Auflage:**

1.000 Exemplare

### **Stand:**

Dezember 2008