Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

Auswertungsbericht „LÜKEX 11“. IT-Sicherheit in Deutschland

Bevölkerungsschutz

Impressum

Auswertungsbericht „LÜKEX 11“.
IT-Sicherheit in Deutschland
(Kurzfassung)

BBK-Projektgruppe LÜKEX Bund

Provinzialstraße 93, 53127 Bonn

Telefon: +49-(0)22899-550-0
Telefax: +49-(0)22899-550-1620

E-Mail: poststelle@bbk.bund.de
URL: www.bbk.bund.de

Grafische Gestaltung:
Anna Müller, www.designflavour.de, Hennef

Druck:
BBK

Stand: 31.05.2012
Auflage: 1000

Länderübergreifende Krisenmanagementübung

Auswertungsbericht „LÜKEX 11“

IT-Sicherheit in Deutschland

(Kurzfassung)

Projektgruppe LÜKEX Bund

Auswertungsbericht „LÜKEX 11“. IT-Sicherheit in Deutschland (Kurzfassung)

Inhalt

LÜKEX, Länderübergreifende Krisenmanagementübung (Exercise)

Seit 2004 regelmäßig auf der Basis unterschiedlicher Szenarien (z. B. Pandemie) stattfindende strategische Stabsrahmenübung im Bereich des nationalen Krisenmanagements für die Krisen- bzw. Verwaltungsstäbe auf Bundes- und Landesebene

Anmerkung: Es handelt sich um eine länder- und bereichsübergreifende Übung auf politisch-administrativer Ebene im Bereich des nationalen Krisenmanagements. Zielgruppe sind die politischen Entscheidungsträger von Bund und Ländern sowie Betreiber Kritischer Infrastrukturen.

A. Allgemeines

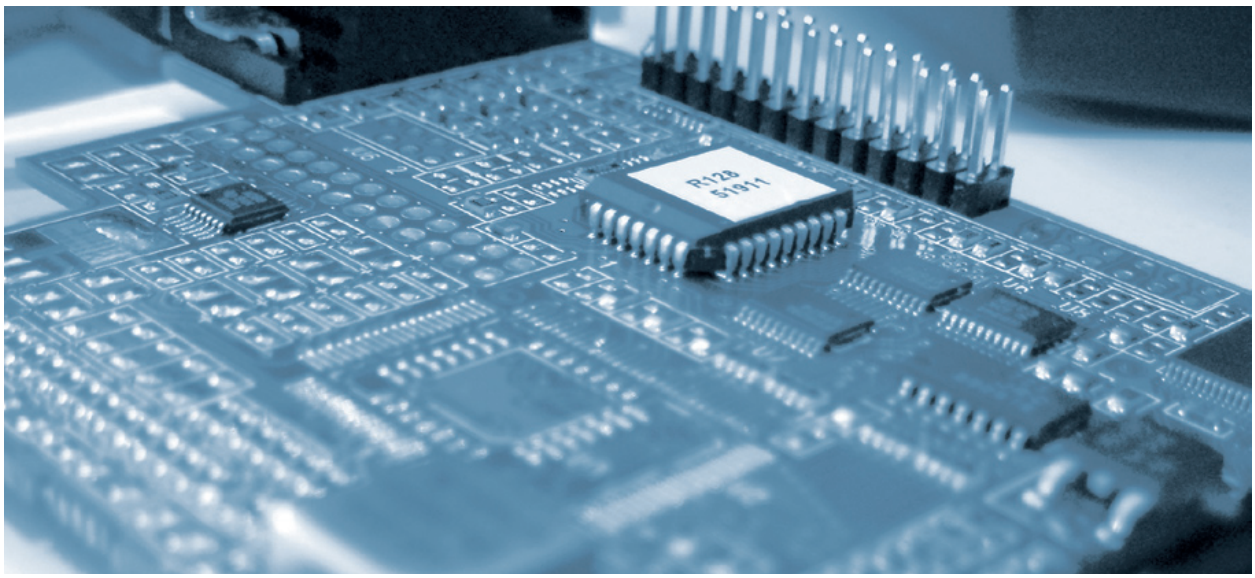


Abbildung 1: Vernetzte Welten

„Der Cyber-Raum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen. In Deutschland nutzen alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die vom Cyber-Raum zur Verfügung gestellten Möglichkeiten. Staat, Kritische Infrastrukturen, Wirtschaft und Bevölkerung in Deutschland sind als Teil einer zunehmend vernetzten Welt auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen.

Fehlerbehaftete IT-Produkte, der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum können zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen Deutschlands führen. Die Verfügbarkeit des Cyber-Raums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten sind zu einer existentiellen Frage des 21. Jahrhunderts geworden.“

BMI: „Cyber-Sicherheitsstrategie für Deutschland“.

A.1. Rechtsgrundlage

Rechtliche Grundlage für die Planung, Vorbereitung, Durchführung und Auswertung der 5. strategischen Krisenmanagement-Übung „LÜKEX 11“ im Rahmen der Übungsserie LÜKEX[1] ist §14 Zivilschutz und Katastrophenhilfegesetz (ZSKG).[2]

Ressort- und länderübergreifende Krisenmanagementübungen

Das „Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes“ (Zivilschutz- und Katastrophenhilfegesetz ZSKG), zuletzt geändert durch Artikel 2 Nr. 1 des Gesetzes vom 29.07.2009 (BGBl. I S. 2350) stellt auch die Aus- und Fortbildungsmaßnahmen des Bundes auf eine moderne Grundlage. Insbesondere ist die erfolgreiche länderübergreifende Krisenmanagement-Übungsserie LÜKEX rechtlich abgesichert. Das Gesetz legt dazu in § 14 fest:

§ 14 Aus- und Fortbildung

Die Aus- und Fortbildungsmaßnahmen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe nach § 4 Abs. 1 Satz 2 Nr. 2 Buchstabe a dienen zugleich den Ländern für die Vorbereitung ihrer Entscheidungsträger, Führungskräfte und sonstigen Fachkräfte auf die Bewältigung von Katastrophen und Unglücksfällen und umfassen insbesondere auch die Planung, Durchführung und Auswertung von ressort- und länderübergreifenden Krisenmanagementübungen. Die Aus- und Fortbildungsmaßnahmen des Bundes bauen auf der Ausbildung der Länder im Bereich des Katastrophenschutzes auf und ergänzen diese.

A.2. Übungsthema

Thema der Übung war die IT-Sicherheit in Deutschland. Das Übungsthema reflektiert die wachsende Bedeutung der Informationstechnik für die öffentliche Sicherheit. Durch eine Vielzahl tatsächlicher IT-Vorfälle und aktuelle Bedrohungsanalysen ist die Vulnerabilität der IT-Infrastrukturen verstärkt in den Fokus gerückt.

[1] Länder Übergreifende Krisenmanagement-Übung/EXercise

[2] Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes / Zivilschutz- und Katastrophenhilfegesetz – ZSKG vom 2. April 2009 (BGBl. I S. 693)

A.3. Eckpunkte der Übung

3.1. Übungsziel

Kernziel der Übung war die Einübung und Erprobung des konzertierten Handelns der Krisen- und Verwaltungsstäbe des Bundes und der Länder auf der politisch-administrativen (strategischen) Entscheidungsebene unter Einbeziehung von privaten Betreibern Kritischer Infrastrukturen. Dabei sollte auch die Wirksamkeit der Strategien zum Schutz der nationalen Informationsinfrastrukturen[3] erstmals in einer gemeinsamen Übung von Bund, Ländern und KRITIS-Unternehmen überprüft werden.

Die Übung „LÜKEX 11“, die eine bundesweite Krise als Folge von Cyber-Attacken zugrunde legte, sollte in erster Linie

- für die Gesamtthematik sensibilisieren,
- zur Vernetzung aller relevanten Akteure beitragen,
- IT-Krisenmanagement und allgemeines strategisches Krisenmanagement in ihrer Gesamtheit kohärent weiterentwickeln und
- den Stand der gesamtstaatlichen und gesamtgesellschaftlichen Vorbereitung im Hinblick auf die neuartige Bedrohung nach Möglichkeit auf ein höheres Niveau heben.

3.2. Übungskonzept

Für die Übung „LÜKEX 11“ wurde der Leitfaden für strategische Krisenmanagement-Übungen[4] zugrunde gelegt. Danach umfasst der in der Regel zweijährige Gesamtübungszyklus die Phasen der

- Planung,
- Vorbereitung,
- Durchführung und
- Auswertung.

Abbildung 2: Der „Leitfaden für strategische Krisenmanagement-Übungen“ stellt Grundsätze für die Anlage strategischer Übungen dar.

[3] Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI); Umsetzungspläne Bund und KRITIS (UP Bund bzw. UP KRITIS), Bundesministerium des Innern, 2007, sowie Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Innern, Februar 2011

[4] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Bonn, 2011, Leitfaden für strategische Krisenmanagement-Übungen

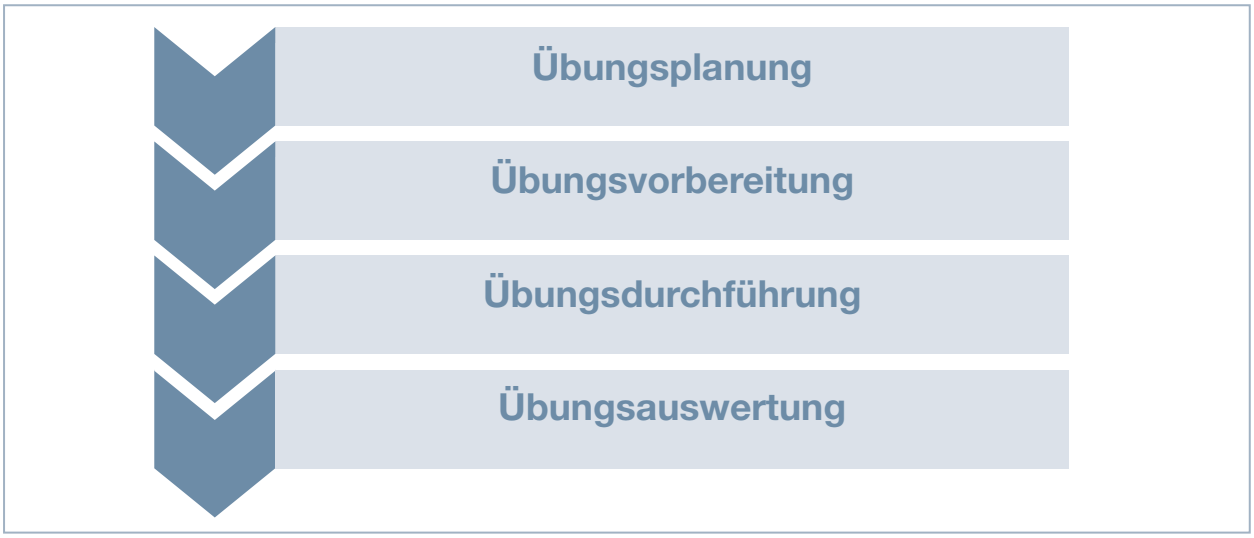


Abbildung 3: „Phasen des Gesamtübungszyklus strategischer Übungen“

„Herzstück“ der Übung ist die Phase der Übungsvorbereitung, in deren Verlauf das Übungsszenario sukzessiv und diskursiv über interdisziplinäre Expertengespräche erarbeitet und mit Hilfe der Expertise der an der Übung Beteiligten realitätsnah gestaltet wird. Das Übungsszenario von „LÜKEX 11“ wurde so über zahlreiche Arbeitstagungen, „Themenworkshops“ zu ausgewählten Fachthemen und szenariobezogene Spezialworkshops im Verlauf von 18 Monaten intensiv vorbereitet. Die Vorbereitungsphase gab den Übungsbeteiligten bereits Gelegenheit, ihre Krisenmanagementstrukturen und -verfahren zu überprüfen und Schwachstellen schon vor der Übungsdurchführung zu beseitigen.

Höhepunkt der Übung war die Phase der Übungsdurchführung am 30. November und 1. Dezember 2011. Die Krisen- und Verwaltungsstäbe des Bundes und der Länder sowie zahlreiche Behörden, Hilfsorganisationen und Unternehmen beteiligten sich überwiegend hochrangig an der Bewältigung der fiktiven nationalen Krise.

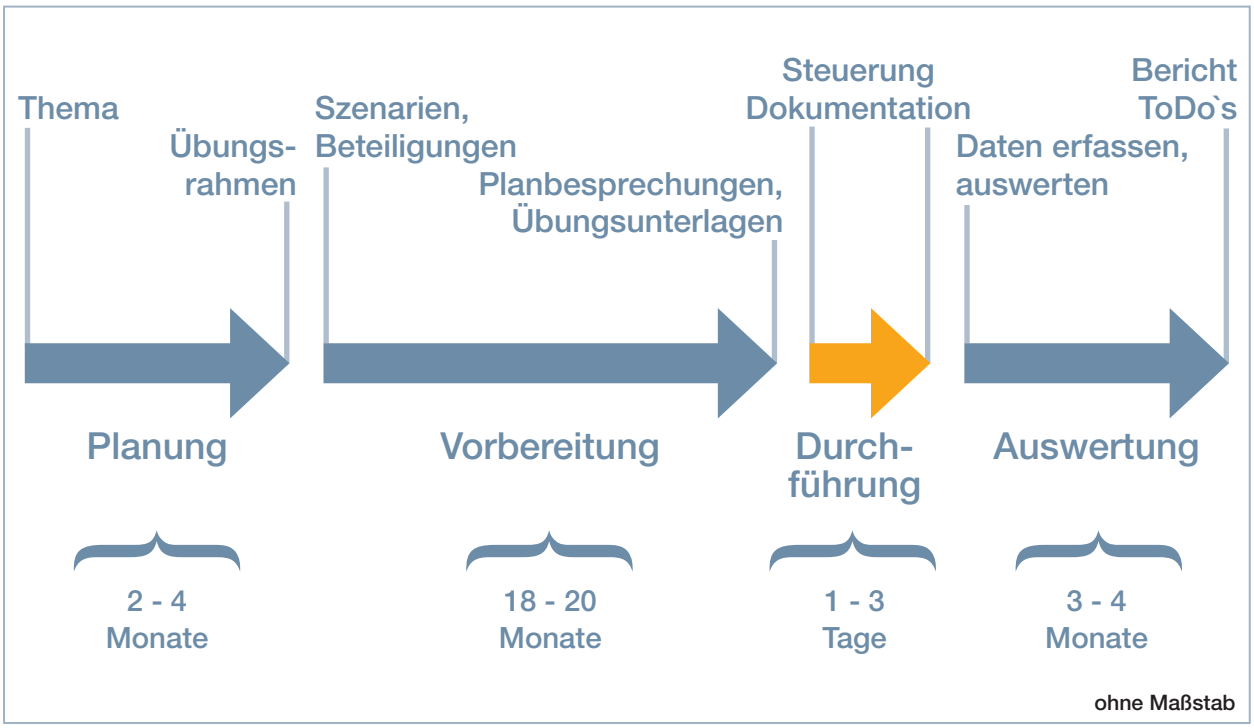


Abbildung 4: Der Übungszyklus von „LÜKEX 11“ umfasste vom Beginn der Planungsphase bis zum Ende der Auswertung einen Zeitraum von ca. 24 Monaten

3.3. Übungsszenario

Das Szenario der Übung „LÜKEX 11“ ging von zielgerichteten IT-Angriffen aus, die Schwachstellen in den IT-Systemen und Regierungsnetzen ausnutzten.
Im Rahmen der Szenario-Gestaltung waren eine einheitlich im Verborgenen agierende Tätergruppe („Hacktivisten“) und eine gemeinsame multifunktionale Schadsoftware („SPYtool“) eingeführt worden, um den notwendigen Gesamtzusammenhang zu stiften und die vielfältigen IT-Störungen und unterschiedlichen Auswirkungen plausibel zu machen.

Besonders betroffen waren die folgenden ausgewählten Sektoren der Kritischen Infrastruktur (KRITIS)[5]:

- Staat und Verwaltung
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Finanz- und Versicherungswesen.

Kritische Infrastrukturen (KRITIS)

Unter Kritischen Infrastrukturen versteht man Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Anmerkung: vgl. BMI, „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 17. Juni 2009.

Quelle: BBK, Schriftenreihe „Praxis im Bevölkerungsschutz, Band 8, „Ausgewählte zentrale Begriffe des Bevölkerungsschutzes“, Bonn, 10/2011

3.4. Übungsbeteiligung

Im Einzelnen waren an der Übung beteiligt:

- 10 Bundesressorts (davon fünf mit eigenen Szenario-Anteilen),
- 20 Bundesbehörden,
- das (im Frühjahr 2011 neu eingerichtete) Nationale Cyber-Abwehrzentrum (Cyber-AZ),
- fünf Länder mit intensiver Beteiligung (sog. „Intensiv-Übungsländer“ Hamburg/HH, Niedersachsen/NI, Hessen/HE, Sachsen/SN und Thüringen/TH) und
- sieben Länder mit geringerer Beteiligung (sog. „Übende Länder” Brandenburg/BB, Berlin/BE, Baden-Württemberg/BW, Bayern/BY, Mecklenburg-Vorpommern/MV, Rheinland-Pfalz/RP, Sachsen-Anhalt/ST),
- 45 KRITIS-Unternehmen und Verbände,
- die Europäische Zentralbank (EZB) und
- EUROCONTROL.

[5] Bundesministerium des Innern (2009), Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Anlage 2 (www.bmi.bund.de)

In der Phase der Übungsdurchführung waren insgesamt ca. 3.000 Personen eingebunden, entweder als Übende in den Krisenstäben oder als Steuernde in der Übungssteuerungsorganisation. Wie in früheren Übungen hat die Schutzkommission beim Bundesministerium des Inneren (SK) den Übungszyklus „LÜKEX 11“ fachlich begleitet.

3.5. Reale Medienarbeit und Besucherprogramm

Bereits im Vorfeld der Übung war das reale Medieninteresse an der Übung „LÜKEX 11“ erheblich. Im Hinblick darauf hatten Bund und Länder für die Phase der Übungsdurchführung Leitlinien zur realen Medienarbeit (einschließlich Fragen- und Antwortenkatalog/FAQ) abgestimmt.

Zusätzlich veranstaltete das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesamt für Verfassungsschutz (BfV), an den Übungstagen ein umfangreiches Besucherprogramm, das unter anderem ein „Begleitforum“ für Übungsbesucher aus dem In- und Ausland umfasste.

Abbildung 5: Das bei “LÜKEX 11” erstmalig durchgeführte Begleitforum für hochrangige Besucher aus dem In- und Ausland fand große Beachtung.

A.4. Übungsauswertung

Inhaltlich orientierte sich die Übungsauswertung an den vorher festgelegten Übungszielen. Ziele und Methoden wurden im Verlauf der Übungsvorbereitung zwischen den Übungsbeteiligten abgestimmt und in einem Rahmenkonzept zusammengefasst.

Dem Konzept lag ein qualitativer Gesamtansatz („Methodenmix“) zugrunde.

Im Rahmen der Nachbereitung der Übung „LÜKEX 11“ wurde eine Vielzahl von Einzelerkenntnissen, Beobachtungen und Schlussfolgerungen aus Fragebögen, Berichten, Veranstaltungen und Einzelgesprächen zusammengetragen.

B. Inhaltliche Feststellungen

B.1. Vorbemerkung

Aufgabe der Krisen- und Verwaltungsstäbe auf Bundes- und Landesebene war die länder- und bereichsübergreifende Abstimmung des Regierungs- und Verwaltungshandelns.

Eine besondere Herausforderung in der Übung „LÜKEX 11“ repräsentierten die noch im Aufbau befindlichen Meldestrukturen im IT-Bereich und das weitgehend noch unerprobte Zusammenwirken zwischen den Strukturen des allgemeinen Krisenmanagements und den teilweise erst im Aufbau begriffenen IT-Krisenmanagementstrukturen. Dies betraf besonders auch die enge Zusammenarbeit mit den jeweiligen IT-Dienstleistern und die Einbeziehung von IT-abhängigen KRITIS-Betreibern in die Entscheidungsfindung.

Verfügbarkeit, Vertraulichkeit und Integrität von Informations- und Kommunikationstechnik sind aufgrund der zunehmenden Durchdringung aller Lebensbereiche mit IKT auch für KRITIS-Betreiber von existenzieller Bedeutung. Ziel der Übung „LÜKEX“ war es auch, die Auswirkungen von massiven IT-Störungen in den vier vorgenannten exemplarisch näher betrachteten Sektoren der Kritischen Infrastruktur festzustellen und geeignete übergreifende Abwehrstrategien zu erproben.

B.2. Übergreifende Feststellungen

2.1. Gesamtstaatliches Krisenmanagement

Insgesamt hat die Übung erneut die im Grundsatz gute und vertrauensvolle Zusammenarbeit von Bund, Ländern und Unternehmen der Kritischen Infrastruktur unter Beweis gestellt. Eine weitergehende Netzwerkbildung zwischen öffentlicher Verwaltung und privaten KRITIS-Betreibern auf allen Ebenen wurde gleichwohl als dringlich angesehen und angemahnt.

Bewährt hat sich die Einbindung von „Fachberatern“ der KRITIS-Unternehmen in die Krisenstäbe auf unterschiedlichen Ebenen.

In der Nachbereitung wurde jedoch festgestellt, dass das Übungsziel des länderübergreifenden Zusammenwirkens nicht überall in vollem Umfang erreicht wurde.

Die Übung machte die existentielle Bedeutung einzelner herausragender IKT-Strukturen, Prozesse und Fachverfahren deutlich. Im Sinne einer strategischen Ausfallvorsorge und gesamtgesellschaftlichen Daseinsvorsorge war zu prüfen, ob die derzeitige Ausfallvorsorge bereits ausreichend ist, um schnelle und wirksame Reaktionen zu ermöglichen. Gegebenenfalls wäre ein Maßnahmenplan für den Fall eines auch längerfristigen Ausfalls der Regelstrukturen zu entwickeln.

In Bezug auf die Abstimmungsprozesse der Länder untereinander besteht noch Optimierungsbedarf. Der gegenseitige Austausch über ergriffene Maßnahmen hätte intensiver sein können.

Darüber hinaus wurde festgestellt:

- Bund, Länder und KRITIS-Unternehmen sollten, sofern noch nicht erfolgt, solche IKT-Strukturen, Prozesse und Fachverfahren identifizieren, die für die Daseinsvorsorge und öffentliche Sicherheit existenziell sind.

- Künftig sollten sich die Länder noch intensiver über getroffene Maßnahmen austauschen, um gegebenenfalls Erkenntnisse in das eigene Handeln einbeziehen zu können.

- Alle Krisenstäbe sollten, soweit noch nicht umgesetzt, IT-Fachbehörden, IT-Dienstleister bzw. IT-Fachberater – temporär auch KRITIS-Unternehmen – möglichst bis zur Leitungsebene (z. B. CIO zur Politikberatung) in die Arbeit des Krisenstabes einbeziehen.

2.2. Krisenmanagement auf Bundesebene

Die im Bundesbereich bestehenden Krisenmanagementstrukturen – sowohl im Bereich des allgemeinen Krisenmanagements wie im IT-Krisenmanagement – haben sich durchweg bewährt. Nach der zugrunde liegenden Konzeption wird der Krisenstab des BMI dann aufgerufen, wenn schwere IT-Sicherheitsvorfälle bzw. eine nationale IT-Krise, insbesondere auch im Bereich von KRITIS-Betreibern, vorliegen.

Zielführend war die vorausschauende und professionelle Krisenführung durch den Krisenstab auf Bundesebene. Den Krisenstab leitete fast durchgängig der Sicherheitsstaatssekretär im BMI; Vertreter war der Leiter der Abteilung „Krisenmanagement und Bevölkerungsschutz“. Die Geschäftsbereichsbehörden des BMI (BSI, BVA, BBK, THW, BKA, BfV und BPOL) waren durch die jeweiligen Haus-

Abbildung 6: Die Krisenführung durch den Krisenstab auf Bundesebene (im Bild) war vorausschauend und professionell.

leitungen vertreten. Im Rahmen der Zuständigkeit des BMI für den Einsatz und die Sicherheit der Informationstechnik in der Bundesverwaltung waren die Beauftragte der Bundesregierung für die Informationstechnik (BfIT) und der IT-Direktor strukturell in die Krisenstabsarbeit eingebunden. Die Zusammenarbeit der Bundesbehörden kann als gut und vertrauensvoll bezeichnet werden.

IT-Aspekte flossen angemessen in die Lagebeurteilung ein, wobei sich die Diskussion in den Stäben als Reaktion auf IT-Störungen und Ausfälle oft auf die technischen Aspekte konzentrierte. Überlegungen zu möglichen Auswirkungen auf Bevölkerung und Verwaltung sollten stärkeres Gewicht erhalten.

Das IT-Krisenmanagement sollte ressortübergreifend institutionalisiert und in das allgemeine Krisenmanagement integriert werden.

Für die IKT-Strukturen und Fachverfahren, die für die Daseinsvorsorge und die Sicherheitsgewährleistung existenziell sind, ist eine redundante, autarke (im Sinne von unabhängig von öffentlichen Netzen) IT-Infrastruktur notwendig.

2.3. Krisenmanagement auf Länderebene

Die beteiligten Intensiv-Übungsländer (HH, NI, HE, SN, TH) haben den Übungszyklus „LÜKEX 11“ ganz überwiegend als erfolgreich und insbesondere vor dem Hintergrund der aktuellen IT-Sicherheitsbedrohung als notwendig und zielführend bewertet.

Eine Zusammenarbeit von zuständigen Verantwortungsträgern im allgemeinen Krisenmanagement mit IT-Sicherheitsexperten des jeweiligen Landes und privaten KRITIS-Betreibern hat in den Ländern überwiegend zum ersten Mal in dieser Form im Rahmen der Übung stattgefunden. Diese Art der Vernetzung wurde als außerordentlich nützlich und hilfreich beurteilt und als wesentlicher Mehrwert der Übung bewertet.

Bereits in der Übungsvorbereitung sind Schnittstellenprobleme zwischen dem allgemeinen Krisenmanagement und dem IT-Krisenmanagement deutlich geworden, das zum Teil außerhalb der Innenressorts oder auch bei privaten Betreibern angesiedelt ist. Daher wurde bereits die Vorbereitungsphase genutzt, diese Probleme anzugehen und entsprechende Strukturen zu etablieren und während der Übung zu erproben. Die Übung hat gezeigt, dass Strukturen und Prozesse zur IT-Krisenreaktion in den Ländern (z. B. Informationsaustausch und „VerwaltungsCERT-Verbund[6]“) unter gleichzeitiger Stärkung der Rolle des nationalen IT-Krisenreaktionszentrums im BSI kontinuierlich verbessert werden müssen. Hierbei muss eine interdisziplinäre Fachexpertise zur Cybersicherheit in geeigneter Form eingebracht werden.

In allen Ländern war im Verlauf der Übungsdurchführung eine kompetente und politisch sensible Führung der Krisenstäbe festzustellen, wobei in der Regel die zuständige Staatssekretärin / der Staatssekretär / der Staatsrat in angemessenen Zeitanteilen präsent war.

[6] CERT= Computer Emergency Response Team, VerwaltungsCERT-Verbund“ = aktuell im IT-Planungsrat diskutierte Bund-Länder-Zusammenarbeit auf operativer CERT-Ebene.

Abbildung 7 und 8: In allen Ländern war im Verlauf der Übungsdurchführung eine kompetente und politisch sensible Führung der Krisenstäbe festzustellen – auf den Bildern: Krisenstab Thüringen (oben), Polizeidirektor Schneider und Thüringens Innenminister Jörg Geibert (unten)

Ständige Krisenmanagementstrukturen (z.B. ständige Stabsstellen in allen Ressorts) haben sich erneut bewährt. Kabinettsbeschlüsse für den Aufbau und die Anpassung von Krisenmanagementstrukturen sind hier förderlich. In einigen Ländern sind verbindliche Regelungen für die Einrichtung von Krisenstäben auf der Basis des IMK-Beschlusses[7] zur Gliederung von Verwaltungsstäben mustergültig umgesetzt. In Einzelfällen ist dabei auch die Integration des IT-Krisenmanagements in das allgemeine Krisenmanagement verbindlich geregelt. Das Innenressort ist aufgrund seiner Einsatzerfahrung in den Bereichen Polizei und Katastrophenschutz und der logistischen Voraussetzungen (Lagezentren, eingespielte Meldewege, Technik etc.) grundsätzlich befähigt, auch bei Krisenlagen mit anderen thematischen Schwerpunkten die Koordination bei systematischer Fachberatung und Hinzuziehung von Experten zu übernehmen. Die Integration des IT-Krisenmanagements in die allgemeinen Krisenmanagementstrukturen ist in allen Ländern im Rahmen der Übungsdurchführung in weiten Teilen gelungen. In mehreren Behörden wurden Notfallplanungen angestoßen bzw. modifiziert.

[7] Bundeseinheitliche Hinweise zur Bildung von Stäben der administrativ-organisatorischen Komponente (Verwaltungsstäbe-VwS), Beschluss der Ständigen Konferenz der Innenminister und -senatoren (IMK) vom 21.11.2003

Darüber hinaus wurden regionale KRITIS-Betreiber – z. B. Banken, Sparkassen, Verkehrsträger – in unterschiedlicher Intensität in die Entscheidungsfindung erfolgreich mit einbezogen. Die diesbezüglich bestehenden und im Laufe der Übungsvorbereitung geschaffenen Netzwerke haben eine enge Abstimmung und Kooperation zwischen den jeweiligen Landeskrisenstäben und den Krisenstäben im KRITIS-Bereich ermöglicht, was sich auch vor dem Hintergrund möglicher Reallagen positiv auswirken dürfte.

Die Übenden Länder BB, BE, BW, BY, MV, RP und ST beteiligten sich in unterschiedlicher Intensität an der Übung. Zum Teil wurden die Krisenstäbe auf Landesebene einberufen und die Auswirkungen der IT-Vorfälle in den Intensiv-Übungsländern auf die landeseigenen Strukturen reflektiert.

Ein Novum bildete die gemeinsame Leitungsstruktur der Länder Berlin und Brandenburg, die auf diese Weise Synergieeffekte erzielen konnten.

Es ist durchweg gelungen, die Verantwortlichen für die IT-Abhängigkeit der Verwaltung insbesondere bei kritischen Geschäftsprozessen zu sensibilisieren.

Im Verlauf der Übung wurde festgestellt, dass die Faktoren

- Institutionalisierung des IT-Krisenmanagements mit aufwachsenden Strukturen,
- Integration des IT-Krisenmanagements in das allgemeine Krisenmanagement und
- „Transferleistungsfähigkeit“ (z. B. Fähigkeit zur allgemeinverständlichen Darstellung von fachlichen Problemlagen) der handelnden Akteure

eine wesentliche Grundlage für eine erfolgreiche Krisenbewältigung bei einer Krise mit IT-Bezug bilden.

Weitere wesentliche Erkenntnisse:

- Stabsstrukturen für das strategische Krisenmanagement sollten verbindlich festgelegt und per Kabinettsbeschluss erlassen werden. Die Ressourcen und Erfahrungen des jeweiligen Innenressorts sollten dabei – auch bei fachlicher Federführung eines anderen Ressorts – grundsätzlich genutzt werden.
- Das in der Regel vorhandene IT-Notfallmanagement der jeweiligen IT-Dienstleister sollte strukturell angepasst und enger an die politisch-administrative Entscheidungsebene angebunden werden.
- Die bereichsübergreifende Zusammenarbeit des Krisenmanagements bei IT-Krisen unter Einbindung der KRITIS-Sektoren sollte weiter optimiert und im Rahmen von Übungen vertieft und in die Praxis umgesetzt werden.
- Bewährte Strukturen und Prozesse zur IT-Krisenreaktion (z. B. Informationsaustausch und „VerwaltungsCERT-Verbund“) sollten sukzessiv bundesweit in die Praxis umgesetzt werden. Die Kapazitäten des nationalen IT-Krisenreaktionszentrums sollten hierbei genutzt und die Rolle des BSI gestärkt werden.

2.4. Zivil-Militärische Zusammenarbeit (ZMZ)

Die Übung war geeignet, Organisation und Verfahren der ZMZ auf strategischer Ebene zu beüben. Die vier Wehrbereichskommandos (WBK) und das Streitkräfteunterstützungskommando (SKUKdo) beteiligten sich an der Übung. Die Beratung der Krisen- und Verwaltungsstäbe durch die Landeskommandos erfolgte auf der Grundlage etablierter Verfahren durch Verbindungspersonen, wobei die Möglichkeiten und Grenzen der Amtshilfe durch die Bundeswehr berücksichtigt wurden. Die bewährte Zusammenarbeit des Bundes und der Länder im Bereich der Zivil-Militärischen Zusammenarbeit (ZMZ) sollte fortgeführt und im Rahmen von strategischen Krisenmanagement-Übungen – auch vor dem Hintergrund des Strukturwandels in der Bundeswehr – am Beispiel neuer Bedrohungsszenarien regelmäßig getestet und geübt werden.

2.5. Informationsmanagement, Lagebeurteilung und Entscheidungsfindung

Die Übung hat gezeigt, dass die informationellen Zusammenarbeitsstrukturen in der IT-Sicherheit unter Berücksichtigung der Übungserkenntnisse weiter optimiert werden müssen. Insbesondere muss ein geregelter Informationsaustausch zwischen Bund, Ländern und KRITIS-Bereichen institutionalisiert und durch die zuständigen Gremien gebilligt werden. Grundsätzlich bewährt haben sich sowohl die Zusammenarbeit des BSI (IT-Lagezentrum) mit dem UP KRITIS als auch der darüber eingerichtete Meldeweg über die Struktur der Single Points of Contact (SPOC). Als erforderlich angesehen werden ein aktives IT-Krisenmanagement und eine Vernetzung über SPOCs mit regionalen KRITIS-Betreibern.

Zu prüfen ist, wie ein formalisierter Informationsaustausch zwischen den SPOCs der KRITIS-Bereiche und der Bundesebene (BBK / GMLZ und BSI / IT-Lagezentrum) stattfinden kann.

Bei der Lagebeurteilung und Entscheidungsfindung durch die Krisenstäbe erschien die prognostische Komponente in vielen Fällen noch zu wenig ausgeprägt. Gleichwohl ist es größtenteils gelungen, gegen Ende der Übung „vor die Lage“ zu kommen.

Der „Umsetzungsplan KRITIS“

Ein wichtiger Baustein zur Umsetzung der Ziele des Nationalen Plans zum Schutz der Informationsinfrastrukturen ist der Schutz der Informationstechnik bei so genannten Kritischen Infrastrukturen.

Wichtige Infrastrukturen, zum Beispiel im Bereich Finanzen, Energie und Versorgung, sind zunehmend von IT abhängig und untereinander vernetzt. In Deutschland befinden sich etwa vier Fünftel der so genannten kritischen Infrastrukturen in privatwirtschaftlicher Verantwortung.

Das Bundesinnenministerium hat deshalb den „Umsetzungsplan KRITIS“ erarbeitet - gemeinsam mit etwa 30 großen deutschen Infrastruktur-Unternehmen und deren Interessenverbänden, die alle in hohem Maß auf IT-Systeme angewiesen sind. Die beteiligten Organisationen verpflichten sich auf freiwilliger Basis, ein Mindestniveau der IT-Sicherheit einzuhalten. Der Umsetzungsplan KRITIS ist damit ein Modell dafür, wie staatliche Stellen auf diesem Gebiet zukünftig mit der Wirtschaft effizient zusammen arbeiten können...

Quelle: BMI, Website

Die zwischen Bund und Ländern durchgeführten Telefonschaltkonferenzen haben sich erneut als probates Mittel erwiesen, um schnelle Abstimmungen und Entscheidungen zwischen Bund und Ländern herbeizuführen.

Zusätzlicher Handlungsbedarf wird wie folgt gesehen:

- Die Möglichkeit, in der Zukunft in den Krisenstäben eigene Prognosezellen und geeignete Simulationssoftware einzusetzen, sollte geprüft werden.

- Bund, Länder, Kommunen und KRITIS-Betreiber sollten bereichsübergreifende Übungen zur IKT-Notfallplanung durchführen.

2.6. Spezielle Feststellungen zum IT-Krisenmanagement

Erstmalig wurde in der Übung „LÜKEX 11“ die Umsetzung der Beschlusslage des IT-Rats zum „IT-Krisenmanagement bei IT-Krisen mit Auswirkungen auf die Bundesverwaltung“[8] geübt. Der Beschluss bildet ein wesentliches Element für das Zusammenwirken der Bundesressorts im gesamtgesellschaftlichen Krisenmanagement.

Erstmals erprobt werden konnten überdies die IT-Zusammenarbeitsstrukturen (Meldewege, Meldeverfahren etc.), die mit den Ländern im Verlauf der Übungsvorbereitung abgesprochen worden waren. Die Zusammenarbeit mit dem BSI wurde insoweit von Länderseite positiv bewertet. Im Sinne der Nachhaltigkeit sollten die Länder im Nachgang zur Übung ihre Kompetenzen im IT-Krisenmanagement weiter auf- und ausbauen und sich über definierte Kontaktstellen mit dem BSI zu wesentlichen IT-Vorfällen austauschen. Die Einrichtung und Intensivierung des „VerwaltungsCERT-Verbunds“ sollte im Rahmen der Bund-Länder-Gremienarbeit weiterverfolgt werden.

Die Übung hat eine Vielzahl von Erkenntnissen zu einer weiteren Optimierung der Abläufe im nationalen IT-Krisenreaktionszentrum (IT-KRZ) des BSI und der Zusammenarbeit im bereichsübergreifenden IT-Krisenmanagement auch mit dem BBK (GMLZ) geliefert. Die vorbereiteten Strukturen und Prozesse zur IT-Krisenreaktion der Bundesverwaltung innerhalb des BSI haben sich grundsätzlich bewährt.

Das BSI konnte in seiner Rolle als Kompetenzzentrum und Koordinierungsinstanz im Bereich IT-Sicherheit wichtige Impulse und Beiträge zur Problemlösung geben. Das BSI hat die Bedarfsträger regelmäßig mit einem aktualisierten IT-Lagebild sowie mit Warn- und Alarmierungsmeldungen bei neuen Erkenntnissen zu den der Lage zugrunde liegenden Bedrohungen versorgt.

In den Ländern sollten – soweit noch nicht eingerichtet – für den IT-Bereich feste Informations- und Meldeverfahren und IT-Sicherheitsstrukturen (z. B. Landes-CERTs) eingerichtet werden, die den länderübergreifenden Informationsaustausch wie auch den Informationsaustausch mit dem Bund gewährleisten, z. B. durch einen „VerwaltungsCERT-Verbund“. Hierbei sind die zuständigen Bund-Länder-Gremien einzubeziehen.

[8] Beschluss IT-Rat zum IT-Krisenmanagement bei IT-Krisen mit Auswirkungen auf die Bundesverwaltung vom 31.03.2011

Abbildung 9: Das IT-Krisenreaktionszentrum während „LÜKEX 11“

2.7. Nationales Cyber-Abwehrzentrum

Das im April 2011 im Rahmen der Nationalen Cyber-Sicherheitsstrategie neu geschaffene Cyber-Abwehrzentrum (Cyber-AZ) wurde erstmalig in eine Übung eingebunden. Dabei trug es im Rahmen seiner Aufgaben als Informationsdrehscheibe zum Austausch von Lagebeiträgen zwischen den beteiligten Behörden und deren Anreicherung durch gemeinsame Bewertungen bei. Folgende Empfehlungen wurden ausgesprochen:

- Die Zusammenarbeit der Behörden im Cyber-AZ als Informationsdrehscheibe sollte ausgebaut werden.
- Die Möglichkeit einer gemeinsamen strategischen Lagebewertung im Cyber-AZ sollte geprüft werden.
- Trotz der nicht-operativen Ausrichtung des Cyber-AZ wird die Erprobung der Kommunikationsfähigkeit in Anbindung an das IT-Krisenreaktionszentrum empfohlen

2.8. Internationale Beteiligung

Die Übung war trotz vielfältiger internationaler Verflechtungen der beteiligten KRITIS-Unternehmen (z. B. in den Bereichen Banken, Luftfahrt und IKT) aus grundsätzlichen Erwägungen und entsprechend dem Charakter der LÜKEX-Übungsserie weitgehend auf die nationale Ebene beschränkt worden.

Die internationale, insbesondere die europäische Dimension, sollte bei zukünftigen strategischen Krisenmanagement-Übungen weiterhin berücksichtigt werden.

B.3. Feststellungen im Bereich KRITIS

3.1. KRITIS-Sektor „Informations- und Kommunikationstechnik“ IKT)

Für den KRITIS-Sektor „IKT“ hat die Übung die ausgesprochene Heterogenität der Organisationsstrukturen von IT-Dienstleistern verdeutlicht. An der Übung haben sich IT-Dienstleister mit unterschiedlichster Rechtsform (Behörden, öffentlich-rechtliche Anstalten und private Unternehmen) und Telekommunikationsunternehmen beteiligt.

IKT-Aspekte des Übungsszenarios wurden in der Regel länderfokussiert wahrgenommen und bearbeitet.

Es hat sich gezeigt, dass die enge Einbindung von IT-Dienstleistern und Telekommunikationsunternehmen schnelle und fachkompetente Entscheidungen unterstützt.

3.2. KRITIS-Sektor „Transport und Verkehr“

Für den KRITIS-Sektor „Transport und Verkehr“ hat die Übung verdeutlicht, welche Auswirkungen und weit reichenden Folgen eine Kompromittierung der IT-Technik zum Beispiel auf die Abläufe im Luftverkehr haben kann. Die Auswirkungen waren an allen beteiligten Flughäfen deutlich spürbar.

Der bei der Übung simulierte Ausfall IT-gestützter Leitsysteme im Straßenverkehr (Tunnelüberwachung, Ampelsteuerungssysteme) hat überregionale und bereichsübergreifende Auswirkungen aufgezeigt, die im Realfall einen kurzfristigen länderübergreifenden Informationsaustausch und entsprechende Notfallmaßnahmen (z.B. Versorgung Betroffener) erfordeten.

Abbildung 10 und 11: Die Auswirkungen von IT-Störungen waren besonders deutlich bei den Abläufen im Luftverkehr spürbar – im Bild: Rhein-Main-Flughafen Frankfurt

3.3. KRITIS-Sektor „Finanz- und Versicherungswesen“

Durch die breite Beteiligung im Bankenbereich (Deutsche Bundesbank, Europäische Zentralbank, Deutsche Bank, Commerzbank, Deutsche Post Rentenservice, Sparkassen-Finanzgruppe, Versicherungswirtschaft) und die Vielzahl unterschiedlichster Szenarien, die geübt wurden, konnten Verfahren der Zusammenarbeit robust getestet werden. Die grundsätzlich erfolgreichen Informationsabläufe zwischen dem BSI und den SPOCs könnten durch eine noch bessere Vernetzung optimiert werden. Festgestellt wurde, dass die Lageberichte des GMLZ, die bisher grundsätzlich nur Behörden zugänglich gemacht werden, auch für den Finanz- und Versicherungsbereich wertvolle Informationen enthalten.

Abbildung 12: Der KRITIS-Sektor „Finanz- und Versicherungswesen“ war an „LÜKEX 11“ breit beteiligt – im Bild: der Stab der Sparkasse Mittelthüringen während der Übungsdurchführung.

Es wurde festgestellt, dass es in Krisensituationen für KRITIS-Unternehmen sinnvoll sein kann, über eine Art „Notruf-Telefonbuch“ zu verfügen, das eine Autorisierung der Kommunizierenden und damit den Austausch auch vertraulicher Informationen ermöglicht. Es wird weiter empfohlen:

- Vor dem Hintergrund der Schnelllebigkeit der Informationstechnik sollte die Funktionsfähigkeit der eigenen Organisation regelmäßig, z. B. durch Übungen, überprüft werden.
- Bei Störungen und Ausfall von gleichartigen IT-Systemen (z. B. im Verkehrssektor) sollte ein unverzüglicher, überregionaler Informationsaustausch sichergestellt werden.
- Die Einbeziehung z. B. der Finanzbehörden und Sparkassen in den Verteiler des GMLZ sollte, wenigstens für den Ereignisfall, geprüft werden.

B.4. Feststellungen im Bereich Medien- und Öffentlichkeitsarbeit

4.1. Vorbemerkung

Risiko- und Krisenkommunikation kann als eine Domäne des strategischen Krisenmanagements bezeichnet werden.[9] Von den Übenden Stäben wurde daher zunächst erwartet, dem herausragenden Stellenwert einer professionellen Medienarbeit in Krisensituationen und den Anforderungen an einen gelingenden Dialog mit der Bevölkerung (Krisenkommunikation) zur Krisenbewältigung gerecht zu werden.

[9] Vgl. die praxisnahen Publikationen: Brandenburgisches Institut für Gesellschaft und Sicherheit (Hg.) (2011) Standpunkt zivile Sicherheit. Behördliche Risikokommunikation im Bevölkerungsschutz, Potsdam; Zukunftsforum Öffentliche Sicherheit e.V. (Hg) (2011) Risiko- und Krisenkommunikation, Berlin (Schriften zur Zukunft der Öffentlichen Sicherheit, Ausgabe 1, 3/2011)

Aufgrund der zunehmenden Bedeutung des Social Web bestand die weitergehende Herausforderung für die Krisenstäbe im Rahmen von „LÜKEX 11“ erstmals auch darin, den Umgang mit (Internet-basierten) „Neuen Medien“ (sog. Social Media, Web 2.0) zu üben.

Zur Vorbereitung waren in der Vorbereitungsphase zwei Kurzgutachten zur Frage der Nutzung von Web 2.0 im Rahmen des strategischen Krisenmanagements in Auftrag gegeben worden.[10] Beide Fachgutachten empfehlen aufgrund des Strukturwandels der Öffentlichkeit eine intensive Auseinandersetzung mit der Funktionsweise, den Nutzungsmustern innerhalb der Bevölkerung und den Potentialen für das strategische Krisenmanagement. Im Verlauf der Übungsvorbereitung wurde die Thematik „Web 2.0“ sowohl im Rahmen des Coaching für Pressesprecher (Workshop Medien- und Öffentlichkeitsarbeit) als auch bei der Mediensimulation („LÜKIleck“, „LÜKITweet“ etc.) erstmals in moderatem Umfang berücksichtigt.

4.2. Inhaltliche Feststellungen

Die Übung hat deutlich gemacht, dass die Krisenkommunikation von der Verfügbarkeit und Integrität der Kommunikationsmittel und Kommunikationswege abhängig ist.

Im Verlauf der Übungsvorbereitung, u. a. während des Workshops Medien- und Öffentlichkeitsarbeit, wurde deutlich, dass die Entwicklung der „Neuen Medien“ perspektivisch zusätzlich Fähigkeiten in den Presse- und Medienabteilungen bedingt, um sie reaktionsschnell mit Antworten, Reaktionen und Informationen bedienen, aber auch Inhalte im Netz beobachten, diese bewerten und in das jeweilige Lagebild integrieren zu können.

Alle Krisenstäbe haben die strategische Bedeutung einer abgestimmten Medien- und Öffentlichkeitsarbeit während der Krise als Schwerpunkt erkannt.

Die Abstimmung der Krisenstäbe bezüglich der Pressemitteilungen mit bundesweiter Relevanz ist noch optimierungsfähig.

Positiv hat sich die Zusammenarbeit benachbarter Länder ausgewirkt, da das Sendegebiet der Rundfunkanstalten teilweise mehrere Länder umfasst. Die Übung hat gezeigt, dass die Einrichtung von sog. „Bürgertelefonen“ und die zielgerichtete Auswertung sozialer Medien Einblicke in die Betroffenheit der Bevölkerung erlauben. Im Krisenstab des Bundes wurde intensiv die Frage erörtert, ob mittels der einheitlichen Behördenrufnummer „D 115“ eine abgestimmte Information der Bevölkerung realisiert werden kann.

Zusätzlich wird angeregt:

- Es sollte untersucht werden, in welchem Umfang Online-Medien und soziale Netzwerke durch Behörden im Rahmen der Krisenbewältigung (einschließlich Risiko- und Krisenkommunikation) genutzt werden können und welche Handlungsanweisungen für die Praxis erforderlich sind.

[10] Krämer, N. (2011) Nutzung sozialer Netzwerke in Krisensituationen. Gutachten für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bereich LÜKEX. Mit Unterstützung von J. Klatt, G. Neubaum, A. von der Pütten, Duisburg; Schmidt, J.-H. (2011) Öffentlichkeiten im Social Web. Praktiken, Strukturen und Einsatzmöglichkeiten in Krisenszenarien. Fachgutachten im Rahmen der LÜKEX 11, Hamburg (Hans-Bredow-Institut für Medienforschung)

4.3. Feststellungen zur Mediensimulation

Das Grundinstrumentarium der Mediensimulation bei LÜKEX-Übungen (LÜKEX TV, Printmedien, Hörfunk) hat sich bewährt. LÜKEX TV hat sich zum entscheidenden Mittel zur schnellen und zielgruppenbezogenen Szenariovermittlung in der Übungsdurchführung entwickelt.

Die erstmalig im Rahmen einer LÜKEX-Übung – moderat – um das Element der sozialen Netzwerke erweiterte Mediensimulation wurde von allen Beteiligten positiv aufgenommen und als zeitgemäß bewertet.

Als vorteilhaft hat sich auch erwiesen, dass die Übungsbeteiligten im Rahmen des Workshops „Medien- und Öffentlichkeitsarbeit“ Gelegenheit hatten, sich durch Vorträge namhafter Referenten, praktische Arbeitshinweise und eine Vertiefung der Inhalte in Arbeitsgruppen inhaltlich und praktisch auf das Übungsszenario einzustimmen.

Von den Übenden wurde positiv bewertet, dass die fiktiven Medien, einschließlich der Live-Radiosendungen zentral verfügbar waren.

Das bewährte Grundinstrumentarium der Mediensimulation bei LÜKEX-Übungen (Printmedien, LÜKEX TV) sollte beibehalten und künftig realitätsnah und maßvoll weiterentwickelt werden (z. B. Live-Radio, Live-TV-Spots, Soziale Medien).

Abbildung 13: Das Instrumentarium der virtuellen Mediensimulation hat sich auch in „LÜKEX 11“ bewährt – im Bild: Medienprodukte und Arbeit im „Nationalen Medienzentrum“ in Ahrweiler während der Übungsdurchführung.

4.4. Dialog mit der Bevölkerung

Die Übung hat deutlich gemacht, dass Krisenstäbe in Krisensituationen angemessen auf Bevölkerungshandeln reagieren müssen, es in einer kritischen Lage eines interaktiven Umgangs mit der Bevölkerung bedarf und das Ausbleiben von Reaktionen zu einer Delegitimierung staatlichen Handelns führen kann.

Im Sinne eines interaktiven Vorgehens hat die „Gruppe Bevölkerung“ im Verlauf der Übungsdurchführung ca. 100 Einlagen zu Reaktionen von Bürgern eingespielt.

Es konnte festgestellt werden, dass die Nutzung Internet-basierter sozialer Medien (z. B.: Blogs, Online-Foren) für Bürgeranfragen grundsätzlich geeignet ist, um die Krisenstäbe für die psychosozialen Aspekte des Krisenmanagements zu sensibilisieren.

Darüber hinaus wird empfohlen:

- In den Krisenstäben sollte der unterschiedliche Informationsbedarf der verschiedenen Bevölkerungsgruppen zukünftig stärker berücksichtigt werden

- Anforderungen und Handlungsempfehlungen zu einer angemessenen Risiko- und Krisenkommunikation unter den erweiterten Möglichkeiten des Web 2.0 sollten mit wissenschaftlicher Begleitung erarbeitet werden. Die Ergebnisse sollten durch Übungen erprobt werden, um den angestrebten Dialog mit der Bevölkerung weiter auszubauen.

Krisenkommunikation – wichtiges Instrument des Krisenmanagements

Im Kontext der weltweiten Informations- und Mediengesellschaft ist die Krisenkommunikation durch Medien- und Öffentlichkeitsarbeit (MÖA) ein wichtiges Instrument des strategischen Krisenmanagements. Sie kann Ausprägung und Verlauf von Krisen entscheidend beeinflussen. Dementsprechend wird bei den LÜKEX-Übungen von den übenden Stäben als Übungsziel „eine breit angelegte, abgestimmte aktive Öffentlichkeitsarbeit zur situationsgerechten Information der Bevölkerung und Einsatzkräfte im Rahmen eines vorausschauenden, ressortübergreifenden Krisenmanagements“ sowie durchgängig eine „aktive Informationsarbeit“ gefordert. Zu diesem Zweck wird für die Übungen eine virtuelle Medienlandschaft entwickelt, die sich so realitätsnah wie möglich an der tatsächlichen Medienlandschaft Deutschlands orientiert. Während der Übungsdurchführung wird in der Zentralen Übungssteuerung aus professionellen Medienfachleuten und Journalisten das “Nationale Medienzentrum”, gebildet. Es spielt spezifische, auf die Drehbuchentwicklung abgestimmte Medieneinlagen ein: Agenturmeldungen; Berichte und Kommentare regionaler und überregionaler Zeitungen; Hörfunk-Beiträge; Anfragen von Journalisten und Bürgern. Auf Grund ihrer zunehmenden Bedeutung wurden bei “LÜKEX 11” erstmals auch die neuen “Sozialen Medien” in das virtuelle Medienbild eingespielt.

C. Übungsbezogene Feststellungen

C.1. Vorbemerkung

Generell hat sich das Übungskonzept in der Übung „LÜKEX 11“ wiederum bewährt. Im Verlauf des Übungszyklus konnte die Konzeption strategischer Krisenmanagement-Übungen, wie sie im *Leitfaden für strategische Krisenmanagement-Übungen* beschrieben ist, in mehrfacher Hinsicht erfolgreich weiterentwickelt werden.

Innovationen betrafen insbesondere

- die Erweiterung des Projektmanagements im Bereich der Bund-Länder-Abstimmung durch die Einführung regelmäßiger „Projektgruppenleiter-Treffen“,
- die Szenario-Entwicklung durch Veranstaltung von sektorbezogenen „Spezialworkshops“,
- die Drehbucherstellung durch verschiedene Verfahren der „Szenario-Gestaltung“ (Visualisierung von Drehbuchkomponenten, Drehbuchbausteinen und Einlagen) und
- die Übungsdurchführung durch Veranstaltung eines „Begleitforums“ für Übungsbesucher.

Jedoch hat sich im Verlauf des Übungszyklus Optimierungspotential im Einzelnen ergeben. Wesentliche Aspekte betreffen die verbindlichere Gestaltung der Übungsplanung, die Reduzierung des Aufwandes und die Initiierung einer Begleitforschung im Verlauf der Übungsvorbereitung sowie die gezielte und nachhaltige Umsetzung der Übungserkenntnisse im Nachgang zur Übung.

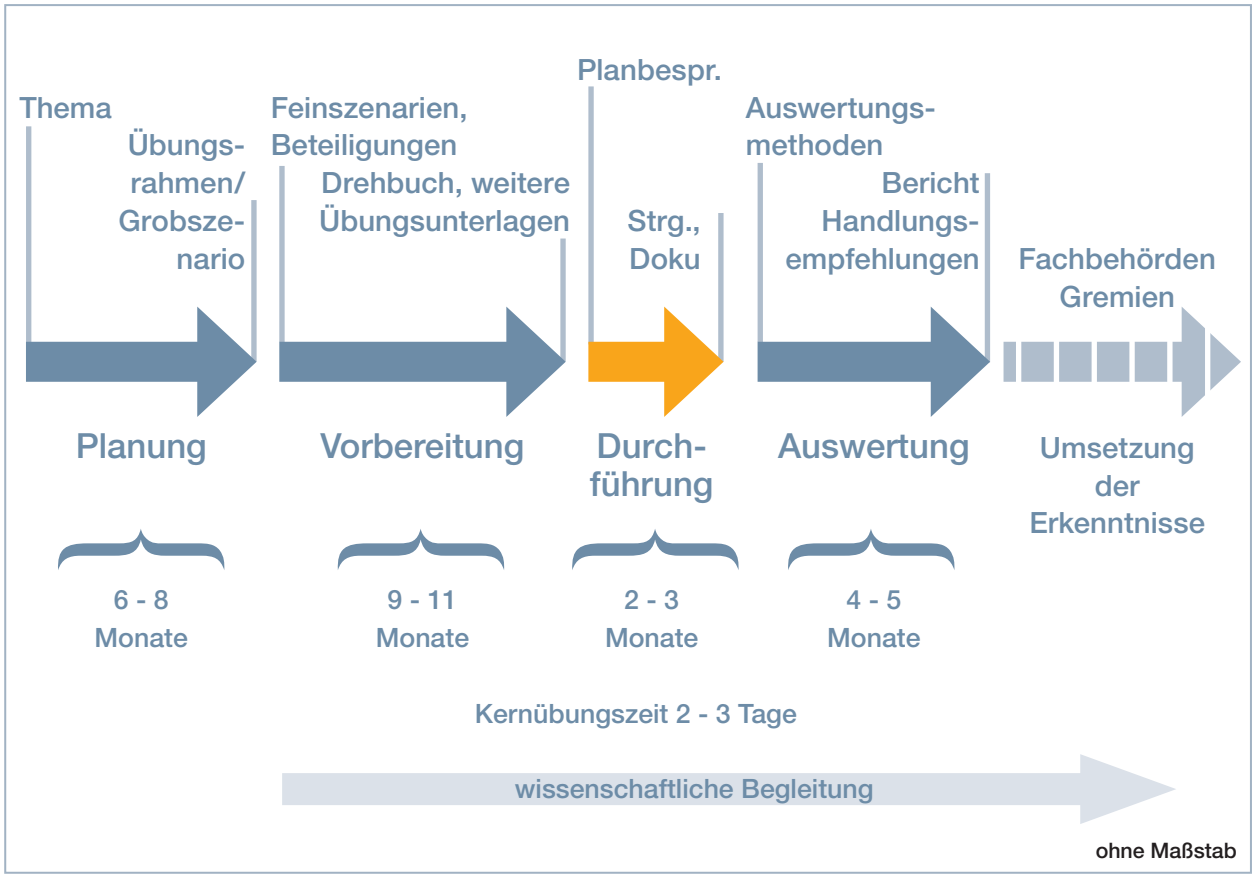


Abbildung 14: Aufgrund der Erfahrungen aus „LÜKEX 11“ weiter entwickelter neuer Gesamtübungszyklus für LÜKEX-Übungen (vgl. Seite 8, Abbildung 4)

C.2. Feststellungen im Einzelnen

2.1. Übungsplanung

Die Übung hat gezeigt, dass der „Übungsrahmen“ als Basisdokument unverzichtbar ist, um alle Beteiligten zielgerichtet einzubinden. Künftig sind bereits in der Planungsphase einheitliche Eckpunkte zum Übungsszenario fest im Übungsrahmen zu verankern, um ein länder- und bereichsübergreifendes Handeln zu generieren.

Aus Gründen der Realitätsnähe des Szenarios sind die betroffenen KRITIS-Bereiche frühzeitig einzubinden und ihre Übungsbeteiligung im Übungsrahmen verbindlich vorzusehen.

Der Lenkungsausschuss LÜKEX ermöglichte eine zielgerichtete Umsetzung des abgestimmten Übungsrahmens. Gleichzeitig gewährleistete er durch die Mitwirkung von Vertretern der betroffenen Bundesressorts und Bund-Länder-Gremien (AK V, IT-Planungsrat) eine angemessene politische Aufsicht über den Gesamtprozess. Weitere Handlungsempfehlungen sind:

- Zukünftig sollten bereits in der Planungsphase wesentliche Eckpunkte des Szenarios und der Übungsbeteiligung mit größerer Verbindlichkeit im Übungsrahmen festgelegt werden.
- Szenarionahe KRITIS-Unternehmen sollten künftig möglichst frühzeitig und verbindlich eingebunden werden, um fachspezifischen Gegebenheiten bereits bei der Entwicklung des Szenarios Rechnung tragen zu können.
- In der Planungsphase sollte sich künftig eine gemeinsame Bund-Länder-Projektstruktur konstituieren, bestehend aus der Projektgruppe LÜKEX des Bundes (PG LÜKEX Bund) und den jeweiligen Projektgruppen der Intensiv-Übungsländer sowie LÜKEX-Beauftragten der betroffenen KRITIS-Unternehmen.

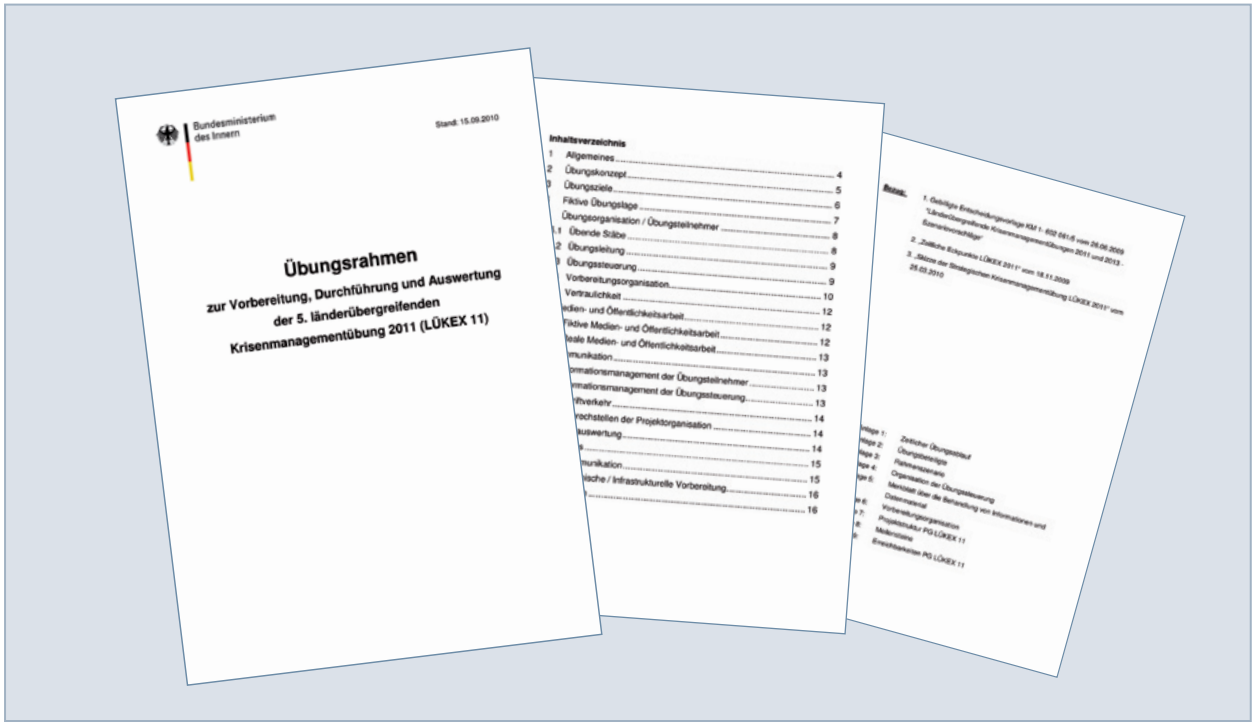
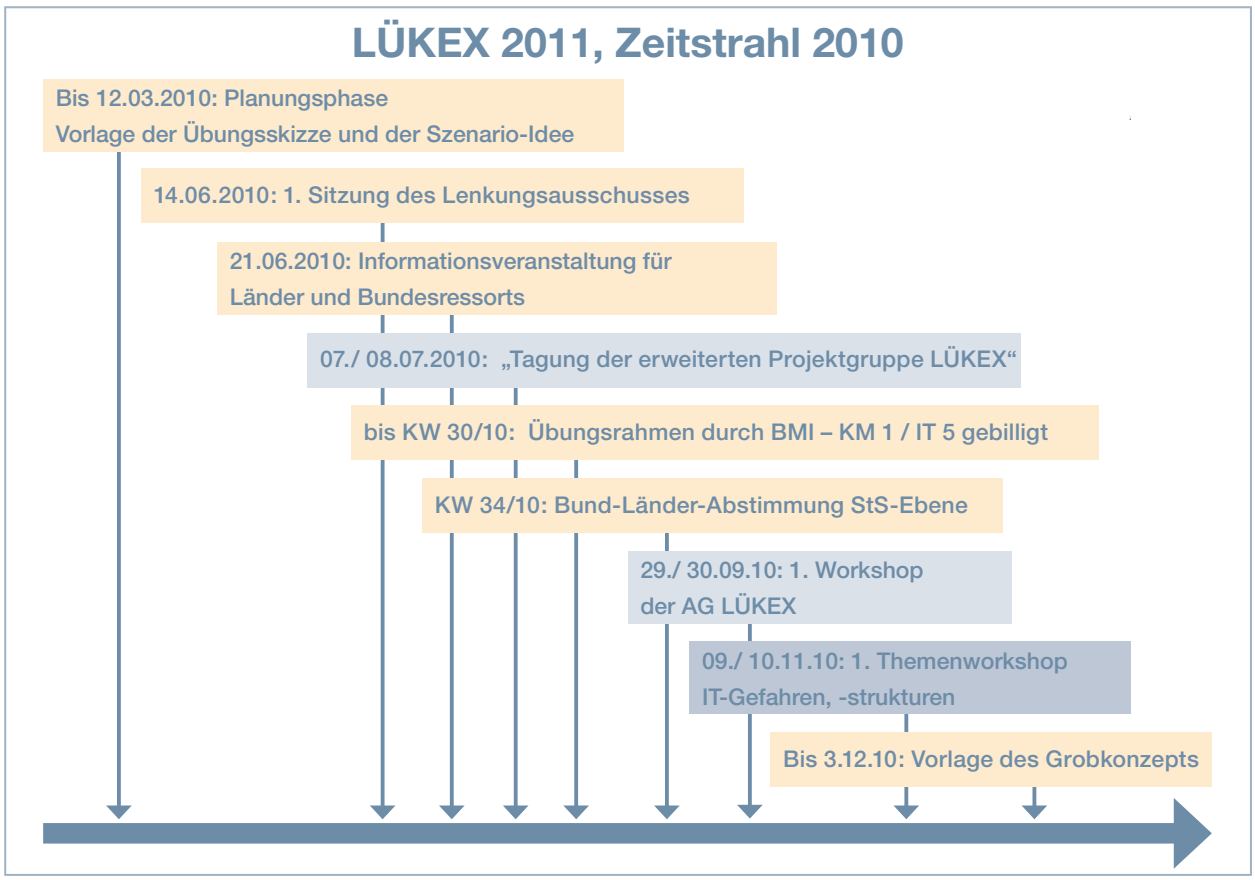
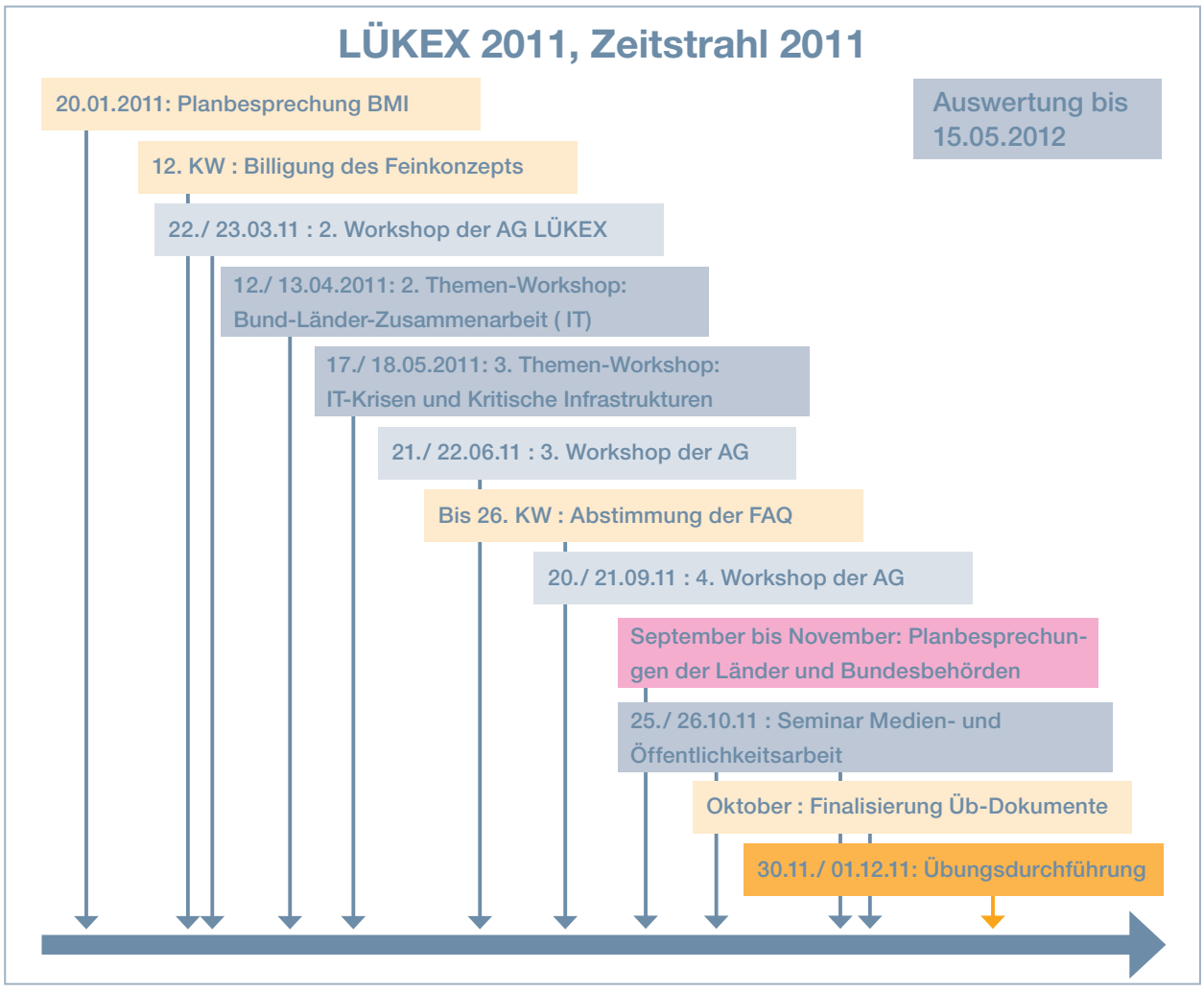


Abbildung 15: Der Übungsrahmen ist das zentrale Grundlagendokument jeder strategischen Übung


LÜKEX 2011, Zeitstrahl 2010
Bis 12.03.2010: Planungsphase
Vorlage der Übungsskizze und der Szenario-Idee
14.06.2010: 1. Sitzung des Lenkungsausschusses
21.06.2010: Informationsveranstaltung für
Länder und Bundesressorts
07./ 08.07.2010: „Tagung der erweiterten Projektgruppe LÜKEX“
bis KW 30/10: Übungsrahmen durch BMI – KM 1 / IT 5 gebilligt
KW 34/10: Bund-Länder-Abstimmung StS-Ebene
29./ 30.09.10: 1. Workshop
der AG LÜKEX
09./ 10.11.10: 1. Themenworkshop
IT-Gefahren, -strukturen
Bis 3.12.10: Vorlage des Grobkonzepts


LÜKEX 2011, Zeitstrahl 2011
20.01.2011: Planbesprechung BMI
Auswertung bis
15.05.2012
12. KW : Billigung des Feinkonzepts
22./ 23.03.11 : 2. Workshop der AG LÜKEX
12./ 13.04.2011: 2. Themen-Workshop:
Bund-Länder-Zusammenarbeit (IT)
17./ 18.05.2011: 3. Themen-Workshop:
IT-Krisen und Kritische Infrastrukturen
21./ 22.06.11 : 3. Workshop der AG
Bis 26. KW : Abstimmung der FAQ
20./ 21.09.11 : 4. Workshop der AG
September bis November: Planbesprechun-
gen der Länder und Bundesbehörden
25./ 26.10.11 : Seminar Medien- und
Öffentlichkeitsarbeit
Oktober : Finalisierung Üb-Dokumente
30.11./ 01.12.11: Übungsdurchführung

2.2. Übungsvorbereitung

Die Übung hat in ihrem Gesamtverlauf gezeigt, dass in der Vorbereitungsphase – dem „Herzstück" der Übung – erhebliche Anstrengungen unternommen werden mussten, um eine enge, länderübergreifende Abstimmung bei der Szenario-Entwicklung und Drehbucharbeit zu erreichen.

Allerdings wurden länderübergreifende Basisszenarien zum Teil bezüglich ihrer Dimensionen und ihrer Auswirkungen nicht ausreichend bzw. unterschiedlich wahrgenommen. Es ist daher erforderlich, bei künftigen Übungen stärker im Wege der Szenario-Gestaltung von Bundesseite einzuwirken, um eine größere übergreifende Bund-Länder Betroffenheit, d. h. die Zusammenführung und Verdichtung verschiedener szenarischer Ansätze, zu erzeugen.

In dieser Hinsicht besonders bewährt haben sich die erstmals im Rahmen der Übungsvorbereitung zur Übung „LÜKEX 11" durchgeführten regelmäßigen Treffen der Projektgruppe auf Bundesebene mit den Projektleitern der Intensiv-Übungsländer. Dadurch konnten Szenario-Entwicklung und Drehbucherstellung zielgerichtet vorangetrieben und Fragen der Übungsorganisation und Unterstützung der Projektarbeit in den Ländergruppen sachgerecht erörtert werden.

Es hat sich als besonders effizient erwiesen, sektorbezogene „Spezialworkshops" zu geschlossenen Themenbereichen (Luftverkehr, Finanzen etc.) durchzuführen, um zielgerichtet ausgewählte Drehbuchkomponenten auf ihre Schlüssigkeit hin zu prüfen und weiterzuentwickeln.

Das in der Übungsdurchführung zugrunde gelegte Szenario sah verschiedene Angriffsvektoren und zahlreiche Einzelereignisse in unterschiedlichen Bereichen vor. Die im übergreifenden Ansatz entwickelten IT-spezifischen Drehbuchbausteine mit erheblicher Betroffenheit von IT- und Telekommunikationsstrukturen, von IT-Strukturen im Banken- und Finanzwesen sowie von Verkehrsträgern im Nah- und Luftverkehr waren in ihrer Gesamtheit realitätsnah konzipiert. Von den Übungsbeteiligten wurde das Gesamtszenario daher überwiegend als geeignet eingeschätzt, um die Übungsziele zu erreichen. Zur Erzeugung einer umfassenden und bundesweiten Betroffenheit sollten künftig nicht eine Vielzahl lokaler Einzelereignisse, sondern wenige, gravierende und länder- und bereichsübergreifende Basisszenarien, die abgestimmte Bund-Länder-Entscheidungen erfordern, entwickelt werden („Tiefe vor Breite"). Handlungsstränge und kritische Geschäftsprozesse können so im Einzelfall von ganz oben bis zur untersten Ebene abgebildet werden.

In organisatorischer Hinsicht hat sich – wie schon bei den vorangegangenen Übungen – die Einrichtung einer bundesweiten „Arbeitsgemeinschaft LÜKEX" (AG LÜKEX), in der Vertreter aller Übungsbeteiligten (Bundesressorts, KRITIS-Betreiber, Länder sowie beteiligte Experten aus Wissenschaft, Hochschulen, Organisationen und Verbänden) repräsentiert sind, im Grundsatz bewährt. Im Hinblick auf die Anzahl der AG LÜKEX-Sitzungen und deren Inhalte besteht Optimierungsbedarf.

Die Einbindung der Übenden Länder in der Phase der Übungsvorbereitung, insbesondere ihre Teilnahme an den vorbereitenden AG-LÜKEX-Sitzungen, hat sich bewährt. Dadurch konnte eine bundesweite Sensibilisierung und ein gesamtstaatlicher Austausch zu den Kernthemen des Szenarios erreicht werden.

Abbildung 18: In der Vorbereitungsphase entstehen im Zuge der lang dauernden Zusammenarbeit aller für das Krisenmanagement Verantwortlichen von Bund, Ländern, gesellschaftlichen Organisationen und Unternehmen der Wirtschaft „Kooperations-Netzwerke", die wesentlich dazu beitragen, über die Übung hinaus die Funktionsfähigkeit des Hilfeleistungssystems in realen Krisensituationen zu gewährleisten.

Besonders bewährt haben sich erneut die – parallel zur Vorbereitung der Übung – durchgeführten „Themenworkshops“ zu folgenden ausgewählten Themen:

- Einführung in IT-Gefahren und Strukturen
- IT-Krisenmanagement bei Bund und Ländern
- IT-Krisen und Kritische Infrastrukturen

Zusätzlich wird empfohlen:

- Die Szenario-Gestaltung sollte nach dem Prinzip „Tiefe vor Breite“ verfahren.
- Die Praxis regelmäßiger Projektgruppenleiter-Treffen sollte fortgeführt werden. Auch sollten vermehrt Arbeitstreffen im kleinen Kreis (z. B. Expertenworkshops mit KRITIS-Unternehmen, Treffen von Drehbuchkoordinatoren) durchgeführt werden.
- Die effiziente Methode der „Themenworkshops“ sollte fortgeführt werden.

2.3. Übungsdurchführung

Im Verlauf der Übungsdurchführung haben sich besonders die vorgeschalteten Planbesprechungen bewährt. Die Planbesprechungen gingen der Übungsdurchführung (30.11.- 01.12.2011) mit fiktivem Datum 25.11.2011 an unterschiedlichen Terminen in den Intensiv-Übungsländern und bei einzelnen Bundesbehörden voraus. Die Planbesprechungen dienten der

- Identifizierung potenzieller eigener Betroffenheit,
- Einübung der Entscheidungsabläufe in den Krisenstäben, die in dieser Form teilweise zum ersten Mal zusammentraten,
- Erörterung und Entscheidung über Präventionsmaßnahmen auf der Grundlage der fiktiven Ausgangslage.

Abbildung 19: Im Verlauf der Übungsdurchführung haben sich besonders die vorgeschalteten Planbesprechungen bewährt – im Bild: Planbesprechung des Krisenstabs Hamburg

Der vorgeschaltete Kommunikationstest in der Übungswoche hat sich als wesentlich herausgestellt, um bei Nutzung unterschiedlicher Kommunikationsmittel (Telefon, Fax, Mail, ÜSA) einen reibungslosen Ablauf der Übung zu gewährleisten. Die Übungssteuerungsanwendung (ÜSA) lief während der Übungsdurchführung stabil. Nach den vorliegenden Rückmeldungen gibt es bei Funktionalität, Ergonomie und Systemadministration der Steuerungssoftware noch Optimierungspotential.

Weiteres Optimierungspotential wird wie folgt gesehen:

- Im Rahmen des Übungszyklus sollten Planbesprechungen künftig integraler Bestandteil der Übungsdurchführung sein.
- Der Kommunikationstest in der Übungswoche sollte in Zukunft zu einer kleinen „Kommunikationsvorübung“ ausgebaut werden, um alle Beteiligten rechtzeitig auf die Übung einzustimmen und einen reibungslosen Start der Übung sicherzustellen.
- ÜSA sollte bedarfsorientiert angepasst werden. Die Funktionalitäten sollten sich auf den für die Übung zwingend notwendigen Funktionsumfang beschränken.

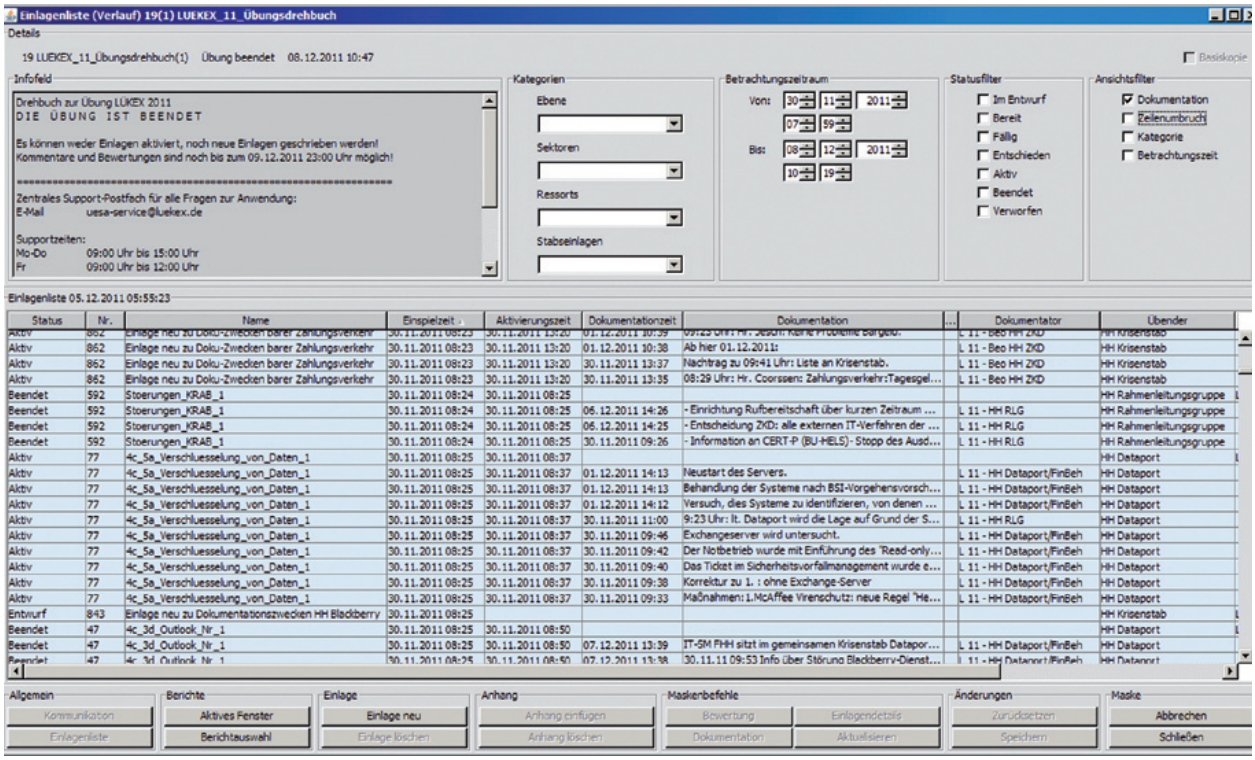


Abbildung 20: Die Übungssteuerungsanwendung (ÜSA) unterstützte Steuerung und Dokumentation des Übungsablaufs – im Bild: Screenshot aus Übungsdrehbuch

2.4. Übungsauswertung

Der qualitative Gesamtansatz zur Übungsauswertung, ausgedrückt in der Nutzung unterschiedlicher Methoden und Erkenntnisquellen (Befragung, Beobachtung, Inhaltsanalyse und konsensuale Verständigung zwischen allen Übungsbeteiligten) für die Zwecke der Übungsauswertung hat sich grundsätzlich bewährt. Das auf dieser Grundlage abgestimmte Rahmenkonzept zur Übungsauswertung sollte praxisnah weiterentwickelt werden, um die Übungsauswertung bei kommenden Übungen zu unterstützen und zu erleichtern.

Es hat sich gezeigt, dass bereits in der Vorbereitungsphase wertvolle Erkenntnisse gewonnen werden können, die strukturiert gesammelt und verstärkt der Übungsauswertung zugeführt werden sollten.

Durch den verstärkten Einsatz von Übungsbeobachtern und Verbindungspersonen während der Übungsdurchführung konnten wertvolle Erkenntnisse über die Arbeit der Übenden Stäbe für die Übungsauswertung gewonnen werden. Zu prüfen ist hier im Besonderen, ob u. U. auch die gegenseitige Übungsbeobachtung der Länder die Erkenntnisbasis verbessern könnte. Im Rahmen der Übungsnachbereitung haben verschiedene Übungsbeteiligte gefordert, die im Verlauf der Übung begonnenen Initiativen unter dem Aspekt der Nachhaltigkeit verstärkt fortzuführen. Erkenntnissen und Befunden aus dem LÜKEX-Prozess sollten daher konsequent im Rahmen der Strategieentwicklung der Behörden und der Bund-Länder-Gremienarbeit Rechnung getragen werden.

Es wird zusätzlich empfohlen:

- Das abgestimmte Rahmenkonzept zur Übungsauswertung und eingeführte Auswertungsbögen sollten praxisnah weiterentwickelt werden, um die Übungsauswertung zu unterstützen und zu erleichtern.
- Es sollte geprüft werden, ob eine prozessbegleitende Übungsauswertung, ggf. unterstützt durch externe wissenschaftliche Evaluation, in Betracht kommt, um die Übungsauswertung in der Vorbereitungsphase zu unterstützen.
- Es sollte geprüft werden, wie der Einsatz von Übungsbeobachtern optimiert werden kann, insbesondere sollte die wechselseitige Übungsbeobachtung zwischen Übungsbeteiligten verstärkt in Erwägung gezogen werden.

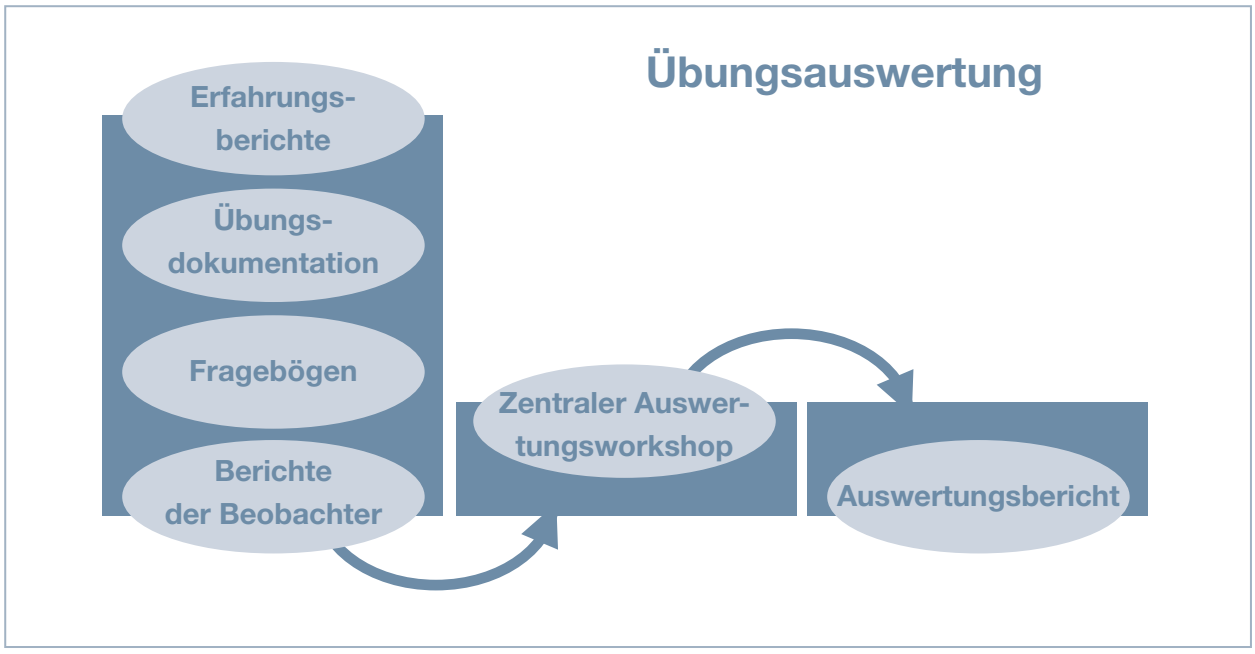


Abbildung 21: Prozess der Übungsauswertung

D. Fazit

Abbildung 22: Übergeordnete Übungsziele von „LÜKEX 11“

Die Übung „LÜKEX 11“ ist, insbesondere im Hinblick auf übergeordneten Übungsziele des Übungsrahmens (siehe Abbildung oben) und hier auf die Sensibilisierung für Fragen der „IT-Sicherheit“ und das In-Gang-Setzen geeigneter Integrationsprozesse (z. B. die Zusammenführung von IT-Krisenmanagement und allgemeinem Krisenmanagement), erfolgreich verlaufen.

Unbenommen noch durch den IT-Planungsrat zu treffender weitergehender Regelungen konnte im Verlauf der Übung erstmalig der Informationsaustausch zwischen Bund und Ländern auf definierten Meldewegen erfolgreich erprobt und damit die Einrichtung eines VerwaltungsCERT-Verbundes angestoßen werden. Die mit der Übung „LÜKEX 11“ erreichte Netzwerkbildung ist eine gute Grundlage für die künftige Zusammenarbeit im allgemeinen Krisenmanagement wie im IT-Krisenmanagement des Bundes, der Länder und der betroffenen KRITIS-Unternehmen und der Verbände.

Im Sinne der Nachhaltigkeit sollten die systematische Umsetzung der Übungserkenntnisse und der Transfer von einschlägigem Fachwissen über den Kreis der Übungsbeteiligten hinaus ein wesentlicher Schwerpunkt nachfolgender Aktivitäten, insbesondere auch der Gremienarbeit sein.

Die Erkenntnisse der Übung sollten zu diesem Zweck in Fachkongressen oder in der Fortbildung an der AKNZ und vergleichbaren Bildungseinrichtungen von Bund und Ländern (Bundesakademie für Sicherheitspolitik, Führungsakademie der Bundeswehr, Deutsche Hochschule der Polizei, Landesfeuerwehrschulen, Hochschulen der Länder etc.) weitergegeben werden, um Impulse für die Konsolidierung des länderübergreifenden strategischen Krisenmanagements unter Einschluss des jeweiligen IT-Krisenmanagements zu vermitteln.

Zusätzlich sollten auf der Ausführungsebene regelmäßig „kleinere“ Übungen durchgeführt werden, um die Übungskultur weiterzuentwickeln und Einzelfragen detailliert untersuchen zu können.

Die Übungsergebnisse sollten darüber hinaus verstärkt im politischen Raum und gegenüber den Medien vermittelt sowie für die begleitende Sicherheitsforschung nutzbar gemacht werden.

Im Hinblick auf die zunehmende internationale Vernetzung sollte zukünftig die europäische Dimension, die mit den involvierten supranationalen Einrichtungen EZB und EUROCONTROL ansatzweise in „LÜKEX 11“ repräsentiert war, noch stärker Berücksichtigung finden.

Für die Beantwortung von Fragen zu strategischen Krisenmanagement-Übungen, zu LÜKEX allgemein und zu „LÜKEX 11“ steht Ihnen das LÜKEX-Team Bund gern zur Verfügung. Sie erreichen uns über die folgende Adresse:

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Projektgruppe LÜKEX Bund - Geschäftsstelle
Ramersbacher Str. 95
53474 Bad Neuenahr-Ahrweiler
Tel.: 0228/99550-5610
Fax: 0228/99550-5630
Mail: luekex.info@bbk.bund.de
www.bbk.bund.de / www.luekex.de

Nachwort

Liebe Leserinnen und Leser!

Der vorliegende Auswertungsbericht „LÜKEX 11“ ist das sichtbare Ergebnis einer konzertierten Aktion von Bund, Ländern und Unternehmen der Kritischen Infrastrukturen. Diese haben sich zum ersten Mal in diesem Umfang im Rahmen der 5. strategischen Krisenmanagement-Übung den neuen Herausforderungen der IT-Sicherheit in Deutschland gestellt. Mit dem Bericht sollen die Erfahrungen aus „LÜKEX 11“ allen Interessierten aus dem weiteren Übungsumfeld – Bildungseinrichtungen, Wissenschaft, Medien, Sicherheitsexperten und anderen – zugänglich gemacht werden. Die Erfahrungen – die *lessons learned* – sollen zugleich Impulsgeber sein für weitere Optimierungen von Strukturen und Verfahren des strategischen Krisenmanagements.

Der Bericht ist überdies Schlusspunkt einer intensiven zweijährigen Projektarbeit. Besondere Erwähnung verdient das große persönliche Engagement, das die Verantwortlichen der Bundes- und Landesbehörden sowie die Mitwirkenden aus Wirtschaft, Wissenschaft und Gesellschaft im Verlauf des gesamten Übungszyklus an den Tag gelegt haben. Szenario-Entwicklung und Drehbucharbeit, ja überhaupt Übungsvorbereitung und Übungsdurchführung - auch die Übungsauswertung - wären ohne das spezifische Wissen und den persönlichen Einsatz der verschiedenen Übungsbeteiligten nicht möglich gewesen. Dadurch konnte das hochkomplexe Übungsthema „IT-Sicherheit“ auch für Fachfremde, aber im Ernstfall ebenfalls Betroffene, handhabbar und greifbar gemacht werden. Diese weniger sichtbaren Übungsergebnisse von „LÜKEX 11“, den Wissenstransfer und die Vernetzungseffekte, gilt es ebenfalls in den Blick zu nehmen.

Im Namen der Projektgruppe LÜKEX Bund danke ich allen Mitwirkenden für das professionelle und fruchtbare Zusammenwirken, das ein „Zusammenspiel“ im besten Sinne des Wortes war.

Norbert Reez
Projektleiter
PG LÜKEX Bund

Das BBK, eine Fachbehörde als Partner, Dienstleister, Koordinator, Moderator

Als wichtiger Beitrag des Bundes zur Neuen Strategie zum Schutz der Bevölkerung in Deutschland wurde im Mai 2004 das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) errichtet. Gemeinsam mit der Bundesanstalt Technisches Hilfswerk (THW) nimmt es als Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des lnnern (BMI) Aufgaben der Zivilen Sicherheitsvorsorge insbesondere im Bevölkerungsschutz und in der Katastrophenhilfe wahr. Es unterstützt das BMI auf den genannten Gebieten und mit dessen Zustimmung die fachlich zuständigen obersten Bundesbehörden. lnsbesondere obliegen dem BBK:

- Erstellung einer bundesweiten Risikoanalyse
- Entwicklung von Standards und Rahmenkonzepten für den Zivilschutz
- Warnung und Information der Bevölkerung
- Ausbau eines Modularen Warnsystems mit dem Kernelement der satellitengestützten Warninformation unter Einbindung aller vorhandenen und zukünftig nutzbaren Alarmierungs- und Warnmedien.
- Information der Bevölkerung über Schutz- und Hilfeleistungsmöglichkeiten
- Förderung der Ausbildung der Bevölkerung
- Ausbildung, Fortbildung und Schulung von Entscheidungsträgern und Führungskräften aus dem Bereich der zivilen Sicherheitsvorsorge
- Unterstützung der Gemeinden in Fragen des Selbstschutzes
- Technisch-wissenschaftliche Forschung
- Auswertung und Sammlung von Veröffentlichungen
- Prüfung von Geräten und Verfahren sowie Mitwirkung bei deren Normung und Zulassung
- Ergänzende Ausstattung und Ausbildung der im Katastrophenschutz tätigen Einheiten in den Aufgabenbereichen Brandschutz, CBRN-Schutz, Sanitätswesen und Betreuung
  Ergänzende Bevorratung von Sanitätsmaterial
- Schutz von Kulturgut nach der Haager Konvention
- Geschäftsstelle der Kommission zum Schutz der Zivilbevölkerung

Des Weiteren sind die der Bundesregierung nach Artikel 85 Abs.4 des Grundgesetzes auf dem Gebiet des Zivilschutzes zustehenden Befugnisse auf das BBK übertragen.

Das BBK legt großen Wert auf die Verwirklichung einer familienbewussten Personalpolitik. Flexible Arbeitszeiten, Eltern-Kind-Zimmer und Telearbeitsplätze zeigen beispielhaft, dass das BBK die Vereinbarkeit von Beruf und Familie durch bewährte und zukunftsorientierte Maßnahmen nachhaltig fördert.

2009 wurde das BBK im Rahmen des audits berufundfamilie zertifiziert. Damit soll der bereits bestehende Katalog an familienfreundlichen Angeboten auch in den nächsten Jahren weiterentwickelt und seine Umsetzung optimiert werden.

Abkürzungsverzeichnis

AG	Arbeitsgemeinschaft
AK	Arbeitskreis
AKNZ	Akademie für Krisenmanagement, Notfallplanung und Zivilschutz
BfIT	Die Beauftragte der Bundesregierung für Informationstechnik
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BPOL	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CERT	Computer Emergency Response Team
Cyber-AZ	Nationales Cyber-Abwehr-Zentrum
EZB	Europäische Zentralbank
FAQ	Frequently Asked Questions
GMLZ	Gemeinsames Melde- und Lagezentrum (von Bund und Ländern)
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnik
KRITIS	Kritische Infrastrukturen
LÜKEX	Länderübergreifende Krisenmanagementübung (Exercise)
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
SKUKdo	Streitkräfteunterstützungskommando
SPOC	Single Point of Contact
THW	Technisches Hilfswerk
ÜSA	Übungssteuerungsanwendung
WBK	Wehrbereichskommando
ZMZ	Zivil-Militärische Zusammenarbeit
ZSKG	Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz)
ZÜST	Zentrale Übungssteuerung

Bildnachweis

Umschlag Titelbild: BMI/BBK
Seite 1 Logo „LÜKEX 11“: BBK
Seite 5 Abbildung 1: strichcode/pixelio.de
Seite 7 Abbildung 2: BBK
Seite 8 oben Abbildung 3: BBK
Seite 8 unten Abbildung 4: BBK
Seite 10 Abbildung 5: BBK
Seite 14 Abbildung 6: BMI
Seite 16 Abbildung 7 und 8: Innenministerium Thüringen
Seite 20 Abbildung 9: BSI
Seite 21 Abbildung 10 und 11: Bundespolizei
Seite 22 Abbildung 12: Innenministerium Thüringen
Seite 24 Collage 13: BBK
Seite 27 Abbildung 14: BBK
Seite 28 Abbildung 15: BBK
Seite 29 Abbildung 16 und 17: BBK
Seite 30 Abbildung 18: BBK
Seite 31 Abbildung 19: Behörde für Inneres und Sport Hamburg
Seite 32 Abbildung 20: BBK
Seite 33 Abbildung 21: BBK
Seite 35 Abbildung 22: BBK
Seite 37 Abbildung 23: BBK

Titelbild: Collage Logo „LÜKEX 11“, BBK, BSI, Krisenstab BMI