IT-Planungsrat

Bericht zur Länderübergreifenden Krisenmanagementübung 2011 (LÜKEX)

Beschluss des IT-Planungsrats

vom

25. Oktober 2012

Erfahrungen aus der LÜKEX 2011 im Hinblick auf ein effektives IT-Krisenmanagement

Bericht des Vertreters im Lenkungsausschuss zur Krisenmanagementübung LÜKEX 2011

Sitzung des IT-Planungsrates am 25. Oktober 2012

Bericht über die Erfahrungen aus der LÜKEX 2011 im Hinblick auf ein effektives IT-Krisenmanagement

Ziel der Übung war die Erprobung der bestehenden Krisenmanagementstrukturen in Bund und Ländern sowie der speziellen Fähigkeiten zur Sicherstellung der staatlichen Handlungsfähigkeit im Falle einer IT-Krise.
Schwerpunkte der Übung waren massive Störungen der staatlichen IT-Infrastruktur und bei Betreibern kritischer Infrastrukturen, die durch einen gezielten Angriff hervorgerufen wurden.
Mit der LÜKEX 2011 sollte, neben der Überprüfung der Strategien zum Schutz der nationalen Informationsstrukturen, insbesondere eine Sensibilisierung für die Thematik Cybersicherheit/Kritische Infrastrukturen erreicht sowie eine Weiterentwicklung des IT-Krisenmanagements und des allgemeinen strategischen Krisenmanagements unterstützt werden.

An der Übung haben sich auf Bundesebene 10 Bundesressorts, 20 Bundesbehörden sowie das das Nationale Cyber-Abwehrzentrum und das Nationale IT-Krisenreaktionszentrum beteiligt. Fünf Länder wirkten als intensiv-übende Länder mit, weitere sieben beteiligten sich an der Übung als übende Länder. 45 KRITIS-Unternehmen und Verbände vervollständigten diesen umfassenden, gesamtstaatlichen Übungsansatz.

Seitens des BMI wurde auf der Basis sowohl eigener Übungserkenntnisse als auch der Auswertungen der intensiv-übenden Länder ein umfassender (Gesamt-)Auswertungsbericht erstellt.

Wesentliche Erkenntnisse für bestehende IT-Krisenmanagementstrukturen

Bereits in der Vorbereitungsphase wurden die bestehenden Krisenmanagementstrukturen auf Ihre Funktionsfähigkeit überprüft und konnten – insbesondere im IT-Bereich – signifikant verbessert werden. So wurden bspw. CERT-Prozesse etabliert und IT-Krisenmanagementstrukturen, u.a. in Form eines ressortübergreifenden Fachgremiums mit eigenen Alarmierungsstrukturen, geschaffen.

Aufgrund der Besonderheit des Themas „Bewältigung einer IT-Krise“ im Rahmen des LÜKEX-Übungszyklus‘ war es eine (neue) Herausforderung für die handelnden Akteure, einen Transfer zwischen den allgemeinen Krisenmanagementstrukturen und denjenigen der IT-Sicherheit herzustellen. Aufgrund des fachlich hochspezialisierten Übungsbezugs kam dem IT-

Krisenmanagement eine besondere Bedeutung zu. So wurde das IT-Krisenmanagement nicht nur in funktionaler und fachlicher Hinsicht auf den Prüfstand gestellt, sondern es galt auch, sich im bereichsübergreifenden Ansatz mit Strukturen, Begrifflichkeiten und Handlungsweisen des allgemeinen Krisenmanagements vertraut zu machen und die Zusammenarbeit zu erproben. Die Schaffung eingeübter ressortübergreifender Krisenmanagementstrukturen hat sich als probates Mittel herausgestellt, auch hochkomplexe Krisenlagen adäquat bewältigen zu können. Hierbei ist es insbesondere hilfreich, dass die beteiligten Akteure hinreichend mit den erforderlichen besonderen Handlungsabläufen in einer Krise und dem notwendigen Zusammenwirken der einzelnen Stabsbereiche, einschließlich der Presse- und Öffentlichkeitsarbeit, vertraut sind und Krisenkommunikation als zentrale Aufgabe eines erfolgreichen Krisenmanagements begreifen.

Speziell in Bezug auf ein erfolgreiches IT-Krisenmanagement kann festgestellt werden, dass drei Faktoren die maßgeblichen Grundlagen für eine erfolgreiche Bewältigung einer IT-Krise bilden. Das IT-Krisenmanagement sollte institutionalisiert sein, es sollte integriert werden und es ist eine ausgeprägte Transferleistungsfähigkeit der handelnden Akteure erforderlich.

a) Institutionalisierung

Das IT-Krisenmanagement sollte ressortübergreifend institutionalisiert, d.h. organisatorisch verfestigt werden. Es ist erforderlich, dass ein fester definierter Mitarbeiterstab, in dem sämtliche Ressorts vertreten sind, mit dieser Aufgabe – nicht erst bei einer aufgetretenen IT-Krise – betraut wird. Diese Mitarbeiter sollten mit den Handlungsabläufen in einer Krise vertraut sein sowie Aufgaben und Zusammenwirken der einzelnen Stabsbereiche, einschließlich der Presse- und Öffentlichkeitsarbeit, kennen, um dem spezifischen Informationsbedarf im Krisenfall Rechnung tragen zu können. Insbesondere sollten die Mitarbeiter des IT-Krisenmanagements darin geübt sein, mit dem allgemeinen Krisenmanagement – wie es im Regelfall auch bei einer (übergreifenden) IT-Krise zur Lagebewältigung zum Einsatz kommt – zusammenzuarbeiten.

Hierzu sind vorherige Festlegungen erforderlich, die bspw. Alarmierung, Rufbereitschaft, Mehrfachbesetzung/Schichtfähigkeit erfassen und durch einen kontinuierlichen Sensibilisierungsprozeß begleitet werden. Darüber hinaus sollte ein IT-basiertes Protokollierungssystem, welches mit demjenigen des allgemeinen Krisenmanagements kompatibel ist, vorgehalten werden. Die Arbeit im Stab sollte – in Anlehnung an vorhandene Stabsdienstordnungen – bestimmten Funktionen zugeordnet und so die Aufgabenerfüllung klar strukturiert und arbeitsteilig organisiert sein. Von besonderer Bedeutung ist die Definition von Schnittstellen zwischen den an der Bewältigung einer Krise beteiligten Institutionen/Akteursgruppen, sowohl innerhalb der Krisenmanagementstrukturen als auch der (zuarbeitenden) Linienorganisationen.

Um im Krisenfall die Handlungsfähigkeit auch des IT-Krisenmanagements sicherstellen zu können, ist es darüber hinaus erforderlich, entsprechend ausgestattete Stabsräumlichkeiten zur Verfügung zu stellen. Die Stabsräumlichkeiten sollten – neben der originären Ausstattung auch über sichere Netzzugänge in die jeweiligen Ressortbereiche und über entsprechende Informationsmöglichkeiten verfügen. Dies kann vor allem durch die Erstellung und Hinterlegung von IT-Strukturinformationen sowie den jeweiligen Abhängigkeiten und Kritikalitäten geschehen. Darüber hinaus sollten sie es den Mitgliedern ermöglichen, die IT-Lage aktuell mitverfolgen zu können.

In einem weiteren Schritt sollte dann auch die Schaffung eines geeigneten Ausweichsitzes geprüft werden.

b) Integration

Damit die Gesamtlage adäquat bewältigt werden kann, sollte der IT-(Krisenmanagement)-Sachverstand in die allgemeinen Krisenmanagementstrukturen integriert werden. Der IT-Sachverstand muss in die Stäbe getragen werden. Dies kann am besten durch einen eigenen IT-Fachberater im jeweiligen Stab geschehen. Darüber hinaus sollte sichergestellt werden, dass der IT-Gesamtverantwortliche (bspw. CIO) in die Leitungsebene eingebunden wird.
Der IT-Fachberater sollte in engem Kontakt mit dem IT-Krisenmanagement stehen, um so den in beide Richtungen erforderlichen Informationsfluss sicherstellen zu können und die zentrale Schnittstelle zwischen den beiden Krisenmanagementinstitutionen zu bilden.

c) Transferleistungsfähigkeit der Akteure

In einer IT-Krise werden hohe Anforderungen an die Transferleistungsfähigkeit und -bereitschaft der Beteiligten gestellt. Die **Akteure der IT-Welt** müssen in der Lage zur allgemeinverständlichen Darstellung der Problemlage und entscheidungserheblichen Tatsachen sein. Sie müssen – auch für IT-Laien – nachvollziehbare und von den Entscheidungsträgern bewertbare Problemlösungsvorschläge mit Folgenabschätzung abgeben können. Aber auch die **Krisenmanagement-Akteure** sind im Falle einer IT-Krise besonders gefordert. Sie sollten bereit sein, in einem arbeitsteiligen Zusammenwirken mit dem IT-Krisenmanagement mit einer ausgeprägten fachlichen Eigenständigkeit, auch ein Stück weit Verantwortung aus der Hand zu geben.
Schließlich sind auch die **politischen Entscheidungsträger** in besonderer Weise gefordert. Hier sollte die Bereitschaft bestehen, sich in gebotenem Maß auch inhaltlich mit stark technikorientierten und hochkomplexen Fragestellungen zu befassen. Gerade vor dem Hintergrund der umfassenden Folgenwirksamkeit von derartigen IT-Störungen, nicht zuletzt auch im politischen Raum, sollten die Lagevorträge eingeordnet und die Entscheidungsvorschläge abgewogen werden. Dies kann bspw. dadurch erreicht werden, dass bereits in Zeiten vor einer Krise den

Entscheidungsträgern die Zusammenhänge und Konsequenzen von IT-Störungen vermittelt werden.

Während der LÜKEX 2011 war festzustellen, dass Schulungen für die Stabsarbeit und kontinuierliche Fortbildungen im Krisenmanagement für die Mitarbeiter der Krisen-/ Verwaltungsstäbe wesentliche Voraussetzungen für das Funktionieren der Stäbe unter den schwierigen Bedingungen von Übungen und somit erst recht für den Einsatz sind.

Bei Auswahl und Schulung der eingesetzten Mitarbeiter muss berücksichtigt werden, dass gerade die Mitarbeiterinnen und Mitarbeiter aus den Ressorts, die keine Sicherheitsaufgaben zu bewältigen haben, rgm. nur auf geringe Kenntnisse in Bezug auf Stabsarbeit etc. zurückgreifen können. Dies muss bei der Konzipierung eines Fortbildungs- bzw. Übungsplans berücksichtigt werden, um den erforderlichen Kenntnis- und Übungsstand gewährleisten zu können.

Weiterhin hat sich in diesem Kontext das Nationale Cyber-Abwehrzentrum als wichtige Informationsdrehscheibe gezeigt, da gerade dort der fachübergreifende Sachverstand zur strategischen Krisenbewältigung zusammengeführt werden konnte. Es stellt eine sinnvolle Ergänzung zu dem für die operative Lagebewältigung zuständigen nationalen IT-Krisenreaktionszentrum (BSI) dar.

Die fach- und ebenenübergreifende Zusammenarbeit des Krisenmanagements sollte gerade im Hinblick auf IT-Krisen weiter optimiert und im Rahmen weiterer Übungen vertieft werden. Routinemäßige Analysen und vorausschauende Lagebewertungen des nationalen IT-Krisenreaktionszentrums stellen eine wichtige Informationsgrundlage für diese Zusammenarbeit dar.

Gerade in Bezug auf die Erhaltung der Funktionsfähigkeit Kritischer Infrastrukturen sollte die Bedeutung von IT-Verfahren auf die Daseinsvorsorge bei der Risikobewertung künftig noch stärker in den Blick genommen werden. Für die relevanten Bereiche sollte Maßnahmenpläne zur strategischen Ausfallvorsorge erstellt werden, die auch redundante und autarke Rückfallebenen einschließen. Hierbei müssen die berechtigten Interessen der KRITIS-Betreiber im Hinblick auf den Schutz von Unternehmensdaten angemessen berücksichtigt werden.

Insgesamt hat sich die LÜKEX 2011 als ein wirksames Instrument erwiesen, um über das IT-Szenario die Zusammenarbeit des Bundes und der Länder in der Krisenbewältigung zu üben und das Bewusstsein für die Notwendigkeit eines gemeinsamen Handelns zu schärfen.

Zusammenfassung der wesentlichen Handlungsempfehlungen

I. Krisenmanagementbezogene Aspekte
- Institutionalisierung, Integration und Transferleistungsfähigkeit
- Verbesserung der Kommunikation und der Entwicklung eines Wissensmanagements des IT-Krisenmanagements
- Regelmäßige Beübung der geschaffenen IT-Krisenmanagementstrukturen

II. Sicherheitsaspekte im IT-Bereich
- Schutzbedarf von IT-Strukturen
  - Die Kritikalität von verwaltungseigenen Fachverfahren und Infrastrukturkomponenten wird erhoben, dokumentiert und aktualisiert.
  - Risikobewertung in Bezug auf die Funktionsfähigkeit Kritischer Infrastrukturen und möglicher Störungen infolge einer Cyber-Attacke
  - Notfallszenarien werden erarbeitet und erprobt
  - Ermittlung der Abhängigkeiten der IT-Verfahren untereinander und von der gemeinsamen Infrastruktur auf der Basis eines einheitlichen Gefährdungsrasters.
- Schaffung eines integrierten IT-Sicherheitsmanagements
  - Härtung der Systeme
    - Aktuelles und verlässliches Patchmanagement für Betriebssysteme, Datenbanken und Anwendungssoftware
    - Einheitliches Virenabwehrmanagement
    - Systematische Deaktivierung nicht benötigter Ports und Protokolle
    - Reduktion der Verfahrensschnittstellen
  - Etablierung von betrieblichen Sicherheitsprozessen
  - Weitere Maßnahmen nach Empfehlungen des BSI

Beschlussvorschlag:

Der IT-Planungsrat nimmt den Bericht seines Vertreters im Lenkungsausschuss zur Krisenmanagementübung LÜKEX 2011 zur Kenntnis und begrüßt die aus der Übung abgeleiteten Handlungsempfehlungen für die IT-Verantwortlichen in Bund und Ländern.