Gesprächsleitfaden / Themenkatalog

der Länder-Unter-Arbeitsgruppe
„Cyber-Sicherheit-KRITIS“ (AG KRITIS)

(Stand: 10.10.2012 14:06)

Themenkatalog zur Bestandsaufnahme der Cyber-Sicherheit kritischer Infrastrukturen

Gesprächsleitfaden / Themenkatalog

der Länder-Unter-Arbeitsgruppe
„Cyber-Sicherheit-KRITIS“ (AG KRITIS)

(Stand: 10.10.2012 14:06)

Gesprächsleitfaden / Themenkatalog

der Länder-Unter-Arbeitsgruppe
„Cyber-Sicherheit-KRITIS“ (AG KRITIS)

(Stand: 10.10.2012 14:06)

1 Ziele

Der vorliegende Gesprächsleitfaden zur Bestandsaufnahme der Cyber-Sicherheit bei Betreibern kritischer Infrastrukturen (KRITIS) dient der Kontaktaufnahme und dem gegenseitigen Austausch mit KRITIS-Betreibern zum Thema Cyber-Sicherheit.

Der Leitfaden ist bewusst nicht als Fragebogen gestaltet worden, sondern soll die gedankliche Vorbereitung für einen Informations- und Erfahrungsaustausch zwischen den Ländern und den KRITIS-Betreibern auf gleicher Augenhöhe erleichtern und die Gleichartigkeit der Gespräche zwischen den Ländern und den KRITIS-Betreibern fördern.

In den Gesprächen soll das Bewusstsein für die Risiken geschärft werden, die sich aus den Bedrohungen aus dem Cyberraum ergeben. Nach der Sensibilisierung der Gesprächspartner sollen in weiteren Gesprächen eine Bestandsaufnahme eingeleitet und Handlungsnotwendigkeiten abgeleitet werden.

2 Rahmenbedingungen

Die Gespräche sollen auf Landesebene jeweils über eine einheitliche Kommunikationsschnittstelle (Single Point of Contact) geführt werden. Dadurch sollen die Gesprächspartner nicht mehrfach mit den Bereichen Katastrophenschutz und Cyber-Sicherheit konfrontiert werden.

Dabei sollen möglichst die auf Länderebene vorhandenen Organisations- und/oder Gremienstrukturen genutzt werden. Es sollten keine zusätzlichen Institutionen geschaffen werden. Die Gesprächsrunden sollten von Seiten der Länder und Unternehmen bzw. Verbände jeweils mit KRITIS- / Krisenmanagement- und IT/Cyber-Fachkompetenz besetzt werden und diese einheitlich nach außen repräsentieren.

3 Mögliche Gesprächsthemen

3.1 Herstellen einer gemeinsamen Gesprächsbasis

Damit Deutschland auf Dauer wettbewerbsfähig bleibt, ist es auf solide und sichere Infrastrukturen angewiesen. Sie sind ein Standortfaktor mit Zukunft. An oberster Stelle steht die Sicherung der Organisationen und Einrichtungen, die eine wichtige Bedeutung für das Gemeinwesen haben und deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere weitreichende Folgen für unsere Gesellschaft hätte, den so genannten Kritischen Infrastrukturen.

3.1.1 Warum trifft man sich zu gemeinsamen Gesprächen?

Die Bedrohungen aus dem Cyberraum wachsen ständig und richten sich zunehmend auch gegen Kritische Infrastrukturen. Deswegen hat die Bundesregierung mit der Cyber-Sicherheitsstrategie dem Schutz Kritischer Infrastrukturen höchste Priorität gegeben. Ziel der Bun-

desregierung ist es, einen signifikanten Beitrag für einen sicheren Cyber-Raum zu leisten. Dadurch sollen die wirtschaftliche und gesellschaftliche Prosperität für Deutschland bewahrt und gefördert werden. Die Cyber-Sicherheit in Deutschland ist auf einem der Bedeutung und der Schutzwürdigkeit der vernetzten Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen. Der Zustand eines sicheren Cyber-Raums ergibt sich dabei als Summe aller nationalen und internationalen Maßnahmen zum Schutz der Verfügbarkeit der Informations- und Kommunikationstechnik sowie der Integrität, Authentizität und Vertraulichkeit der sich darin befindenden Daten. Cyber-Sicherheit kann nur in einem umfassenden Ansatz verfolgt werden. Dies erfordert die weitere Intensivierung des Informationsaustausches und der Koordinierung.[1]

Ergänzend zu den Aktivitäten der Bundesregierung bemühen sich auch die Länderregierungen um entsprechende Gespräche mit Unternehmen und Verbänden, um im Rahmen ihrer Zuständigkeit für den Schutz Kritischer Infrastrukturen durch Cybersicherheit zu sorgen.

Die Gespräche auf Länderebene werden ergänzend und parallel zu den Bundesaktivitäten geführt. Die Anknüpfungspunkte zum Bund sind dabei insbesondere:

- Die KRITIS-Strategie des Bundes, die Zusammenarbeit des Bundes und der Länder gem. § 18 Abs. 2 ZSKG und der Beschluss des AK V zu KRITIS aus Herbst 2011.
- die Cybersicherheitsstrategie, der UP-KRITIS, die Gespräche des Bundesinnenministers mit KRITIS-Betreibern sowie die Allianz für Cybersicherheit des BSI.

Die Gespräche sollen im Gleichklang zu den Bundesaktivitäten stehen und der Verstetigung des von Bund und Ländern gemeinsam initiierten Prozesses auf Länderebene dienen.

Über die jeweiligen Gespräche wird mit den Partnern Vertraulichkeit vereinbart.

3.1.2 Liegt eine Kritische Infrastruktur vor?

Da es derzeit – unterhalb der Sektoren- und einer gegebenenfalls landespezifischen Brancheneinteilung – keine Kataster mit konkrete Einrichtungen oder Anlagen als KRITIS gibt, ist mit den Gesprächspartnern die Bedeutung der einzelnen Organisation bzw. des einzelnen Unternehmens, möglicherweise auch nur die Bedeutung einzelner Bestandteile der Organisation oder des Unternehmens als Kritische Infrastruktur im Gesamtsystem einvernehmlich zu bewerten.

Die KRITIS-Strategie des Bundes definiert Kritische Infrastrukturen als „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.“

[1] Cyber-Sicherheitsstrategie für Deutschland, BMI, 2011

Hierbei ist vorrangig die Kritikalität zu beurteilen: Infrastrukturen gelten dann als „kritisch“, wenn sie für die Funktionsfähigkeit moderner Gesellschaften von wichtiger Bedeutung sind und ihr Ausfall oder ihre Beeinträchtigung nachhaltige Störungen im Gesamtsystem zur Folge hat. Ein wichtiges Kriterium dafür ist die Kritikalität als *relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat*.[2]

Zur Feststellung der Kritikalität betrachtet man Teilprozesse und Komponenten einer Sektoren- oder Branchenaufgabe. Die Kritikalität und somit der Schutzbedarf des jeweiligen Teilprozesses und der Komponente sind abhängig von deren Einfluss auf die Folgeprozesse und -komponenten und somit die Funktionsfähigkeit des gesamten Infrastruktursystems. Kritikalität und Schutzbedarf sind somit ein relatives Maß der Folgen bei Eintritt einer Gefahr. Die Folgen durch den Ausfall der einzelnen Komponente können durch Bildung relevanter Gefahrenszenarien (z. B. Unwetter oder Cyberangriff) und der Betrachtung der Auswirkungen (Ausfälle) im betroffenen Infrastruktursystem festgestellt werden. Hierzu bietet sich der Ansatz des BBK an:

1. Handelt es sich um eine Infrastruktur aus den KRITIS-Sektoren / -Branchen laut www.kritis.bund.de und aus den gegebenenfalls landesspezifisch festgelegte Branchen?
2. Sind von einem Ausfall auch andere KRITIS betroffen?
3. Ist die Infrastruktur die größte Versorgungsquelle für den Untersuchungsraum?
4. Ist die Infrastruktur die einzige Versorgungsquelle für den Untersuchungsraum?
5. Ist die Infrastruktur auch für andere außerhalb des Untersuchungsraums die einzige Versorgungsquelle?

Mögliche Kriterien zur Identifizierung von KRITIS können sein:

- Marktbeherrschung (Monopol-, Oligopolbranchen)
- Versorgungsgrad (prozentualer Anteil der Versorgung in Region/Land)
- Zeitlicher Aspekt (wie schnell treten Folgen auf, wie lange ist Ausfall)
- Auswirkung auf Bevölkerung / andere Infrastrukturen / Wirtschaftsstandort (Folgenbetrachtung)

[2] KRITIS-Strategie des Bundes, 2009

3.2 Strukturen und Kooperationen (Organisation und Management)

3.2.1 Etablierung eines IT-Sicherheitsmanagementsystems

Das IT-Sicherheitsmanagementsystem bedarf einer entsprechenden Bedeutung im unternehmerischen Optimierungsprozess und sollte Bestandteil des Qualitätsmanagement und Risikomanagement sein.

Im Unternehmen existieren angemessene Beziehungen oder Kooperationsstrukturen zwischen materieller Sicherheit, IT-Sicherheit und personeller Sicherheit. Schadensfälle werden unternehmensintern, aber auch innerhalb der Branche oder der Aufsichtsbehörden analysiert (Rekonstruktion der Schadensursache, Schlussfolgerungen, Umsetzung einschließlich Erfolgskontrolle). Die Erkenntnisse fließen in die Weiterentwicklung in allen Bereichen der Informationssicherheit ein.

Die Fähigkeit zur Planung wirksamer Cyber-Sicherheits-Maßnahmen wird im Wesentlichen durch die Qualität und den Umfang des eigenen Informationsstands bestimmt. Das Unternehmen ist daher an einen entsprechenden CERT-Verbund angeschlossen und wird mit aktuellen und fachlich verlässlichen Informationen zur Cyber-Sicherheit versorgt.

3.2.2 Gewährleistung der Verfügbarkeit notwendiger Ressourcen, Bereitstellung angemessener eigener Ressourcen

Die wirksame Abwehr von Bedrohungen der Cyber-Sicherheit erfordert auch die Bereitstellung angemessener Ressourcen. Diese Aufwände müssen von Unternehmen und Behörden in jeder Phase der IT-Planung und dem anschließenden IT-Betrieb hinreichend berücksichtigt werden. Entsprechende finanzielle und personelle Mittel müssen bereitgestellt werden.

3.2.2.1 Zusammenarbeit im Schadensfall

Gerade Ressourcen, die erst bei unvorhergesehenen Sicherheitsvorfällen benötigt werden, sollten rechtzeitig eingeplant werden. Bereits lange vor dem tatsächlichen Vorfall muss feststehen, auf welchen externen Dienstleister im Ernstfall verlässlich und kurzfristig zurückgegriffen werden kann.

Daher muss ausgeschlossen werden, dass ein unverzichtbarer Vertragspartner nicht ebenfalls durch ein extremes Ereignis seine Leistungen einstellen muss, insbesondere, weil er kein umfassendes Risiko- und Krisenmanagement-System betreibt.

Über die unmittelbaren Betriebsprozesse hinaus muss feststehen, welche weiteren Kooperationen für den Großschadensfall erforderlich sind, bspw. zur Aufrechterhaltung oder Wiederherstellung der für die IT notwendigen Energie- und Kommunikationsnetze. Hierzu ist die Zusammenarbeit mit beteiligten Sicherheitsbehörden sowie Rettungs- und Katastrophenschutzorganisationen evaluierbar zu regeln.

3.2.2.2 Sicherheitsüberprüfung von Fremdfirmen

In der sicherheitsrelevanten Zusammenarbeit mit anderen Unternehmen – wie im Rahmen von Outsourcing sowie mit anderen Nutzern der IKT-Infrastruktur, beispielsweise in regionalen Verbünden – sind die unternehmensinternen Sicherheitsrichtlinien entsprechend anzuwenden.

3.2.2.3 Einbindung externer Dienstleister

Das für einen umfassenden Schutz erforderliche Know-how ist, angesichts der hohen Spezialisierung und Veränderungen, oftmals in der Organisation nicht oder nicht wirtschaftlich darstellbar. Um IT-Sicherheitsmaßnahmen vollständig und wirksam umzusetzen zu können, muss regelmäßig auch auf externes Fachwissen zurückgegriffen werden. Dies kann insbesondere für folgende Bereiche sinnvoll sein:

- Durchführung einer herstellerneutralen Cyber-Sicherheitsberatung,
- Penetrationstests gegen die eigene IT,
- regelmäßige Cyber-Audits, Cyber-Quickcheck, automatisierte Schwachstellenüberprüfungen, Grundschutz-Audits,
- Informationssicherheits-Revisionen,
- Analyse und Bewältigung von Sicherheitsvorfällen durch ein externes Computer Emergency Response Team (CERT), sowohl in simulierten Übungsszenarien als auch im Ernstfall,
- Durchführung forensischer Maßnahmen.

3.3 Untersuchungen, Konzepte (Analyse des Schutzbedarfs)

3.3.1 Festlegung der Basismaßnahmen zur Cyber-Sicherheit

Risikoanalysen, wie bspw. die Bestimmung der Cyber-Sicherheits-Exposition der zu schützenden Infrastruktur gemäß BSI, bilden die Voraussetzung für die Planung und Umsetzung angemessener Maßnahmen und ihre anschließende Bewertung auf Notwendigkeit, Angemessenheit und Wirtschaftlichkeit. Mithilfe der in Kapitel 3.4, „Präventionsmaßnahmen (innerer, äußerer und personeller Schutz)“ dargestellten Maßnahmen der Cyber-Sicherheit sollen die Verantwortlichen für IT-Planung und -Betrieb in die Lage versetzt werden, orientiert an der zuvor bestimmten Cyber-Sicherheits-Exposition, ein angemessenes Cyber- Sicherheits-Niveau zu realisieren. Die Risikoanalyse der IKT muss mit den sonstigen Unternehmenssicherheitskonzepten auf systemübergreifende Interdependenzen (Domino- und Kaskadeneffekte) überprüft werden. Cyber-Sicherheitsmaßnahmen müssen auch mittels Kosten-Nutzen-Analysen hinsichtlich des möglichen Schadensausmaßes beurteilt werden.

Kritische Infrastrukturen können nur dann ohne nennenswerte Unterbrechungen funktionieren, wenn ihre Kernprozesse und die zugrunde liegenden IT-Prozesse robust ausgestaltet sind. Eine umfassende und konsequent wirkungsvolle Umsetzung von Schutzmaßnahmen, die dem jeweiligen Schutzbedarf entsprechen, ist grundlegend. Für eine nachvollziehbare Überprüfung bedarf es regelmäßiger Sicherheitsaudits.

3.3.2 Zusatzmaßnahmen bei höherer Cyber-Sicherheits-Exposition

Die Verfügbarkeit, Vertraulichkeit und Integrität von Informationstechnik bilden die klassischen Grundwerte für einen sicheren Betrieb. In Abhängigkeit des individuellen Schutzbedarfs eines Systems, Netzsegments oder der gesamten Organisation sind zur Gewährleistung dieser Grundwerte zusätzliche Maßnahmen gemäß spezieller Sicherheitskonzepte erforderlich. Die Notwendigkeit folgt insbesondere aus der oben beschriebenen Feststellung der Cyber-Sicherheits-Exposition, sobald hohe oder sehr hohe Werte in Bezug auf Vertraulichkeit, Verfügbarkeit oder Integrität festgestellt werden. Es empfiehlt sich, Konzepte aus vergleichbaren Bereichen oder Branchen auszuwerten. Auch aus besonders gravierenden Vorfällen im Zusammenhang mit dem Kerngeschäftsfeld des Unternehmens müssen entsprechende, herausragende Konsequenzen gezogen werden.

Besondere Prozesse bedürfen darüber hinaus besonderer Sicherheitsmaßnahmen. Diese Prozesse sollten weder mit dem Internet und mit öffentlichen Netzen verbunden sein, noch von über das Internet angebotenen Diensten abhängig sein.

3.3.3 Produkt- und Dienstleistungssicherheit gewährleisten

Umfassende IT-Sicherheit lässt sich nur durch Security-by-Design erreichen. Daher fließen IT-Sicherheitsaspekte von Beginn an in die Planung von IKT-Netzen und –Anwendungen sowie bei der Beschaffung von IKT-Produkten mit ein. Wo verfügbar, kommen für besonders sensible Bereiche zertifizierte Produkte bzw. Dienstleistungen zur Anwendung.

3.3.4 Erfassung und sicherheitstechnische Bewertung der IT-Systeme und IT-Verfahren

Zur Planung und anschließenden Umsetzung von Abwehrmaßnahmen auf den eingesetzten IT-Systemen ist zunächst eine vollständige Inventarisierung der eingesetzten IT-Systeme notwendig[3]. Mithilfe dieses Inventarverzeichnisses ist insbesondere zu klären, welche verschiedenen Systemtypen in der Organisation im Einsatz sind.

Anhand der Inventarisierung sollte auch die Frage geklärt werden, ob die erhobene Vielfalt an Systemen sicherheitstechnisch und administrativ beherrschbar ist.

[3] im Sinne des BSI-Grundschutz und BSI-Basismaßnahmen

3.4 Präventionsmaßnahmen (innerer, äußerer und personeller Schutz)

3.4.1 Sicherstellung eines aktuellen Informationsstands

Eine umfassende Information über die aktuelle Cyber-Gefährdungslage ist Voraussetzung für die eigene Handlungsfähigkeit und Grundlage für eine abgestimmte, effektive Reaktion.

Grundlegend wichtige Informationsquellen sind:

- Warn- und Informationsmeldungen eines etablierten CERT,
- Warn- und Informationsmeldungen zu industriellen Steuerungsanlagen (Industrial Control Systems CERT, ICS-CERT),
- Lagebilder von staatlichen Stellen, Herstellern und Sicherheitsdienstleistern,
- Warnungen und Sicherheitsempfehlungen von zuständigen Sicherheitsgruppen der jeweiligen Hersteller innerhalb des Unternehmens oder der Behörde eingesetzter Informationstechnik, z.B. des Microsoft Security Response Centers oder des Adobe Product Security and Incident Response Teams.

Diese Quellen müssen täglich ausgewertet werden. Kritische Informationen müssen unmittelbar zu Reaktionen führen.

Mechanismen zur Früherkennung von Gefährdungen und eine Anbindung an die Warn- und Alarmierungsmechanismen (i.d.R. über sogenannte Single Points of Contact, SPOCs) des Umsetzungsplan KRITIS gewährleisten die nationale Handlungsfähigkeit – hierfür sind gegenüber dem BSI „Warn- und Alarmierungskontakte“ benannt. Nur so kann sichergestellt werden, dass bei schwerwiegenden Beeinträchtigungen oder Cyber-Angriffen andere betroffene kritische Infrastrukturen und das Lagezentrum des BSI unverzüglich informiert werden.

3.4.2 Absicherung von Netzübergängen

3.4.2.1 Identifikation aller Netzübergänge

Netzzugänge sind im Rahmen einer Netzstrukturaufnahme vollständig zu erfassen. Hierzu zählen auch insbesondere:

- individuelle DSL-Zugänge,
- UMTS-Datenverbindungen mobiler Geräte und
- verschlüsselte Kommunikationswege wie z.B. von IT-Nutzern selbst eingerichtete und genutzte VPN-Verbindungen,

die Schutzmaßnahmen der allgemeinen Netzinfrastruktur umgehen können.

Von besonders kritischer Bedeutung sind Zugänge zu Netzen und IT-Systemen für Administratoren, vor allem solche Zugänge, die auch eine Fernwartung/Fernadministration erlauben.

Darüber hinaus sind auch Netzübergänge zwischen verschiedenen Liegenschaften und Anbindungen von Produktivsystemen zu erfassen.

3.4.2.2 Segmentierung des Netzes und Minimierung der Übergänge

Voraussetzung für eine in der Praxis umsetzbare und im Betrieb beherrschbare Lösung ist eine am Schutzbedarf unterschiedlicher Bereiche orientierte Netzsegmentierung sowie eine weitgehende Minimierung der externen Netzübergänge. Eine Umgehung dieser minimierten Zahl an Netzübergängen, z. B. durch parallel betriebene DSL- oder UMTS-Zugänge, muss technisch und organisatorisch unterbunden werden.

3.4.2.3 Sicherheitsgateways

Die minimierte Zahl an Netzübergängen muss mit einem geeigneten Sicherheitsgateway abgesichert werden, das mindestens über folgende Eigenschaften verfügt:

- Application Level Gateway bzw. Proxy Firewall
- Intrusion Detection (ab einer hohen Cyber-Sicherheits-Exposition in Bezug auf Vertraulichkeit oder Integrität)
- Intrusion Prevention (ab einer sehr hohen Cyber-Sicherheits-Exposition in Bezug auf Vertraulichkeit oder Integrität)
- Überprüfung von Datenströmen wie E-Mail, http, https und ftp auf Schadprogramme
- Möglichkeit für Blacklist- und Whitelist-Lösungen, insbesondere beim Zugriff auf Webseiten

Mit einem geeigneten Set von Überwachungswerkzeugen muss erreicht werden, dass auch Erkenntnisse zu nicht erfassten Zwischenfällen (Dunkelfelderhellung) möglich sind (s.a. Kapitel 3.4.6, Logdatenerfassung und -auswertung).

3.4.2.4 Schnittstellenkontrolle

Eine Umgehung des Sicherheitsgateways ist durch eine technische Schnittstellenkontrolle auf Client-Systemen, Servern oder weiteren IT-Systemen auszuschließen, um beispielsweise Angriffe über externe Speichermedien (z.B. USB-Speichermedien, Digitalkameras oder MP3-Player) abwehren zu können.

3.4.2.5 Absicherung mobiler Zugänge

Mobile IT-Systeme - wie Smartphones oder Laptops - unterliegen einem sehr hohen Verlust- und Diebstahlrisiko. Daher sind die Berechtigungen, mit denen sich Nutzer über ein mobiles

IT-System im Netz bewegen können, auf das unbedingt erforderliche Mindestmaß zu beschränken. Verlustfälle mobiler IT-Systeme müssen im Vorfeld eingeplant werden. Reaktive Maßnahmen müssen geübt und im Ernstfall schnell umgesetzt werden, auch außerhalb üblicher Arbeitszeiten.

3.4.3 Abwehr von Schadprogrammen

Die gestaffelte Verteidigung von Angriffen unter dem Einsatz von Schadprogrammen (Viren, Würmer und Trojanische Pferde) muss über eine große Zahl von Systemen verteilt werden. Der eigentliche Client als Arbeitsplatzsystem ist dabei die letzte Verteidigungslinie.

Insbesondere sind Schutzprogramme gegen Schadsoftware auf folgenden Systemen durchgängig einzusetzen:

- Sicherheitsgateway,
- E-Mail-Server,
- Dateiserver,
- mobile und stationäre Arbeitsplatzsysteme.

Bei der Auswahl von Schutzprogrammen sollte ab einer hohen Cyber-Sicherheits-Exposition in Bezug auf Vertraulichkeit oder Integrität darauf geachtet werden, dass mehrere Lösungen unterschiedlicher Anbieter eingesetzt werden.

3.4.4 Vermeidung von offenen Sicherheitslücken

Der überwiegende Teil von Angriffen gegen IT-Systeme erfolgt über Schwachstellen in eingesetzten Softwareprodukten, die in aktuelleren Versionen bereits durch die Hersteller geschlossen oder für die neue Schutzmaßnahmen entwickelt wurden. Mit vergleichsweise geringem Aufwand kann daher eine besonders große Schutzwirkung durch:

- ein effizientes Patchmanagement,
- stärkere Abwehrmechanismen in aktuellerer Software und
- Workarounds und Sicherheitsaktualisierungen

erzielt werden. Aktualisierungen der eingesetzten Software müssen stets kurzfristig installiert werden.

3.4.5 Sichere Interaktion mit dem Internet

Alle Vorgänge, bei denen Daten und Dienste aus dem Internet abgefragt und verarbeitet werden, sind mit geeigneten Maßnahmen abzusichern. Dabei ist insbesondere in Betracht zu ziehen, dass ein zu schützendes System dem Angreifer ggf. nur als Zwischenstation für ei-

nen darüber hinaus gehenden Angriff gegen vollkommen andere Ziele im selben Netzsegment dient. Deshalb sind ausschließlich

- sichere Browser,
- sichere E-Mail-Anwendungen und
- Verfahren zur sicheren Darstellung von Dokumenten

einzusetzen. Beispiele für letzteres sind die „Geschützte Ansicht“ in Microsoft Office 2010 oder der „Geschützte Modus“ im Adobe Reader X.

3.4.6 Logdatenerfassung und -auswertung

Mithilfe eines gut getarnten und hinreichend vorsichtigen Vorgehens ist es Angreifern u. U. möglich, über längere Zeiträume die Kontrolle über Zielsysteme zu übernehmen, ohne dass diese Angriffe unmittelbar aufgrund singulärer Ereignisse detektiert werden.

Eine zentrale Rolle spielt daher hierfür die regelmäßige Auswertung von Logdaten. Wichtige Quellen für Logdaten sind in jedem Fall das Sicherheitsgateway (s. a. Kapitel 3.4.2.3) und die eingesetzten Betriebssysteme.

Insbesondere die auf Intrusion Detection Systemen (IDS) anfallenden Daten sind ab einer hohen Cyber-Sicherheits-Exposition in Bezug auf Vertraulichkeit oder Integrität bei der regelmäßigen Auswertung mit einzubeziehen. Der Einsatz von Lösungen zum Security Information and Event Management (SIEM) ist vorzusehen.

3.4.7 Sichere Authentisierung

Im Rahmen der Authentisierung, für die eine Nutzung eines sicheren Verzeichnisdienstes vorausgesetzt wird, sollte ab einer hohen Cyber-Sicherheits-Exposition in Bezug auf Vertraulichkeit oder Integrität ein Zweifaktor-Mechanismus verwendet werden.

Unterschiedliche Rollen (s. a. Kapitel 3.4.8.2) erfordern zudem verschiedene Authentisierungsdaten. Weiterhin sind Bereiche unterschiedlichen Schutzbedarfs zu identifizieren, die in der Folge unterschiedliche Authentisierungen erfordern. Dabei ist besonders auf eine Trennung der Konten von Administratoren und anderen Nutzern zu achten.

3.4.8 Durchführung nutzerorientierter Maßnahmen

3.4.8.1 Sensibilisierung und Schulung

Auch das eigene Personal muss in den Mittelpunkt einer Cyber-Sicherheitsstrategie gerückt werden. Sämtliche technischen Vorkehrungen können durch menschliche Fehler oder bewusste Fehlhandlungen unwirksam werden.

Daher ist das Personal - vom Nutzer der Informationstechnik bis hin zum Administrator, von der Arbeitsebene bis hin zur Leitungsebene, umfassend zu sensibilisieren. Dies gilt auch für die Mitarbeiter externer Dienstleister, die in der Organisation eingesetzt werden.

3.4.8.2 Rollentrennung

Die Personalplanung muss zudem in Bezug auf die eingesetzte IT folgende Aspekte umfassen:

- Die Definition der technischen und organisatorischen Rollen,
- die Klärung von Verantwortlichkeiten eines jeden Einzelnen und
- die Festlegung von Zuständigkeiten (auch unter Einbeziehung externer Dienstleister).

Diese Planung soll eine klare Trennung von Rollen vorsehen. Eine Konzentration vieler oder aller Zuständigkeiten in einer Rolle sollte vermieden werden und Zielkonflikte bei der Rollenzuweisung sollen ausgeschlossen sein.

3.5 Krisenmanagement bei Großschadenslagen (Ausfallplanung, Redundanzen, Notfallmanagement, Rückfallebenen)

3.5.1 Mit Übungen auf den Ernstfall vorbereiten

Die Bewältigung von Sicherheitsvorfällen muss geübt werden, um die Geschäftsabläufe auch unter den erschwerten Bedingungen eines Sicherheitsvorfalls aufrecht erhalten oder zumindest schnell wiederherstellen zu können. Maßnahmen zur Eingrenzung des Schadens müssen bei der IT-Planung konzipiert werden, im Ernstfall schnell umsetzbar sein und eben daher immer wieder geübt werden.

Eine der wichtigsten Maßnahmen dabei ist eine regelmäßige Erstellung von Backups, die im Ernstfall auch tatsächlich wieder zurückgespielt werden können.

Regelmäßige Cyber-Sicherheitsübungen und die Teilnahme an größeren, branchenübergreifenden Übungen schaffen Vertrauen in die Strukturen und die gegenseitige Zusammenarbeit in IT-Krisensituationen und helfen, sektorspezifische Ansätze und Handlungsanleitungen zur Differenzierung und Bewältigung von Schadenslagen zu bilden.

Weiterhin kann die Einbindung von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sowie des BSI zur Bewältigung von Großschadenslagen optimiert werden.

3.5.2 Meldung von Sicherheitsvorfällen

Informationen zu sicherheitsrelevanten IT-Vorfällen sind die Grundlage zur Bewertung der Sicherheitslage und der Notwendigkeit, eigene Sicherheitsmaßnahmen anzupassen. Daher

sollten Informationen von bedeutenden sicherheitsrelevante IT-Vorfälle und Angriffen an die zuständigen Stellen frühzeitig gemeldet werden, um Zusammenhänge erkennen zu können.

Neben der Bewältigung des eigenen Schadens sollte bei Verdacht frühzeitig Strafanzeige erstattet werden, um weitere Vorfälle in anderen Organisationen zu vermeiden und den Polizeibehörden weitergehende Ermittlungen zu ermöglichen.

Darüber hinaus kann sowohl bei vorsätzlichen Handlungen als auch bei gravierenden technischen Problemen (zumindest anonym) eine Meldung an das BSI erfolgen, damit die Informationen zu dem gemeldeten Vorfall in das allgemeine Lagebild einfließen und übergreifende Zusammenhänge erkannt werden können. Nur so kann großflächigen IT-Schadensereignissen koordiniert begegnet werden.

Quellen:

Schutz Kritischer Infrastrukturen – Basisschutzkonzept des BMI

Diskussionspapier IT-Schutz Kritischer Infrastrukturen in Deutschland 25. Januar 2012 des BMI

Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus Herausgeber: © Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Basismaßnahmen der Cyber-Sicherheit, BSI