

IT-Sicherheits-Forum 2006

IT-Sicherheit in kritischen Infrastrukturen





- Unternehmensstandort Hamburg
- gegründet 1.4. 2005
- langjährige Beratungserfahrungen
 - Business Continuity / IT-Recovery
 - IT-Sicherheit
 - Service Level Agreements
- bei Großunternehmen und Mittelstand
 - Banken und Versicherungen
 - Industrie und Handel
 - Logistik- und Medienunternehmen
 - Behörden
- Wir helfen unseren Kunden,
 - ihre Geschäftsfähigkeit gegen operationelle Risiken abzusichern
 - und so ihre Wettbewerbsfähigkeit zu verbessern.





Einführung kritische Infrastrukturen



Definition - Kritische Infrastrukturen

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen

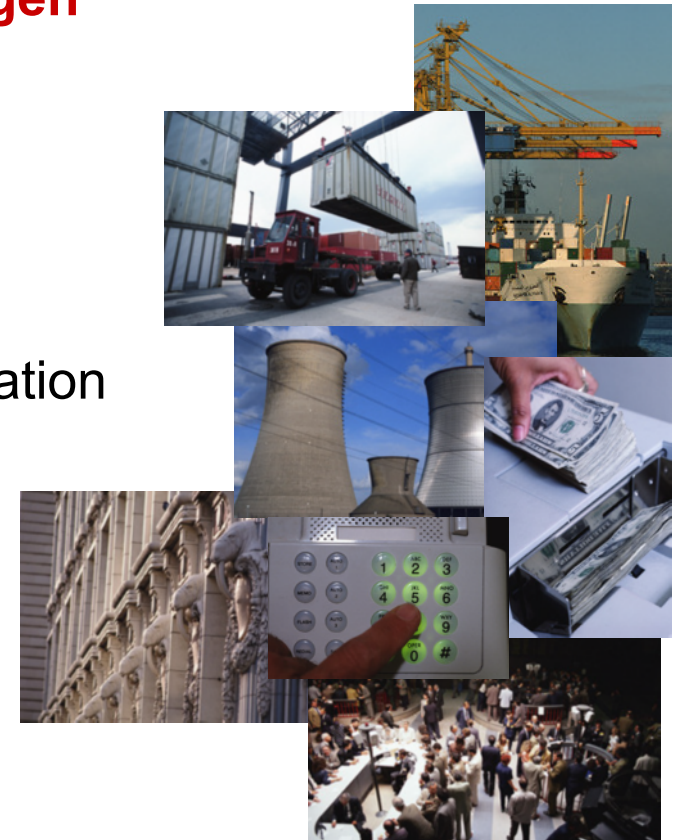
Bei Ausfall oder Beeinträchtigung **nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen**

KRITIS-Bereiche:

- Transport und Verkehr
- Energie
- Gefahrenstoffe
- Informationstechnik und Telekommunikation
- Finanz-, Geld und Versicherungswesen
- Versorgung
- Behörden, Verwaltung und Justiz

.....

Hohe gegenseitige Abhängigkeit





Rolle der IT

These:

Mit 10 exzellenten Hackern und 10 Mio. Dollar lassen sich die USA in die Knie zwingen [1]

These:

Ohne den umfassenden Einsatz unterschiedlichster Informationstechnologien wäre unsere Energie- und Trinkwasserversorgung nicht gesichert, finanzielle Transaktionen könnten nur eingeschränkt oder gar nicht stattfinden und auch Regierungen wären in ihrer Arbeit deutlich eingeschränkt [2]



[1] Arnaud de Borchgrave, Center for Strategic and International Studies (CSIS)

[2] Dr. Udo Helmbrecht, Bundesamt für Sicherheit in der Informationstechnik



Aktivitäten national und international



KRITIS-Aktivitäten USA



- Hauptfokus
 - terroristische Bedrohungen
- Beteiligte Stellen
 - Department of Homeland Security (DHS)
 - Federal Emergency Management Agency (FEMA)
 - US Commerce Department - National Institute of Standards and Technology (NIST)
 - Information Sharing and Analysis Centers (ISACs) - Branchenspezifische Frühwarnsysteme
- Aktivitäten
 - National Strategy to Secure Cyberspace
 - Protected Critical Infrastructure Information (PCII) Program
 - National Vulnerability Database



KRITIS-Aktivitäten EU



- Hauptfokus
 - terroristische Bedrohungen
- Beteiligte Stellen
 - EU-Kommission – Justiz und Inneres usw.
 - European Network and Information Security Agency (ENISA)
 - bisher keine erkennbaren Aktivitäten in Richtung KRITIS
- Aktivitäten
 - Strategiepapier «Critical Infrastructure Protection in the Fight Against Terrorism»
 - Management Decision Support for Critical Infrastructures Krisenmanagement-Tool (MEDSI)
 - Analysis & Assessment for Critical Infrastructure Protection (ACIP)
 - European Programme for Critical Infrastructure Protection (EPCIP)
 - Critical Information Infrastructure Research Coordination (CI2RCO)
 - Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN)



KRITIS-Aktivitäten Deutschland



- Hauptfokus
 - All-hazards-Ansatz
- Beteiligte Stellen
 - BMI
 - BSI zuständig für Informationssicherheit
 - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK)
 - BKA, BMWi,
- Aktivitäten
 - Gesetzgebung, z.B. (TKÜV) Telekommunikationsüberwachungsverordnung Überarbeitung 11/2005
(keine umfassenden gesetzlichen KRITIS-Vorschriften geplant)
 - Übungen, z.B. 2001 CYTEX (Cyber Terror Exercise), 2004 / 2005 LÜKEX (Länderübergreifendes Krisenmanagement Exercise)
 - Ausbildung (Akademie für Krisenmanagement und Zivilschutz)
 - Ausbau CERT-Bund als Krisenreaktionszentrums IT des Bundes und nationales Frühwarnsystem
 - Öffentlich verfügbare Hilfsmittel (BSI, BMI)



Hilfsmittel des BSI

BSI-Hilfsmittel für den Schutz Kritischer Infrastrukturen

(<http://www.bsi.de/fachthem/kritis/hilfsmittel.htm>)

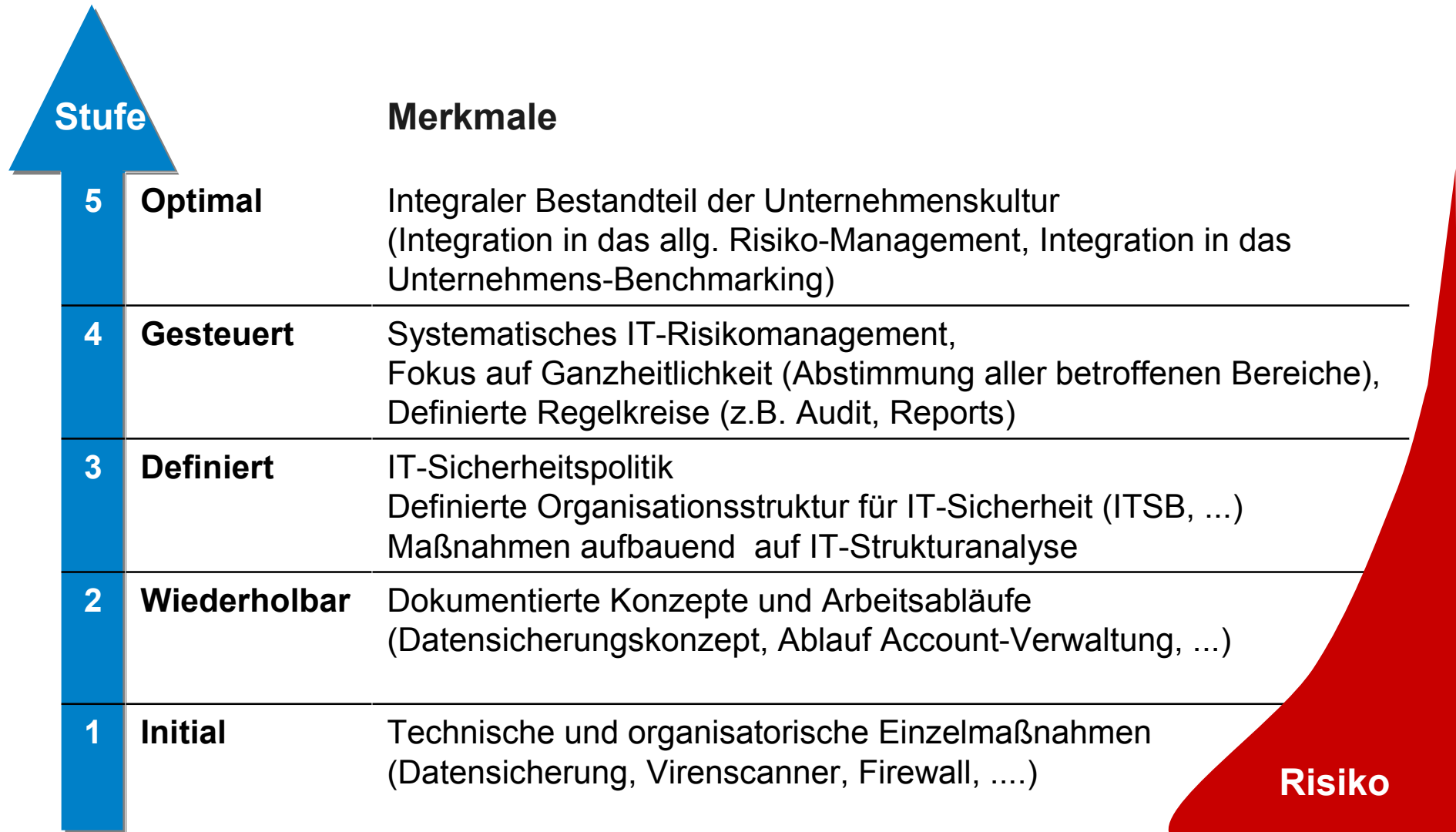
- **Beispielrichtlinie**
 - Verdichtung der IT-Sicherheitsdokumentation eines internationalen Unternehmens aus der Mineralölbranche
 - Regeln für die sichere Gestaltung von Management-Prozessen im IT-Umfeld und von technischen IT-Lösungen
 - Behandelt auch SCADA
- **Standort-Sicherheitscheck**
 - Umsetzung der Regeln der Beispielrichtlinie als Audit
 - Für dezentrale IT-Standorte
- **Weitere**
 - GSHB
 - BMI Schutz kritischer Infrastrukturen – Basisschutzkonzept
 -



Sicherheitsrichtlinie und –check in der Praxis



Reifegrad des IT-Sicherheits-Managements



Risiko

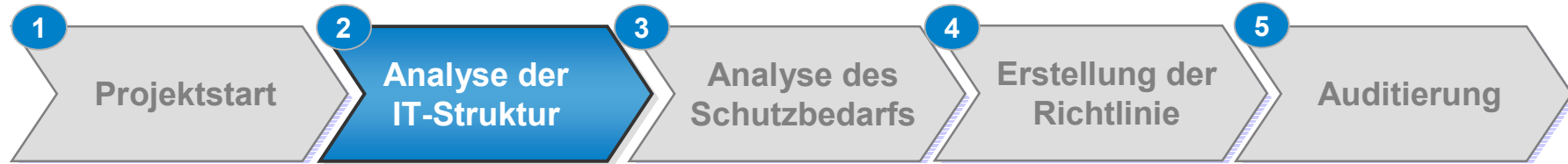


Beispielprojekt

- Mittelständisches Unternehmen der Finanzbranche (ca. 500 MA)
- Ausgangslage (Reifegrad 3)
 - IT-Sicherheits-Rollen eingeführt
 - IT-Strategie und IT-Sicherheitsleitlinie vorhanden
 - zahlreiche technische Vorkehrungen
 - Für IT-Sicherheit relevante Arbeitsdokumente vorhanden (aber nicht vollständig und durchgängig)
 - Zahlreiche, umfangreiche Quellen mit Anforderungen, z.T. in der Praxis nicht umsetzbar
- Projektziele
 - Definition umfassender Sicherheitsziele
 - Soll/Ist-Vergleich
 - Maßnahmenkatalog zur Optimierung
- Projektumfang
 - Dauer ca. 6 Monate
 - Aufwand ca. 3-4 Personenmonate



Projekttablauf I



Aktivitäten

- Analyse Regulationsanforderungen
- Analyse vorhandener IT-Schutzmaßnahmen
- IT-Strukturanalyse
(Geschäftsfunktionen -> Anwendungen / Daten -> IT-Komponenten)



Projekttablauf II



Aktivitäten

- Festlegung der Schutzbedarfsklassen für IT-Anwendungen und IT-Komponenten
- Workshop zur Ermittlung des Schutzbedarfs
- Übertragung des Schutzbedarfs auf IT- und Netzkomponenten

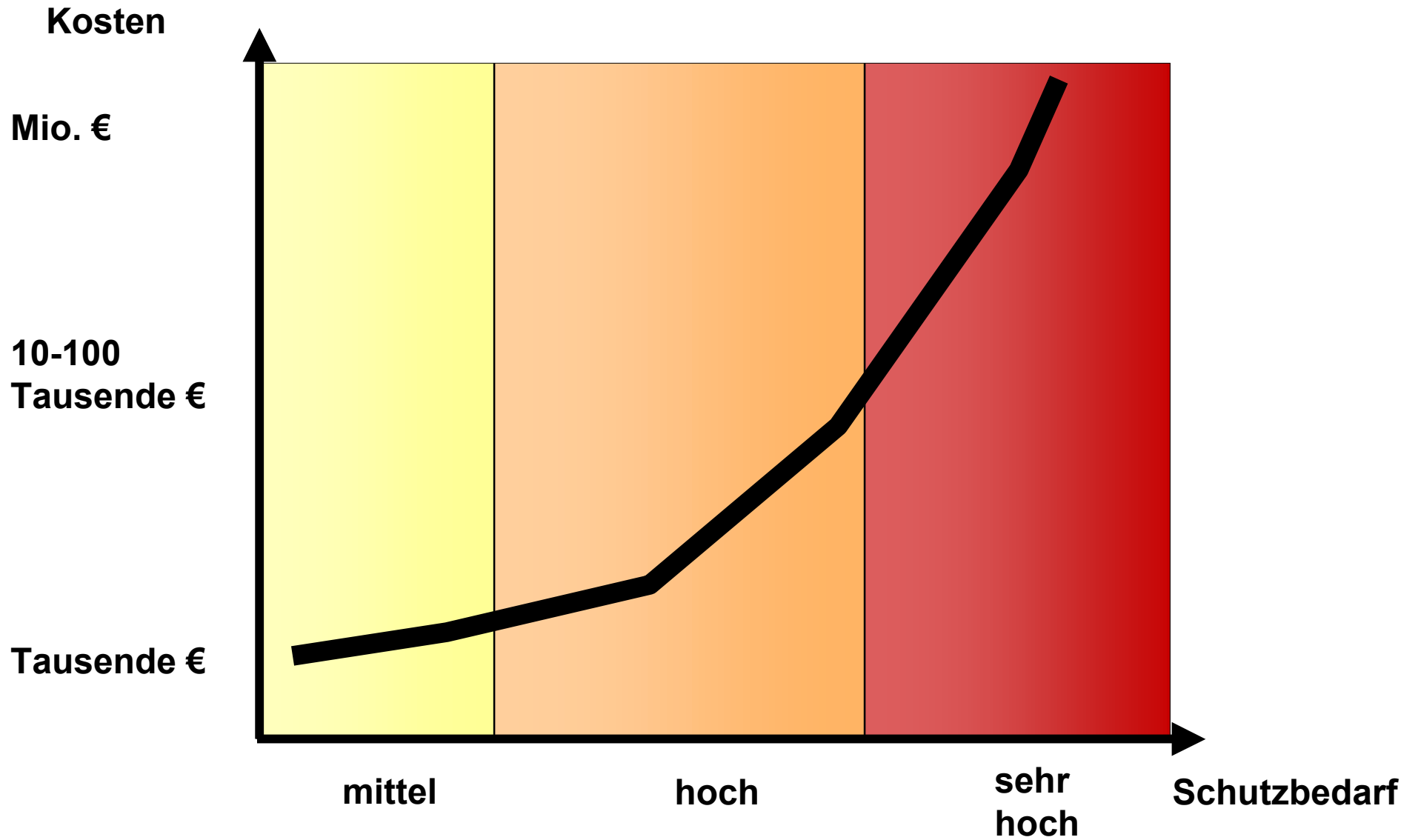


Schutzbedarfsklassen

Klasse	mittel	hoch	sehr hoch
Schadensbetrachtung			
Beeinträchtigung des Geschäftsablaufs	Betriebsbehinderung	deutliche Einschränkung	existenzbedrohende Handlungsunfähigkeit
negative Außenwirkung/ Wettbewerbsnachteile	Beschwerden, evtl. Kundenverluste	erhebliche Kundenverluste	existenzbedrohende Marktverluste
direkte finanzielle Auswirkungen	Geringe - spürbare Beträge	erhebliche Bilanzauswirkung	existenzbedrohend / Konkurs
Verstoß gegen Gesetze / Vorschriften / Verträge	geringe - spürbare Strafen u. Haftungsschäden	hohe Strafen u. Haftungsschäden	existenzbedrohende Strafen u. Haftungsschäden
Versorgungsengpässe, Störungen der öffentlichen Sicherheit usw.	Kurzfristige noch tolerierbare Einschränkung / kein wahrnehmbarer Schaden	Nachhaltige spürbare Einschränkung / spürbarer Schaden	Nachhaltige erhebliche Einschränkung / deutlich wahrnehmbarer Schaden
Anforderungen			
Verfügbarkeit - Hardwareausfälle - im täglichen Betrieb	Mittlere Ausfallzeit <= 48h max. Datenverlust >= 24h	Mittlere Ausfallzeit <= 24h max. Datenverlust 24h	Mittlere Ausfallzeit <= 4h ohne Datenverlust
Vertraulichkeit	Technische und organisatorische Grundschutzmaßnahmen	Erweiterte Schutzmaßnahmen	Technische und organisatorische Maximalmaßnahmen auf Grundlage einer detaillierten Risikoanalyse
Integrität			

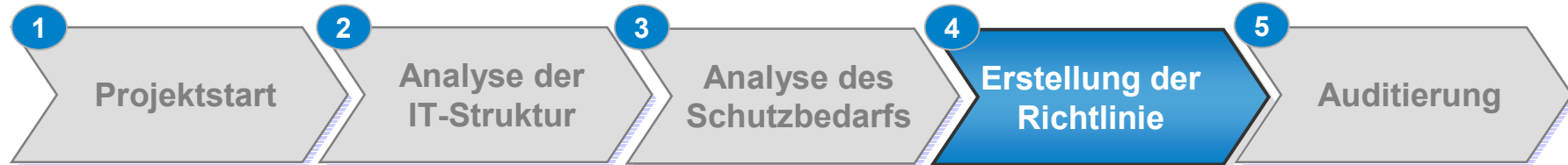


Kosten der Absicherung





Projekttablauf III

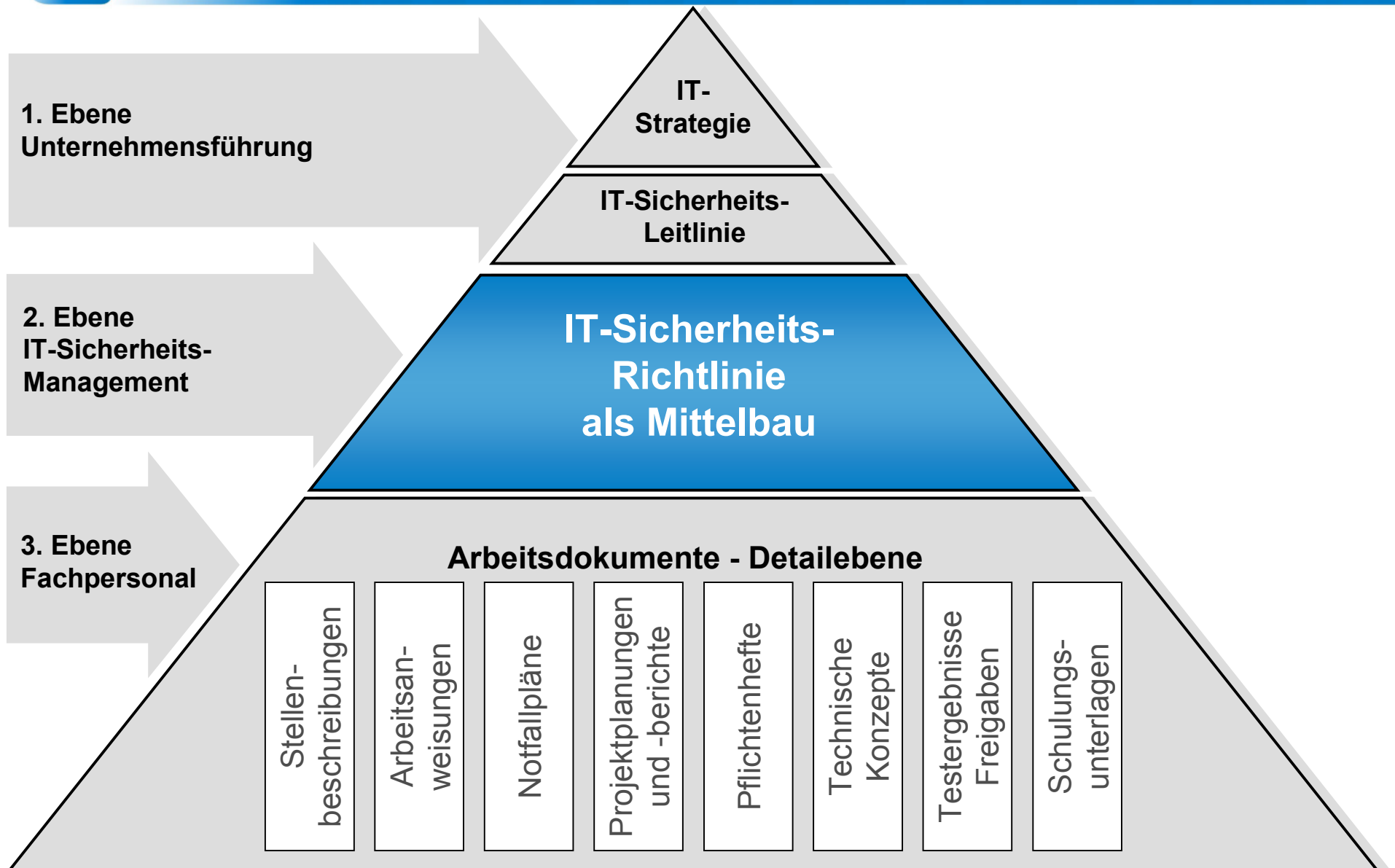


Aktivitäten

- Ausarbeitung von Struktur und Regeln
- Zuweisung von Verantwortungsträgern für Regeln
- Verweise auf vorhandene IT-Sicherheits-Dokumentation einarbeiten
- Review
- Freigabe



Dokumentations-Modell IT-Sicherheit





IT-Sicherheits-Richtlinie: Gliederung

- 1 Einleitung**
- 2 Regeln zu Organisation und Personal**
Leitungsaufgaben, Rollen, Personalpolitik
- 3 Regeln für IT-relevante Steuerungs- und Verwaltungsprozesse**
Risikomanagement, Change Mgm, Notfallplanung ...
- 4 Regeln für Fachbereiche zum Umgang mit der IT**
Genereller Umgang mit der IT, sensible Informationen
- 5 Regeln für die Administration der IT-Infrastruktur**
Datennetzwerke, Server, Arbeitsplatz-PCs
- 6 Regeln zur räumlichen Infrastruktur und für Versorgungseinrichtungen für die IT**
Perimeterschutz, Brandschutz, Stromversorgung
- 7 Sicherheitsrelevante Objektklassen**
Schutzbedarfsklassen, Informationsklassen, Raumklassen ...
- 8 Zuordnung von Verantwortlichkeiten und Aufgaben**
- 9 Weiterführende Dokumentation**



IT-Sicherheits-Richtlinie: Textbeispiel I

2.3 Steuerung von IT-Risiken (RIS)

Die Steuerung von Risiken, die durch den Einsatz von IT bedingt sind, ist Teil des operationellen Risikomanagements. Die besondere Natur der IT und ihr hoher Stellenwert für das Unternehmen erfordern spezielle Steuerungsprozesse.

RIS010

Die Steuerung der IT-Risiken ist in das operationelle Risikomanagement des Unternehmens integriert.

RIS020

Der Schutzbedarf von IT-Anwendungen, –Daten und –Komponenten ist analysiert und dokumentiert.

RIS030

Bei größeren Änderungen in der technischen IT-Infrastruktur und dem Einsatz von IT wird der Schutzbedarf für die betroffene IT neu analysiert und die Dokumentation ggf. aktualisiert.

RIS040

IT-Anwendungen, –Daten und -Komponenten, deren Schutzbedarf sehr hoch eingestuft ist, werden einer detaillierten Risikoanalyse unterworfen.

Die individuelle Risikolage solcher IT-Anwendungen, –Daten und –Komponenten kann Maßnahmen erforderlich machen, die über die in der Sicherheitsrichtlinie niedergelegten Regeln hinausgehen.



IT-Sicherheits-Richtlinie: Textbeispiel II

IT1070

Nicht benötigte Programme und Features von IT-Systemen, die bezüglich eines oder mehrerer der Schutzziele (Verfügbarkeit, Vertraulichkeit und Integrität) der Schutzbedarfsklasse **SBK hoch** oder **SBK sehr hoch** zugeordnet sind, werden nach Möglichkeit gesperrt oder entfernt.

Auf Windows XP-Rechnern sollte die Sperrung bzw. die Entfernung zahlreicher Dienste in Betracht gezogen werden wie z.B. IIS Services, Alerter, Computer Browser, Error Reporting Service, Messenger, Remote Registry Service, Server, SNMP.

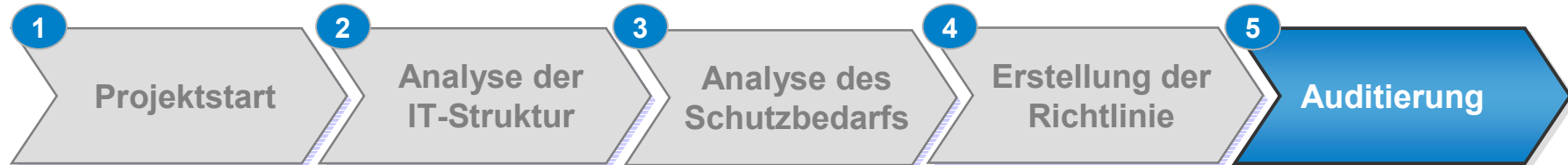
Auf Routern sollte z.B. die Sperrung von Zugriffsmöglichkeiten per HHTP, Finger, RCP, RSH, TELNET, SNMP erwogen werden. Darüber hinaus sollten risikobehaftete Leistungsmerkmale wie z.B. das Source Route Feature abgeschaltet werden.

VS1030

Datenträger, die Daten der Klassen **IK intern**, **IK vertraulich** oder **IK Kundendaten** enthalten oder enthalten haben, werden so entsorgt, dass Unbefugten Zugriff auf die dort gespeicherten Daten nicht möglich ist.



Projekttablauf IV



Aktivitäten

- Erstellung der Audit-Fragebögen
- Auditierung (Interviews)
- Auswertung und Review der Ergebnisse



Auszug Audit-Fragebogen

UH **EDV-Orga User Help Desk**

100% beantwortet

Gemittelte Bewertung des Sicherheitsniveaus

8,7 **kritisch**

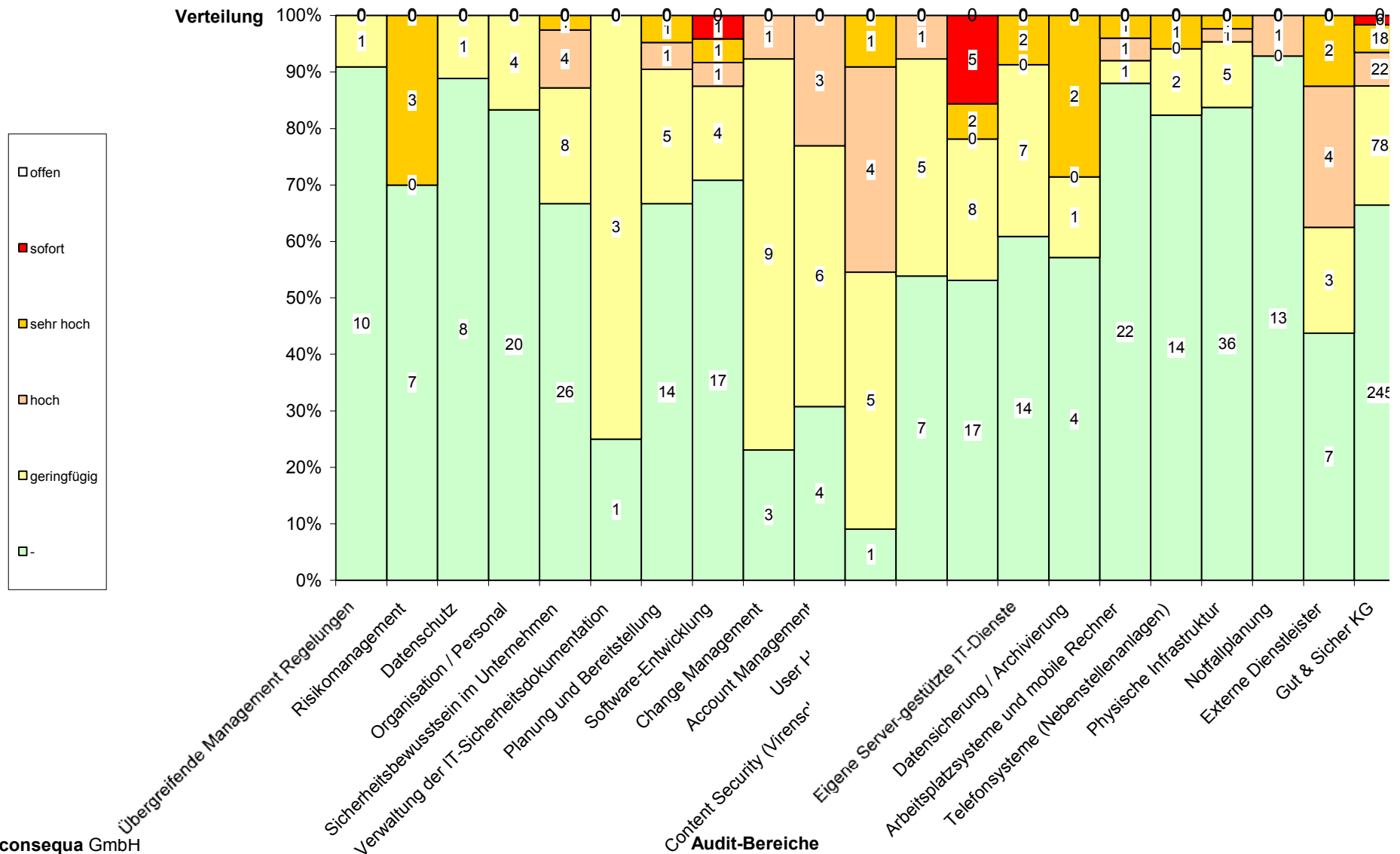
Regel Nr.	Kommentare	Bewertungsfrage	Priorität	Prüfmethode	Erfüllungsgrad	Erläuterung	Handlungsbedarf	HB-Wert	Empfohlene Maßnahme
ICM030		Vorfälle, für deren Bearbeitung andere Stellen herangezogen werden müssen, werden zeitnah an definierte Second- bzw. Third-Level-Einrichtungen weitergegeben. Der Bearbeitungsstand wird regelmäßig überprüft.	6		Vollständig 0			0	
ICM010		Vorfälle werden gemäß festgelegter Bewertungsstufen und -kriterien danach klassifiziert, wie kritisch sie für das Unternehmen sind.	6		In einigen Teilen 2	Derzeit existieren keine klaren Kriterien, nach denen eine Kritikalitätseinstufung erfolgt.	hoch	12	Richtlinien zur Kritikalitätseinstufung in der Arbeitsanweisung UHD ergänzen.
ICM020		Bei kritischen Vorfällen werden folgende Personen zeitnah benachrichtigt und ggf. in den Bearbeitungsprozess mit eingebunden: - der IT-Leiter, - der IT-Sicherheits-Beauftragte, - der Datenschutz-Beauftragte (wenn die Vertraulichkeit personenbezogener Daten gefährdet ist), - alle möglicherweise von dem Vorfall betroffenen Geschäftsfunktionen, - betroffene Partner und IT-Dienstleister.	6		In großen Teilen 1	Verfahren und Kriterien nicht eindeutig festgelegt	geringfügig	6	Eskalationsverfahren in Arbeitsanweisung UHD ergänzen (siehe auch ICM010)
ICM050		Es existiert ein Dokumentationssystem, in dem alle aufgetretenen Vorfälle und die damit verbundenen Untersuchungen und Lösungen erfasst werden.	6		kaum oder gar nicht 3	Vorfälle werden derzeit nicht systematisch aufgezeichnet. Vorfälle, die an den Dienstleister weitgereicht werden, werden dort erfasst. Der Bearbeitungsstand kann jederzeit eingesehen werden.	sehr hoch	18	Einführung eines UHD-Support Tools



Beispiel für Übersichtgrafik

Rückspung

Übersicht Handlungsbedarf Gut & Sicher KG



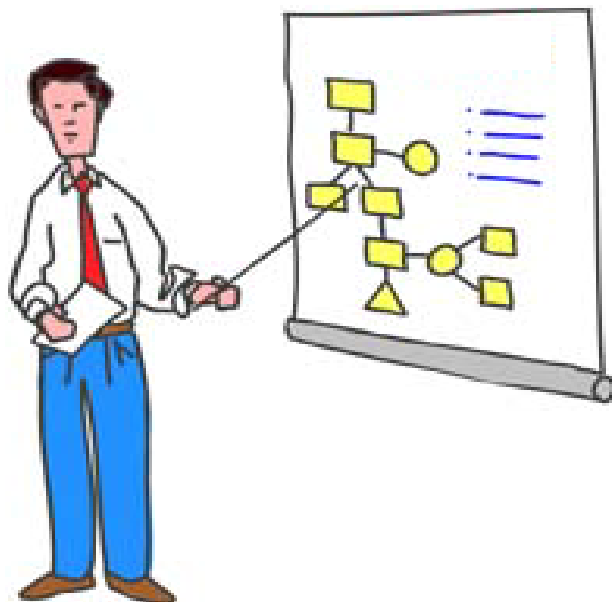


Projektergebnisse

- Richtlinie - konsistente, vollständige Dokumentation der Sicherheitsanforderungen für den gesamten IT-Lebenszyklus:
 - unter Beachtung relevanter Standards auf die Voraussetzungen und Bedürfnisse des Unternehmens zugeschnitten
 - berücksichtigt organisatorische und technische Aspekte
 - kurze, verständliche Texte
 - klar identifizierbar (ID)
 - keine technischen, organisatorischen Details
 - legt fest, was zu dokumentieren ist
 - legt fest, wer verantwortlich ist
 - Audit – Soll / Ist-Vergleich
 - zeigt Handlungsbedarf auf
 - festgelegte Maßnahmen und Verantwortlichkeiten
 - Sensibilisierung
- Erleichterung der Prüfbarkeit



Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Ing.

Stefan Gunzelmann

Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 63
Fax: 040 / 78 89 70 66

stefan.gunzelmann@consequa.de



USA	
<ul style="list-style-type: none">• Department of Homeland Security (DHS)<ul style="list-style-type: none">• DHS Critical Infrastructure• DHS Research & Technology Information & Infrastructure	http://www.dhs.gov http://www.dhs.gov/dhspublic/display?theme=31 http://www.dhs.gov/dhspublic/display?theme=26
<ul style="list-style-type: none">• Federal Emergency Management Agency	http://www.fema.gov
<ul style="list-style-type: none">• US National Institute of Standards and Technology (NIST)<ul style="list-style-type: none">• NIST Computer Security Ressource Center• NIST National Vulnerabilty Database	http://www.nist.gov/ http://csrc.nist.gov/ http://nvd.nist.gov/
<ul style="list-style-type: none">• Information Sharing and Analysis Centers (ISACs)<ul style="list-style-type: none">• World Wide ISAC• Financial Services ISAC• Information Technology ISAC	http://www.wwisac.com/ http://www.fsisac.com https://www.it-isac.org/
EU	
<ul style="list-style-type: none">• European Network and Information Security Agency (ENISA)	http://www.enisa.eu.int/
Deutschland	
<ul style="list-style-type: none">• Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	http://www.bbk.bund.de
<ul style="list-style-type: none">• BSI / KRITIS	www.bsi.de/fachthem/kritis/index.htm