Checkliste zur Informations-Sicherheit

Verlässliche Zahlen zu Risiken, Angriffen und dem Stand der Informationssicherheit sind Mangelware. Dabei sind sie eine wesentliche Hilfe, um die eigene Sicherheitslage und neue Bedrohungen richtig einzuschätzen. Alle zwei Jahre fragt die <kes> daher nach Erfahrungen aus der Praxis und möchte mit dem Fragebogen zur Studie gleichzeitig eine Checkliste für Ihre Sicherheit liefern.

Vermissen Sie bisweilen belastbare Zahlen und Fakten zur Lage der Informations-Sicherheit, die unbelastet sind von spezifischen Interessen eines einzelnen Anbieters? Wir auch – deswegen gibt es seit über zwanzig Jahren die <kes>-Sicherheitsstudien. Wie die Anforderungen an die Informations-Sicherheit wandelt sich regelmäßig auch der zugehörige Fragebogen. Neben der Grundlage zur Daten-Erfassung für die Studie kann er daher gleichzeitig jedem Ausfüller als Arbeitshilfe zur Reflexion und Evaluierung seiner eigenen Sicherheitslage dienen.

Im Zuge der aktuellen Überarbeitung hat diese „Checkliste zur Information-Sicherheit“ eine deutliche strukturelle Änderung erfahren: Der Teil A beherbergt auf den ersten Seiten des Fragebogens nunmehr alle abstrakteren Fragen zur Risiko-Bewertung und Sicherheits-Strategie – Teil B enthält vertiefende Fragen zu eingesetzten Mechanismen und Maßnahmen sowie das Kapitel Schulung und Informationsquellen. Grob gesagt betrifft der erste Teil stärker den „Policy-Maker“, der zweite stärker die Security-Administration – Abschnitt 4 (Info und Schulung) darf wohl als Schnittmenge für alle Beteiligten gelten.

Neben einer klareren Struktur möchten wir mit dieser Gliederung einerseits eine leichtere Arbeitsteilung beim Ausfüllen des Fragebogens durch mehrere Mitarbeiter ermöglichen. Zum anderen können Sie bei Bedarf auch „inhouse“ verschiedene Meinungen zu den Risiko-Fragen sammeln oder differierende Wahrnehmungen verschiedener Beteiligter aufdecken. Und nicht zuletzt: Wer wirklich keine Möglichkeit hat, sich mit dem vollständigen Fragebogen zu beteiligen, kann sich nun auf Teil A beschränken und dennoch mitmachen.

Wie immer erhalten alle Teilnehmer die veröffentlichte Auswertung frei Haus und zudem exklusiven Online-Zugriff auf die tabellarische Auswertung *aller* Fragen sowie ein kleines Dankeschön-Geschenk (siehe Seite 82).

So gehts

_____ Die Teilnahme ist nicht vom Kauf oder Abonnement der Zeitschrift <kes> abhängig.

_____ Sie können den Fragebogen aus dem Heft heraustrennen oder fotokopieren. Sollten Sie die Studie weiterempfehlen mögen: Auf www.kes.info/studie2008/ liegt eine PDF-Version des Fragebogens zum Download bereit.

_____ Behalten Sie bitte eine Kopie ihres ausgefüllten Fragebogens. Sie dient zum Vergleich mit der Gesamtauswertung und als Checkliste des eigenen Sicherheits-Levels.

_____ Einsendeschluss: 1. Mai 2008

_____ **Ich garantiere mit meinem Namen absolute Vertraulichkeit.** Unmittelbar nach Eingang entfernen wir vom Fragebogen den Coupon mit Ihrer Adresse. Nur der Frageteil geht direkt und ohne Kennzeichnung zur Auswertung. Nach dem Erfassen werden die eingesandten Bögen vernichtet.

_____ Sollten Sie die Anonymität selbst sicherstellen wollen, können Sie Coupon und Fragebogen auch getrennt einsenden. Bitte beachten Sie dazu die Hinweise auf den Seiten 81 und 82.

_____ Falls Sie trotz allem befürchten, dass Ihnen eine korrekte Antwort auf bestimmte Fragen oder Fragenteile schaden könnte, streichen Sie bitte die entsprechende Alternative oder Frage großflächig durch. Dies liefert uns bei der Auswertung wertvolle Hinweise auf problematische Fragen.

Peter Hohl, <kes>-Herausgeber

Wir danken den Sponsoren unserer Studie

Microsoft

D-TRUST WE DEFINE SECURITY

GeNUA

F.-J. Lang IT-Security Consulting GmbH

eset DATSEC DATA SECURITY

it.sec security for your information

phion

ROG

TRUST

Jürgen Jakob Software-Entwicklung

AVG Anti-Virus

secunet

entrada IT-Security

TESIS SYSware

EUROSEC

KPMG

Für zusätzliche Anregungen und Hinweise bedanken wir uns beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Weiterhin gilt unser Dank den Verbänden und Anwendervereinigungen, die den Fragebogen der Studie ihren Mitgliedern zugänglich machen sowie schon jetzt allen Teilnehmern an der Befragung, die durch ihre wertvolle Mitarbeit ein sinnvolles Gesamtbild entstehen lassen.

Hinweise zum Ausfüllen

Seit 2004 erscheint unser Fragebogen in neuer Aufmachung. Außer den „Zebra-Streifen" soll Ihnen auch die Form und Gruppierung der Kästchen beim Ausfüllen eine Hilfe sein. **Kreise** kennzeichnen dabei **alternative Antwortmöglichkeiten:** Von allen durch eine Linie verbundenen Kreisen sollten Sie **nur eine Option** ankreuzen, gegebenenfalls wählen Sie bitte die passendste Antwort (s. etwa Frage 1.02: pro Zeile ist nur eine Notenstufe möglich). Die Abkürzung „**n. b.**" steht dabei für „**nicht beantwortbar**" oder „nicht beantwortet".

Quadratische Kästchen kennzeichnen hingegen Fragen, bei denen **Mehrfachnennungen** vorgesehen sind. Teilweise sind mehrere Kästchen durch eine Umrandung gruppiert, wenn sie ein logisches Gegengewicht zu anderen Optionen bilden (vgl. Frage 2.04 b: eine oder mehrere „eingesetzte Methodiken" schließen „keine Methodik" aus).

Für weitere Fragen zu den Fragen oder Antwortmöglichkeiten sowie Anregungen und Kritik haben wir die spezielle Mail-Adresse studie@kes.info eingerichtet. Auf www.kes.info/studie2008/ werden wir zudem bei Bedarf eine FAQ-Sammlung pflegen.

Fragebogen für die <kes>/Microsoft-Sicherheitsstudie 2008

Im Folgenden bitten wir Sie um eine Reihe von Angaben zum Stand der Informationssicherheit (ISi). Wenn diese Angaben nicht genau oder nicht aktuell verfügbar sind, bitten wir Sie um eine Schätzung. Wenn Sie eine Frage nicht beantworten möchten, streichen Sie diese bitte gut sichtbar durch.

1 Aktuelle Risikosituation

1.01 Gefahrenbereiche

a Identifizieren Sie bitte die Gefahrenbereiche, die aus Ihrer Sicht für Ihr Haus gesteigerte Bedeutung haben und daher besondere Priorität erhalten.

b Wie schätzen Sie die zukünftige Entwicklung der Risiken in diesen Gefahrenbereichen für Ihr Haus ein?

c Haben diese Gefahren in Ihrem Haus 2006/2007 tatsächlich zu mittleren bis größeren Beeinträchtigungen geführt?

	a: höchste Priorität	a: erhöhte Priorität	a: normale/keine Priorität	b: abnehmend stark	b: abnehmend etwas	b: gleichbleibend	b: zunehmend etwas	b: zunehmend stark	c: ja	c: nein
• **von Menschen direkt verursachte Gefahren**										
– Irrtum und Nachlässigkeit eigener Mitarbeiter	○	○	○	○	○	○	○	○	○	○
– unbeabsichtigte Fehler von Externen (z. B. Wartungstechniker)	○	○	○	○	○	○	○	○	○	○
– Manipulation zum Zweck der Bereicherung	○	○	○	○	○	○	○	○	○	○
– unbefugte Kenntnisnahme Informationsdiebstahl, Wirtschaftsspionage	○	○	○	○	○	○	○	○	○	○
– Sabotage (inkl. DoS)	○	○	○	○	○	○	○	○	○	○
– Hacking (Vandalismus, Probing, Missbrauch, ...)	○	○	○	○	○	○	○	○	○	○
• **Malware** (Viren, Würmer, Trojanische Pferde usw.)	○	○	○	○	○	○	○	○	○	○
• **technische Defekte/ Qualitätsmängel**										
– hardwarebedingt	○	○	○	○	○	○	○	○	○	○
– softwarebedingt	○	○	○	○	○	○	○	○	○	○
– Mängel der Dokumentation	○	○	○	○	○	○	○	○	○	○
• **höhere Gewalt** (Feuer, Wasser usw.)	○	○	○	○	○	○	○	○	○	○
• **Sonstiges**	○	○	○	○	○	○	○	○	○	○

Bitte nennen Sie gegebenenfalls fehlende Gefahrenbereiche: _____

1.02 Wie schätzen Sie die Informationssicherheit (ISi) in Ihrem Haus ein?

bezogen auf ...	sehr gut	gut	befriedigend	ausreichend	nicht ausreichend	n. b.
• Rechenzentrum/Mainframe	○	○	○	○	○	○
• Server	○	○	○	○	○	○
• Clients/PCs	○	○	○	○	○	○
• mobile Endgeräte (Notebooks, PDAs, ...)	○	○	○	○	○	○
• Teleworking-PCs	○	○	○	○	○	○
• Speichermedien (Tapes, CDs, USB-Speicher, ...)	○	○	○	○	○	○
• IT-Netzwerk (kabelgebunden)	○	○	○	○	○	○
• IT-Netzwerk, drahtlos (WLAN/WiFi/UMTS, ...)	○	○	○	○	○	○
• TK-Netzwerk	○	○	○	○	○	○
• Applikationen/Geschäftsanwendungen	○	○	○	○	○	○

A

1.03 Vertraulichkeitsbrüche

a Haben Unbefugte 2006/2007 über die folgenden Wege Zugriff auf schutzwürdige Daten erlangt?

	ja (gesicherte Erkenntnis)	vermutlich ja	vermutlich nicht	nein (gesicherte Erkenntnis)	n. b.
• Online-Angriff (Hacking, Backdoors, Systemeinbruch, ...)	○	○	○	○	○
• Abhören von Kommunikation (E-Mail, FTP, VoIP, ...)	○	○	○	○	○
• Verlust/Diebstahl mobiler Systeme (Notebook, PDAs, ...)	○	○	○	○	○
• Verlust/Diebstahl von Speichermedien (Backup, USB-Sticks, CDs ...)	○	○	○	○	○
• Einbruch in Gebäude	○	○	○	○	○
• Missbrauch/bewusste Weitergabe durch Berechtigte	○	○	○	○	○
• Social Engineering/Phishing/Unachtsamkeit	○	○	○	○	○
• sonstiger Weg: _____	○	○	○	○	○

b Welche Konsequenzen hatten diese Vorfälle?

	ja	nein	n. b.
• Imageschaden	○	○	○
• verlorene Kunden oder Aufträge	○	○	○
• missbräuchliche Verwendung der Daten durch Dritte	○	○	○
• Sanktionen gegenüber Ihrem Haus oder einem Mitarbeiter (Konventionalstrafe, Bußgeld, Geld- oder Haftstrafe)	○	○	○
• Disziplinarmaßnahmen (Abmahnung, Versetzung, Entlassung, ...)	○	○	○
• Strafanzeige gegen Verursacher (evtl. gegen Unbekannt)	○	○	○
• Sonstige	○	○	○

ggf. bitte benennen: _____

1.04 Malware-Vorfälle

a Hatte Ihr Haus 2007 Vorfälle mit Malware (Viren, Würmer, Trojaner, Spyware usw.)?

○ ja
○ nein

b falls ja: Welche Systeme waren betroffen?

	häufig	selten	nie	n. b.
Server	○	○	○	○
Desktop-PCs/Clients	○	○	○	○
Notebooks	○	○	○	○
PDAs	○	○	○	○
Handys/Smartphones	○	○	○	○

c Tendenz

○ weniger Vorfälle als 2006
○ mehr Vorfälle als 2006
○ n. b.

d Bitte bewerten Sie die Infektionswege für Malware-Vorfälle in Ihrem Haus:

	häufig	selten	nie	n. b.
• Datenträger (CDs, DVDs, USB-Speicher, Diskette, ...)	○	○	○	○
• mobile Systeme (Notebooks, PDAs, Handys)	○	○	○	○
• internes Netz	○	○	○	○
• E-Mail	○	○	○	○
• Internet-Download	○	○	○	○
• Internet (autom. Verbreitung)	○	○	○	○
• WWW-Seite (aktive Inhalte)	○	○	○	○
• unbekannte Herkunft	○	○	○	○

1.05 Häufigkeit und Aufwand von Sicherheitsvorfällen/Fehlalarm

Wie hoch schätzen Sie in Ihrem Haus verursacht durch eine(n) einzelne(n):	**a** Häufigkeit des Auftretens	**b** Ausfallzeit*	**c** Kosten*
• Virus-/Wurm/Trojaner-Infektion	_____ mal/Jahr	_____ Std.	_____ €
• Spyware-Befall	_____ mal/Jahr	_____ Std.	_____ €
• Malware-Fehlalarm (unbegründete Fehlermeldung)	_____ mal/Jahr	_____ Std.	_____ €
• unbegründete Warnung (Hoax)	_____ mal/Jahr	_____ Std.	_____ €
• (erfolgreicher) Online-Angriff	_____ mal/Jahr	_____ Std.	_____ €
• Phishing-Vorfall (inkl. Pharming usw.)	_____ mal/Jahr	_____ Std.	_____ €

*Ausfallzeit = Systemausfallzeit x Anzahl der betroffenen Nutzer
Ausfallzeiten bzw. Kosten bei einem durchschnittlichen Fall

1.06 Beschreiben Sie bitte das größte in den letzten beiden Jahren aufgetretene Schadenereignis:

- auslösendes Ereignis _____
- betroffene Anwendung / Systeme

- Ausfallzeit _____ Stunden
- Kosten _____ €

Wurden in der Folge des Vorfalls	ja	nein	n. b.
• Angriffspunkte beseitigt	○	○	○
• Sicherheitsmechanismen neu eingerichtet	○	○	○
• bestehende Mechanismen verstärkt	○	○	○
• organisatorische Konsequenzen gezogen	○	○	○

1.07 Wenn in Ihrem Haus alle elektronisch gespeicherten Daten vernichtet würden, wie hoch würden Sie den Verlust schätzen? _____ €

(Anhaltspunkt für Ihre Schätzung kann der mögliche Wiederherstellungsaufwand und/oder der Umsatzausfall sein.)

2 ISi-Strategie und -Management

2.01 Gibt es in Ihrem Haus ...?	ja	nein
• eine schriftlich fixierte *Strategie* für die Informations*verarbeitung*	○	○
• eine schriftlich fixierte *Strategie* für die Informations*sicherheit*	○	○
• ein umfassendes, integriertes Sicherheitshandbuch	○	○
• schriftlich fixierte spezifische ISi-*Konzepte/Richtlinien*		
– zur Handhabung sensitiver/kritischer Daten	○	○
– zur Nutzung von Internet, E-Mail, ...	○	○
– zur Nutzung serviceorientierter Architekturen (SOA, inkl. Web-Services, SaaS usw.)	○	○
– zum Softwareeinsatz auf PCs	○	○
– zum Einsatz von Verschlüsselung/elektronischen Signaturen	○	○
– zur Nutzung mobiler Endgeräte (Notebook, PDA, ...)	○	○
– zur Nutzung mobiler Speicher und Plug&Play-Peripherie	○	○
– Sonstige: _____	○	○
• schriftlich formulierte ISi-*Maßnahmen*	○	○

2.02 Wird die (fortdauernde) *Eignung* der Konzepte / Richtlinien überprüft?

a ja ○ nein ○

b falls ja: Diese Prüfung erfolgt mithilfe von ...

- (erneuten) Risikoanalysen ☐
- (erneuten) Schwachstellenanalysen ☐
- Simulationen oder Szenarien ☐
- Übungen (Notfall, Wiederanlauf) ☐
- Penetrationsversuchen ☐
- Sonstigem (bitte nennen): _____ ☐

c Wie lange liegt die letzte Prüfung zurück? _____ Monate

d Welche Reichweite hatte diese Überprüfung?

alle geschäftskritischen Systeme ○ einzelne Systeme ○ nicht bekannt ○

e Führte die letzte Überprüfung zur Aufdeckung von Schwachstellen?

ja ○ nein ○

2.03 Wird die *Einhaltung* vorgesehener Maßnahmen geprüft?

a ja ○ nein ○

b falls ja: Durch wen erfolgt diese Prüfung?

- IT-Abteilung ☐
- eigene ISi-Abteilung ☐
- Datenschutzbeauftragter ☐
- interne Revision ☐
- Geschäftsführung ☐
- externe Berater/Wirtschaftsprüfer ☐
- Sonstige (bitte nennen): _____ ☐

A

2.04 Risikobewertung

a Hat Ihr Haus die Anwendungen / Systeme hinsichtlich ihrer Bedeutung für die Aufgabenerfüllung (Abhängigkeit, Schutzbedarf) sowie der bestehenden Risiken bewertet und klassifiziert?

- ja, für *alle* Anwendungen / Systeme ○
- ja, für *einzelne* Anwendungen / Systeme ○
- nein ○

b falls ja: Welche Methodik setzt Ihr Haus hierbei ein?

falls ja:

- eigene Methodik/Software ☐
- standardisiertes Verfahren (Grundschutz, ISO, ...) ☐
- Verfahren eines Herstellers oder Beraters ☐
- Risikomanagement-Software ☐
- sonstige Methodik: ☐
- kein strikt methodisches Vorgehen ○

c Ist das IT-Risikomanagement in Ihrem Hause in ein allgemeines Risikomanagement des (Gesamt-)Unternehmens eingebunden?

ja ○ nein ○ n. b. ○

2.05 Wie wichtig sind die folgenden Kriterien für die Klassifizierung von Anwendungen / Systemen in Ihrem Haus?

	sehr wichtig	wichtig	unwichtig	n. b.
• direkter finanzieller Schaden an Hardware u. Ä.	○	○	○	○
• direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	○	○	○	○
• Verzögerung von Arbeitsabläufen	○	○	○	○
• indirekte finanzielle Verluste (z. B. Auftragsverlust)	○	○	○	○
• Imageverlust	○	○	○	○
• Verstöße gegen Gesetze / Vorschriften / Verträge	○	○	○	○
• Verstöße gegen interne Regelungen	○	○	○	○
• Schaden bei Dritten / Haftungsansprüche	○	○	○	○
• Sonstiges (bitte nennen): _____	○	○		

2.06 Kennen Sie die folgenden Kriterienwerke?

b falls ja: Welche praktische Bedeutung haben diese Werke für Ihr Haus/Ihre Arbeit?

	a ja	nein	sehr wichtig	weniger wichtig	unwichtig	n. b.
• ITSEC	○	○	○	○	○	○
• Common Criteria	○	○	○	○	○	○
• FIPS 140	○	○	○	○	○	○
• ITIL	○	○	○	○	○	○
• COBIT	○	○	○	○	○	○
• ISO 2700x	○	○	○	○	○	○
• BS 7799 / ISO IEC 17799	○	○	○	○	○	○
• ISO 13335	○	○	○	○	○	○
• IT-Grundschutz	○	○	○	○	○	○
• ISO 900x	○	○	○	○	○	○

c Wurden Teile Ihrer Organisation nach einer oder mehreren dieser Kriterien zertifiziert

ja ○ nein ○

d falls ja: nach welchen Kriterien?

_____

2.07 Systemsicherheit

	ja	nein	
a Setzt Ihr Haus zurzeit sicherheitszertifizierte Produkte ein?	○	○	
b falls ja: Haben sich Ihre Erwartungen an Nutzen und Zuverlässigkeit erfüllt?	○	○	
c Rechtfertigt ein zertifiziertes Produkt Ihrer Meinung nach einen höheren Preis?	○	○	
d Werden Sie in Zukunft sicherheitszertifizierte Produkte bevorzugt einsetzen?	○	○	○ noch unentschieden
e Planen Sie künftig bevorzugt Systeme mit Trusted-Computing-Komponenten einzusetzen?	○	○	○ noch unentschieden

f Sind Sicherheits-Aspekte für Ihr Haus bei der Beschaffung von IT-Systemen ...?

sehr wichtig ○ weniger wichtig ○ unwichtig ○

g Wird die Erfüllung von ISi-Anforderungen als Voraussetzung für die Inbetriebnahme verifiziert? ○ ja ○ nein

2.08 Welche der folgenden Gesetze/Regelungen sind für Ihr Haus in Bezug auf Schutz- und Sicherheitsproblemstellungen relevant?

	a Kenntnis: inhaltlich bekannt		b Relevanz: relevant		c Umsetzung: bereits erfolgt		
	ja	nein	ja	nein	umfassend	teilweise	gering
• BDSG	○	○	○	○	○	○	○
• TKG/TDSV/TKÜV	○	○	○	○	○	○	○
• TMG	○	○	○	○	○	○	○
• ZKDSG	○	○	○	○	○	○	○
• SigG/SigV	○	○	○	○	○	○	○
• KonTraG	○	○	○	○	○	○	○
• GDPdU	○	○	○	○	○	○	○
• Basel II	○	○	○	○	○	○	○
• Solvency II	○	○	○	○	○	○	○
• SOX	○	○	○	○	○	○	○

Basel II = Baseler Akkord, Eigenkapitalvorschriften für das Kreditgewerbe, BDSG = Bundesdatenschutzgesetz
TKG = Telekommunikationsgesetz, TDSV = Telekommunikationsdienstleistungsunternehmen-Datenschutzverordnung
TKÜV = Telekommunikationsüberwachungsverordnung, TMG = Telemedien-Gesetz
ZKDSG = Zugangskontrolldiensteschutzgesetz, SigG/SigV = Signaturgesetz/-Verordnung
KonTraG = Gesetz zur Kontrolle und Transparenz bei Aktiengesellschaften und publizitätspflichtigen Gesellschaften
GDPdU = Grundsätze zu Datenzugriff und Prüfbarkeit digitaler Unterlagen
Solvency II = EU-Projekt zum Rahmenwerk für die Versicherungsaufsicht, SOX = Sarbanes-Oxley Act

d Wie beurteilen Sie die deutsche Gesetzgebung/Regulierung in Bezug auf ...?

	überzogen	angemessen	unzureichend	n. b.
• Datenschutz	○	○	○	○
• TK-/Internet-Überwachung	○	○	○	○
• Strafgesetze (bzgl. Computer-Kriminalität)	○	○	○	○
• Signaturgesetz	○	○	○	○
• E-Business (Verträge, Haftung, ...)	○	○	○	○
• Risikomanagement	○	○	○	○

2.09 Welche Probleme behindern Sie am meisten bei der Verbesserung der ISi?
(Bitte alle zutreffenden Aussagen ankreuzen)

- ☐ Es fehlt an Bewusstsein und Unterstützung im Top-Management
- ☐ Es fehlt an Bewusstsein beim mittleren Management
- ☐ Es fehlt an Bewusstsein bei den Mitarbeitern
- ☐ Es fehlen die strategischen Grundlagen / Gesamt-Konzepte
- ☐ Es fehlen realisierbare (Teil-)Konzepte
- ☐ Es fehlen geeignete Methoden und Werkzeuge
- ☐ Es fehlt an Möglichkeiten zur *Durchsetzung* sicherheitsrelevanter Maßnahmen
- ☐ Es fehlen verfügbare und kompetente Mitarbeiter
- ☐ Es fehlen geeignete Produkte
- ☐ Anwendungen sind nicht für ISi-Maßnahmen vorbereitet
- ☐ Es fehlt an praxisorientierten Sicherheitsberatern
- ☐ Es fehlt an Geld
- ☐ Die vorhandenen Konzepte werden nicht umgesetzt
- ☐ Die Kontrolle auf Einhaltung ist unzureichend
- ☐ Sonstiges (bitte nennen): _____
- ○ keine

2.10 Wie beurteilen Sie den Kenntnisstand zur ISi in Ihrem Hause?

	sehr gut	gut	befriedigend	ausreichend	nicht ausreichend	n. b.
• Top-Management	○	○	○	○	○	○
• Mittelmanagement	○	○	○	○	○	○
• IT-Sicherheitsfachleute	○	○	○	○	○	○
• Anwender in hochsensitiven Bereichen	○	○	○	○	○	○
• Anwender in weniger sensitiven Bereichen	○	○	○	○	○	○

A

2.11 Stellenwert der ISi im Top-Management

ISi birgt Mehrwert für andere Bereiche (Rationalisierung, Business Enabler, ...)	○
ISi ist ein vorrangiges Ziel der Informationsverarbeitung	○
ISi ist ein gleichrangiges Ziel der Informationsverarbeitung	○
ISi ist eher ein „lästiges Übel“	○
n. b.	○

3 Statistische Angaben

3.01 Bitte nennen Sie uns einige Zahlen zur Hardware-Ausstattung Ihres Hauses (ggf. bitte schätzen):

• Mainframes _____	• PDAs/Smartphones _____
• Server _____	• VoIP-Systeme (inkl. Softphones) _____
• Clients/PCs _____	• WAN (inkl. VPN und gemietete Netze) _____
• Heim-/Telearbeitsplätze (auch Teilzeit) _____	• LAN / PC-Netze _____
• Notebooks _____	• WLAN _____

3.02 Zu welcher Branche gehört Ihr Haus?

Energieversorgung	○	Berater	○
Handel	○	Telekommunikationsdienstleister/Provider	○
Handwerk	○	Behörden	○
Transport/Verkehr	○	Outsourcing-Dienstleister	○
Kreditwirtschaft	○	Wissenschaft/Forschung/Schulen	○
Versicherungen	○	Chemische Industrie	○
Verlage/Medien	○	übrige Industrie	○
Gesundheitswesen	○	Sonstiges (bitte nennen): _____	○

3.03 In welchem Land hat Ihr Haus seinen (Haupt-)Sitz?

Deutschland ○ Schweiz ○ Österreich ○ Sonstiges (bitte nennen): _____ ○

3.04 Mitarbeiterzahl

a Wieviele Beschäftigte hat Ihr Haus etwa insgesamt?	_____ Mitarbeiter
b Wieviele Beschäftigte hat die Informationsverarbeitung?	_____ Mitarbeiter IT
c Wieviele Mitarbeiter der Informationsverarbeitung befassen sich speziell mit ISi?	_____ Mitarbeiter ISi

3.05 Funktionsträger

Gibt es in Ihrem Hause ...?

ISi-Beauftragter	☐	Leiter IT / DV / RZ	☐	Leiter Sicherheit/Werkschutz	☐
ISi-Ausschuss (o. Ä.)	☐	IT / DV-Revision	☐	Administratoren	☐
Datenschutzbeauftragter	☐	Leiter Organisation	☐	DV-orientierter Jurist	☐

3.06 Welche Funktionsbezeichnung trifft auf Sie am ehesten zu?

Geschäftsführer	○	RZ-/IT-Leiter	○	IT-Mitarbeiter	○
IT-Sicherheitsverantwortlicher	○	DV-/Orga-Leiter	○	Sonstiges:	○
IT-Sicherheitsadministrator	○	Revisor	○	_____	
Datenschutzbeauftragter	○	Administrator/Systemtechniker	○	_____	

3.07 Der Umsatz bzw. die Bilanzsumme Ihres Hauses betrug im Jahr 2007 ...

(falls nicht bekannt, bitte Angabe für 2006 bzw. das letzte Wirtschaftsjahr)

• _____ € Umsatz • _____ € Bilanzsumme (nur Kreditinstitute / Versicherungen)

• nicht relevant, da Behörde oder ähnliches (bitte ggf. ankreuzen) ☐

3.08 Budget

a Das Budget für Informationsverarbeitung (inkl. Personalkosten)

umfasst im Jahr 2007 _____ € geschätzt ○ ermittelt ○

b Der Anteil für ISi-Maßnahmen (inkl. Personalkosten)

an diesem Budget beträgt _____ % geschätzt ○ ermittelt ○

4 Informationsquellen und Schulung

4.01 Wen informiert/schult Ihr Haus zu Fragen der ISi?	häufig/regelmäßig (min. 1xjährl.)	gelegentlich / zu speziellen Anlässen	nie	n. b.
• Benutzer	○	○	○	○
• freie/externe Mitarbeiter	○	○	○	○
• IT-/DV-Mitarbeiter	○	○	○	○
• Datenschutzbeauftragte	○	○	○	○
• ISi-Beauftragte	○	○	○	○
• Revisoren, Prüfer	○	○	○	○
• Management	○	○	○	○
• andere	○	○	○	○

4.02 Welche Ausbildungsmethoden setzt Ihr Haus auf dem Gebiet der ISi bevorzugt ein?	häufig	gelegentlich	nie	n. b.
• interne Schulungen	○	○	○	○
• externe Schulungen	○	○	○	○
• Materialien (Unterlagen, CDs/DVDs) zum Selbstlernen	○	○	○	○
• Online-Trainings-Anwendungen/-Tools	○	○	○	○

4.03 Berufszertifikate

a Für wie bedeutsam bzw. aussagekräftig halten Sie ...?	sehr wichtig	weniger wichtig	unwichtig	n. b.
• herstellerspezifische Zertifikate zur Aus-/Weiterbildung (z. B. MCSE, CCNE, ...)	○	○	○	○
• herstellerunabhängige Zertifikate zur Aus-/Weiterbildung (z. B. CISSP, CISM, ...)	○	○	○	○

b Welche herstellerunabhängigen ISi-Zertifikate kennen Sie?

• CISA	☐	• CISSP	☐	• IT-Grundschutz-Auditor	☐
• CISM	☐	• SSCP	☐	• Sonstige (bitte ausschreiben):	
• CISO	☐	• TISP	☐	_____	

4.04 Wo informieren Sie sich über ISi?

• CeBIT ☐ • IT-SecurityArea (SYSTEMS) ☐ • Infosecurity ☐ • BSI-Kongress ☐ • ISSE ☐ • Security Essen ☐

• andere Messen / Konferenzen / Kongresse / Seminare	(welche?)	_____
• Zeitschriften / Magazine	(welche?)	_____
• Hersteller-/Anbieter-Dokus (White Paper, Guidelines, ...)	(welche?)	_____
• Internet / WWW / Mailinglisten	(welche?)	_____

_____

4.05 Wo erhalten Sie Informationen über aktuelle Sicherheits-Updates?

a	• aktiv vom Hersteller (push)	☐
	• aktiv durch Anbieter (Systemhäuser, Händler ...)	☐
	• aktiv durch Dritte (push, z. B. Mailingliste)	☐
	• auf Informationsseiten des Herstellers (pull)	☐
	• auf Informationsseiten von Dritten	☐

b In welcher Frequenz prüfen Sie passive Kanäle? ○ täglich ○ wöchentlich ○ monatlich ○ quartalsweise ○ seltener/unregelmäßig ○ gar nicht

c Welche ISi-Bulletins haben Sie abonniert? ☐ Microsoft ☐ Symantec ☐ CERT-Bund ☐ US-CERT.gov ☐ SANS.org ☐ heisec.de

Sonstige: _____

4.06 Qualität von Herstellerinformationen	sehr gut	gut	befriedigend	ausreichend	nicht ausr.	n. b.
a Umfang/Vollständigkeit	○	○	○	○	○	○
b Verständlichkeit	○	○	○	○	○	○
c Geschwindigkeit	○	○	○	○	○	○

B

5 Methoden und Maßnahmen

5.01 Welche der folgenden Maßnahmen sind in Ihrem Haus realisiert/geplant?

	a Server/ Zentrale			**b** Clients/ Endstellen			**c** mobile Endgeräte (Notebooks, PDAs)		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
• Firewalls	○	○	○	○	○	○	○	○	○
• Intrusion Detection/Prevention Systems	○	○	○	○	○	○	○	○	○
• Netzwerkzugangskontrolle (EAP, NAC, ...)	○	○	○	○	○	○	○	○	○
• Schnittstellenüberwachung/-schutz (USB, ser., par., Bluetooth, ...)	○	○	○	○	○	○	○	○	○
• Durchgängige Benutzerverwaltung (Identity-Lifecycle-Management)	○	○	○	○	○	○	○	○	○
• Authentifizierung									
– Hardware-Token	○	○	○	○	○	○	○	○	○
– Passwort	○	○	○	○	○	○	○	○	○
– Chipkarte	○	○	○	○	○	○	○	○	○
– biometrische Verfahren	○	○	○	○	○	○	○	○	○
– SSL-Zertifikate	○	○	○	○	○	○	○	○	○
• Security-Event-Management (Protokollierung/Auswertung)	○	○	○	○	○	○	○	○	○
• zentralisiertes System-/Patch-Management	○	○	○	○	○	○	○	○	○
• zentralisiertes Schwachstellen-Management (Vulnerability-Mgmt.)	○	○	○	○	○	○	○	○	○
• Malware-/Spyware-Abwehr	○	○	○	○	○	○	○	○	○
• Spam-Abwehr	○	○	○	○	○	○	○	○	○
• Content-Inspection/Filtering (Adress-/Inhaltsfilter eingehend)	○	○	○	○	○	○	○	○	○
• Data Leak Prevention (Inhaltskontrolle abgehend)	○	○	○	○	○	○	○	○	○
• Verschlüsselung/VPN									
– sensitive Dateien	○	○	○	○	○	○	○	○	○
– Festplatten (komplett/partitionsweise)	○	○	○	○	○	○	○	○	○
– mobile Speicher (USB, Firewire usw.)	○	○	○	○	○	○	○	○	○
– Archivdatenträger/Backups	○	○	○	○	○	○	○	○	○
– drahtlose Peripherie (Funktastatur, Bluetooth, ...)	○	○	○	○	○	○	○	○	○
– LAN / Intranet-Verbindungen	○	○	○	○	○	○	○	○	○
– WLAN-Verbindungen	○	○	○	○	○	○	○	○	○
– WAN / Internet-Verbindungen	○	○	○	○	○	○	○	○	○
– mobile Verbindungen (UMTS, Hotspots usw.)	○	○	○	○	○	○	○	○	○
– Telefon / Fax	○	○	○	○	○	○	○	○	○
– Voice over IP (VoIP)	○	○	○	○	○	○	○	○	○
– E-Mail	○	○	○	○	○	○	○	○	○
• Datensicherung (Backup)	○	○	○	○	○	○	○	○	○
• Langzeit-Archivierung	○	○	○	○	○	○	○	○	○
• Physische Sicherheit									
– Zutrittskontrolle, biometrisch	○	○	○	○	○	○			
– Zutrittskontrolle, sonstige	○	○	○	○	○	○			
– Bewachung	○	○	○	○	○	○			
– Video-Überwachung	○	○	○	○	○	○			
– Einbruchmeldesysteme	○	○	○	○	○	○			
– Schutz von Glasflächen gegen Durchbruch / Durchwurf	○	○	○	○	○	○			
– Sicherheitstüren	○	○	○	○	○	○			
– Brandmeldesysteme	○	○	○	○	○	○			
– Löschanlagen	○	○	○	○	○	○			
– andere Meldesysteme (z. B. Gas, Staub, Wasser)	○	○	○	○	○	○			
– Datensicherungsschränke/-räume	○	○	○	○	○	○			
– Schutz gegen kompromittierende Abstrahlung (TEMPEST)	○	○	○	○	○	○	○	○	○
– Maßnahmen gegen Hardwarediebstahl	○	○	○	○	○	○	○	○	○
• physikalisches Löschen von Datenträgern	○	○	○	○	○	○	○	○	○
• Unterbrechungsfreie Stromversorgung (USV)	○	○	○	○	○	○	○	○	○
• Überspannungsschutz für Stromleitungen	○	○	○	○	○	○	○	○	○
• Überspannungsschutz für Daten-/IT-Leitungen	○	○	○	○	○	○	○	○	○
• Klimatisierung	○	○	○	○	○	○			
• Rückrufautomatik bei Modemzugriff	○	○	○	○	○	○	○	○	○
• Reserve-Netzzugang (IT/TK) zur Ausfallüberbrückung	○	○	○	○	○	○	○	○	○

5.02 Segmentierung

a Gibt es in Ihrem Haus Daten, die als besonders sensitiv klassifiziert sind (z. B. Verschlusssachen, bes. Geheimhaltung usw.)?

- ja ○
- nein ○

b Gibt es in Ihrem Haus Bereiche, die als besonders risikobehaftet oder gefährdet klassifiziert sind (z. B. aufgrund von Publikumsverkehr, Produktionsumgebungen usw.)?

- ja ○
- nein ○

c falls ja (bei a oder b): Werden klassifizierte Systeme und Daten speziell abgeschottet?

- ☐ ja, durch Netzwerkmechanismen (VLAN, NAC usw.)
- ☐ ja, durch allgemeine Sicherheitssysteme (Firewalls usw.)
- ☐ ja, durch spezielle Systeme für eingestufte Daten
- ☐ ja, durch vollständige physische Trennung vom allgemeinen Hausnetz
- ○ nein, es erfolgt keine Sicherung gegenüber dem allgemeinen Hausnetz

5.03 Welche Internetnutzung gestattet Ihr Haus den Mitarbeitern?

	a geschäftliche Nutzung von Multimedia, „Web 2.0“	WWW	E-Mail	**b** private Nutzung gestattet
• für alle Mitarbeiter	○	○	○	○
• für spezielle Mitarbeiter/Abteilungen/Bereiche	○	○	○	○
• nur an ausgewählten Arbeitsplätzen	○	○	○	○
• generell nicht gestattet	○	○	○	○
• n. b.	○	○	○	○

c Nutzt Ihr Haus ein Berechtigungskonzept für aktive Inhalte (JavaScript, ActiveX, Java, Flash usw.) im Web-Browser (IE-Zonenmodell, URL-basierte Beschränkungen)? ja ○ nein ○

d Werden diese Berechtigungen zentral gesteuert (z. B. per Gruppenrichtlinie) ja ○ nein ○ n. b. ○

5.04 Protokolldateien und -auswertung

a Welche Log-Daten wertet Ihr Haus aus?	regelmäßig	anlassbezogen	nie	n. b.	**b** falls regelmäßig: alle...
• Anti-Virus-Lösungen	○	○	○	○	_____ Tage
• Firewall(s)	○	○	○	○	_____ Tage
• Intrusion Detection/Prevention Systems	○	○	○	○	_____ Tage
• Netzkomponenten (Router, Switches etc.)	○	○	○	○	_____ Tage
• Betriebssysteme	○	○	○	○	_____ Tage
• Web-/E-Commerce-Applikationen	○	○	○	○	_____ Tage
• sonstige Applikationen: _____	○	○	○	○	_____ Tage

c Eine Zusammenfassung und übergreifende Auswertung im Rahmen eines zentralen Security-Event-Managements ist ... realisiert ○ geplant ○ nicht vorgesehen ○

5.05 Multi-Vendor-Strategie

Nutzen Sie aus Sicherheitsgründen auf verschiedenen Systemen oder Netzwerksegmenten Produkte mehrerer verschiedener Anbieter?	Einsatz von Produkten von nur einem Anbieter(n)	zweier	von drei o. mehr	n. b.
• Anti-Virus-Software*	○	○	○	○
• Firewalls	○	○	○	○
• Router	○	○	○	○
• Server-Betriebssysteme	○	○	○	○
• Web-Server	○	○	○	○
• Applikations-Server	○	○	○	○
• Sonstiges: _____	○	○	○	○

*(Multi-Engine-Lösungen bitte wie Multi-Vendor angeben)

B

5.06 Open-Source-Software

a Wie schätzen Sie die Sicherheit von Open-Source-Software im Vergleich zu Produkten mit nicht-offengelegtem Quelltext ein? erheblich sicherer ○ etwas sicherer ○ gleich sicher ○ weniger sicher ○ erheblich unsicherer ○ n. b. ○

b Setzt Ihr Unternehmen Open-Source-Software ein?

ja ○

nein ○

c falls ja: Warum?

- aus Kostengründen ☐
- aus Sicherheitsgründen ☐
- Sonstige Gründe (bitte nennen): ☐

_____

d Prüfen/bearbeiten Sie oder Mitarbeiter Ihres Hauses Open-Source-Code?

	häufig	gelegentlich	nie	n. b.
• Prüfungen hinsichtlich der Sicherheit erfolgen	○	○	○	○
• Prüfungen hinsichtlich funktionaler Aspekte erfolgen	○	○	○	○
• Modifikationen/lokale Anpassungen erfolgen	○	○	○	○

5.07 Content Security (Malware, Spam, Filter)

a Welche Vorsorge gegen Malware hat Ihr Haus getroffen?

	ja	nein	**b Update-Frequenz**
• Wir benutzen Viren-Scanner			
– an der Firewall/Internet-Gateway	○	○	_____ Std.
– auf dem Mail-/File-/Applikations-Server	○	○	_____ Std.
– auf den PCs/Workstations	○	○	_____ Std.
– auf mobilen Systemen	○	○	_____ Std.
• Wir nutzen Online-Virenwächter auf PCs	○	○	
• Isolierte Testumgebung steht zur Verfügung	○	○	

c Welche Funktionen erwarten Sie von einer Content-Security-Lösung?

• Virenschutz ☐	• Spyware-Schutz ☐	• Spam-Abwehr ☐
• Phishing-Abwehr ☐	• Desktop-Firewall ☐	• Inhaltsfilter ☐
• Reporting-Tools ☐	• Monitoring/Alerting ☐	• zentrale Administration ☐

d Wie bewerten Sie Malware-Präventions-Mechanismen, die bereits vor der Verfügbarkeit von Viren-Signaturen-/Pattern-Updates schützen?

sehr wichtig ○ wichtig ○ unwichtig ○

e Der Einsatz einer derartigen Lösung ist... realisiert ○ geplant ○ nicht vorgesehen ○

f Wie hoch ist in Ihrem Unternehmen der Spam-Anteil bei E-Mails?

geschätzt ○ ermittelt ○ _____% Spam

5.08 E-Mail-Sicherheit

a Nutzen Sie in Ihrem Unternehmen E-Mail-Signaturen und Verschlüsselung, sofern der Kommunikationspartner über einen Kryptoschlüssel verfügt?

	Signaturen	Verschlüsselung
• für alle E-Mails	☐	☐
• für externe Kommunikation	☐	☐
• für sensitive Nachrichten	☐	☐
• nie	○	○

b Welchen Standard verwenden Sie dabei?

- S/MIME ☐
- (Open)PGP/GPG ☐
- Sonstige (bitte nennen): ☐

_____

c Der Einsatz einer „virtuellen Poststelle“ (Ver-/Entschlüsselung und/oder Signaturerstellung/-prüfung am Gateway/Server) ist ...

realisiert ○ geplant ○ nicht vorgesehen ○

5.09 Welche Infrastruktur nutzt Ihr Haus für digitale/elektronische Signaturen?

	realisiert	geplant	nicht vorgesehen
• nur Software	○	○	○
• Hardwaremodule (HSM)	○	○	○
• Hardware-Token	○	○	○
• Chipkarten	○	○	○
• „Klasse-2"-Chipkartenterminal (sichere PIN-Eingabe)	○	○	○
• „Klasse-3"-Chipkartenterminal (mit eigenem Display)	○	○	○
• laut Signaturgesetz			
– fortgeschrittene Signatur	○	○	○
– qualifizierte Signatur	○	○	○
– qualifizierte Signatur mit Anbieterakkreditierung	○	○	○
• Sonstiges: _____	○	○	

5.10 Virtual Private Networks (VPNs)

Welche VPN-Verfahren nutzt Ihr Haus?

	realisiert	geplant	nicht vorgesehen	n. b.
• IPsec	○	○	○	○
• SSL	○	○	○	○
• MPLS	○	○	○	○
• Sonstige: _____	○	○		

5.11 Public Key Infrastructure (PKI)

	realisiert	geplant	nicht vorgesehen	n. b.
a Die Implementierung einer PKI ist ...	○	○	○	
b Für welche Zwecke nutzen/planen Sie in Ihrem Haus eine PKI?				
• allgemeine elektronische Signaturen (E-Mail, Dateien usw.)	○	○	○	○
• Code-Signaturen (Software)	○	○	○	○
• Verschlüsselung	○	○	○	○
• Authentifizierung (VPN, SSL, Web-/Remote-Access usw.)	○	○	○	○
• Autorisierung (Zugriffsrechte, Single-Sign-on usw.)	○	○	○	○
• Sonstiges: _____	○	○		

5.12 Identity-Management (IdM)

	realisiert	geplant	nicht vorgesehen	
a Die Implementierung einer IdM-Lösung ist ...	○	○	○	
b Welchen Nutzen versprechen Sie sich vom Einsatz einer IdM-Lösung?	**sehr wichtig**	**wichtig**	**unwichtig**	**n. b.**
• Kostenersparnis (ROI)	○	○	○	○
• Steigerung der Unternehmenssicherheit (Policy Enforcement)	○	○	○	○
• Realisierung einer konsistenten Rechtevergabe	○	○	○	○
• delegierte Administration	○	○	○	○
• hoher Automatisierungsgrad	○	○	○	○
• Compliance	○	○	○	○
• Nachvollziehbarkeit (Revisionierbarkeit)	○	○	○	○
• Sonstiges: _____	○	○		
c Welche Hemmnisse sehen Sie für den Einsatz einer IdM-Lösung?	**sehr problematisch**	**problematisch**	**unproblematisch**	**n. b.**
• technische Komplexität/aufwändige Einführung	○	○	○	○
• organisatorische Komplexität/aufwändige Einführung	○	○	○	○
• hohe Produktkosten	○	○	○	○
• hohe Betriebskosten	○	○	○	○
• Herstellerabhängigkeit	○	○	○	○
• ROI schwer berechenbar/nachvollziehbar	○	○	○	○
• Sonstiges: _____	○	○	○	

5.13 Device-Management

a Wie sichert Ihr Haus Schnittstellen gegen unerwünschte Nutzung?

- ☐ organisatorisch/per Dienstanweisung
- ☐ durch BIOS- oder lokale Betriebssystem-Funktionen
- ☐ durch zentralisierte Funktionen der Betriebssysteme (z. B. Gruppenrichtlinien)
- ☐ durch physische Blockade (Vergießen, Versiegeln, Abklemmen, ...)
- ☐ mit selbstentwickelter Software
- ☐ mit kommerzieller Software
- ○ keine Sicherung vorgesehen

B

Ist es Mitarbeitern erlaubt, folgende *privat* beschafften oder administrierten Systeme mit Unternehmenshardware oder -netzen zu verbinden? Wie wird das technisch überwacht bzw. verhindert?

	b Aufschaltung gestattet			**c** technische Kontrolle		
	ja	nein	n. b.	umfassend	teilweise	keine
• Notebooks, PDAs usw. (LAN/WLAN-Zugang)	○	○	○	○	○	○
• PDAs, Smartphones usw. (Synchronisation mit PCs)	○	○	○	○	○	○
• mobile Speicher (USB, Firewire, Digitalkameras, ...)	○	○	○	○	○	○
• Netzwerkhardware (Switches, WLAN-APs, Modems ...)	○	○	○	○	○	○
• sonstige Peripherie (z. B. Drucker)	○	○	○	○	○	○

5.14 Notfallvorsorge

a Besteht ein EDV-Notfall/-Wiederanlaufkonzept?	**b falls ja: Wurde dieses Konzept schriftlich fixiert?**
ja ○	○ ja
nein ○	○ nein
	○ n. b.

c falls ja: Berücksichtigt dieses Konzept explizit die speziellen Anforderungen für/bei ...?	ja	nein
• Hochverfügbarkeit des E-Business	○	○
• Hardware-Ausfall/-Wiederbeschaffung	○	○
• Software-Sicherheitsvorfälle (Bekanntwerden von Schwachstellen o. Ä.)	○	○
• Viren/Würmer/Exploit-„Epidemien“	○	○
• Denial-of-Service-Attacken	○	○
• gezieltes Eindringen durch Einzeltäter (Hacker, Spionage, ...)	○	○
• physische Einwirkungen (Brand, Naturkatastrophen, Terror, ...)	○	○
• Zusammenbruch externer Infrastrukturen	○	○

d Hält Ihr Haus wesentliche Komponenten seiner Informationsverarbeitung an verschiedenen Orten vor?	• Backup-Datenträger	• gespiegelte Daten	• zus. Rechner/ Cluster
ja, in einem getrennten Brandabschnitt	○	○	○
ja, in einem anderen Gebäude	○	○	○
ja, bei einem Kooperationspartner	○	○	○
ja, bei einem externen Anbieter	○	○	○
nein	○	○	○

Was hat Ihr Haus für längere Ausfälle bereitgestellt?	**e** Unternehmens-server/Mainframe			**f** Abt.-Rechner PC, LAN		
	realisiert	geplant	nicht vor-gesehen	realisiert	geplant	nicht vor-gesehen
• Räume („kalte Lösung“ bzw. „empty shell“)	○	○	○	○	○	○
• Räume mit (wichtiger) Hardware („warme Lösung“)	○	○	○	○	○	○
• Cluster/Load Balancing (mit Überkapazität)	○	○	○	○	○	○
• laufende Systeme („heiße Lösung“)	○	○	○	○	○	○
• konfigurationsidentische Netze	○	○	○	○	○	○
• Ersatzräume für Personal (mit installierter Infrastruktur)	○	○	○	○	○	○
• Ersatzräume für Personal (ohne installierte Infrastruktur)	○	○	○	○	○	○
• Verträge mit externen Dienstleistern/Partnern						
– über die Nutzung von deren Ressourcen (stationäres Ausweich-RZ)	○	○	○	○	○	○
– über die Nutzung von kurzfristig verfügbaren Containern	○	○	○	○	○	○
• Verträge über die schnelle Lieferung von Hardware	○	○	○	○	○	○
• Versicherung abgeschlossen	○	○	○	○	○	○

g falls Sie einen Recovery-Vertrag haben:

Wie oft mussten Sie diesen in Anspruch nehmen? ○ mehrmals ○ einmal ○ nie ○ n. b.

h Existiert in Ihrem Hause eine Notfalldokumentation?	realisiert	geplant	nicht vorgesehen
• manuelles Handbuch (PC-Textsystem, Host-Texte)	○	○	○
• online-gestütztes Handbuch	○	○	○
• Online-Anwendung	○	○	○

i Was umfasst Ihre Dokumentation?	ja	teilweise	nein	n. b.
• Aktionspläne für den Notfall („K-Fall“)	○	○	○	○
• Recovery Units mit				
– Aktionsplan	○	○	○	○
– benötigte Ressourcen (HW, SW etc.)	○	○	○	○
• Aktionspläne Störungen im Tagesbetrieb	○	○	○	○
• IT-Dokumentation (Arbeitsanweisungen)	○	○	○	○
• Allgemeine Dokumentationen	○	○	○	○
• Inventarisierung				
– Hardware	○	○	○	○
– Software	○	○	○	○
– Infrastruktur (Klima etc.)	○	○	○	○

j Welches Produkt setzen Sie dafür ein? _____

k Wie oft wird die Dokumentation aktualisiert? ○ alle ____ Tage ○ anlassbezogen ○ nie ○ n. b.

l Deckt das eingesetzte Produkt die Anforderungen nach ITIL/BSI-Grundschutz ab?	ITIL	BSI	nein	n. b.
	□	□	○	○

m Werden „abgearbeitete“ Pläne zu Revisonszwecken archiviert und können jederzeit wieder eingesehen werden?	ja	nein	n. b.
	○	○	○

5.15 System-Recovery

a Welche Maßnahmen zur Datenrückgewinnung sind für den Fall vorgesehen, dass ein System nicht mehr wie vorgesehen startet oder arbeitet?

- „Bordmittel“ des Betriebssystems (z. B. Systemwiederherstellung) □
- Booten von Rettungs-/Live-CD des Betriebssystemanbieters □
- Booten von Rettungs-/Live-CD eines kommerziellen Drittanbieters □
- Booten von frei erhältlicher Unix-/Linux-Rettungs-/Live-CD □
- Booten von selbst erstellter Rettungs-/Live-CD □
- Wiedereinspielen eines Festplatten-Images bei „ausgespartem“ Datenbereich (bzw. -partition) □
- Wiedereinspielen eines Festplatten-Images unter Inkaufnahme eines evtl. Datenverlusts seit dem letzten Backup □
- Sonstiges: _____ □
- nichts dergleichen ○

b Nutzt Ihr Haus Virtualisierungslösungen, um bei Ausfällen hardware- und ortsunabhängig Ersatz-Systeme in Betrieb nehmen zu können? realisiert ○ geplant ○ nicht vorgesehen ○

5.16 Computer-Forensik

a Wurde in Ihrem Haus 2006/2007 ein Sicherheitsvorfall rechtlich verfolgt?

ja ○
nein ○

b falls nein: Warum?

weil kein Vorfall ○
mangels Verfolgungsinteresse ○
mangels Wissen um Ermittlungsmöglichkeiten ○
n. b. ○

c Wen würde Ihr Haus im Bedarfsfall für forensische Analysen ansprechen?	auf jeden Fall	bevorzugt	normalerweise	nachrangig	keinesfalls	n. b.
• eigene IT-Abteilung	○	○	○	○	○	○
• eigene Revision	○	○	○	○	○	○
• eigene Rechtsabteilung	○	○	○	○	○	○
• externer Rechtsbeistand	○	○	○	○	○	○
• externe Wirtschaftsberatung/-prüfer	○	○	○	○	○	○
• externer, bereits bekannter IT-Dienstleister	○	○	○	○	○	○
• Fachdienstleister für Computer-Forensik	○	○	○	○	○	○
• externes CERT/CSiRT	○	○	○	○	○	○
• BSI	○	○	○	○	○	○
• Strafverfolgung (Polizei, Staatsanwaltschaften)	○	○	○	○	○	○

B

5.17 CERT/CSIRT

a Unterhält Ihr Haus ein *eigenes* Computer Emergency or Security Incident Response Team (CERT/CSIRT)? ja ○ — ○ nein

b Nutzt Ihr Haus Dienstleistungen eines *externen* CERT/CSIRT? ja, kostenpflichtig ○ ja, kostenlos ○ nein ○

c falls ja: Von welchem CERT/CSIRT? _____

5.18 ISi-Beratung

a Nutzt Ihr Haus externe ISi-Beratung?

- ja, häufig ○
- ja, gelegentlich ○
- nein, nie ○

b falls ja: in welcher Form?

- ☐ Strategie- und Managementberatung
- ☐ Durchführung von Inhouse-Schulungen
- ☐ Durchführung von Risikoanalysen und Konzeptentwicklung
- ☐ Durchführung von Schwachstellenanalysen
- ☐ Durchführung von Penetrationstests
- ☐ Umsetzung von Konzepten und Maßnahmen
- ☐ Kontrolle vorhandener Konzepte auf Eignung und Einhaltung
- ☐ Produktberatung und Kaufunterstützung
- ☐ Prozess-Entwicklung und -Optimierung
- ☐ Sonstiges (bitte nennen): _____

c falls ja: Bitte benoten Sie die Beratungsleistungen

sehr gut ○ gut ○ befriedigend ○ ausreichend ○ nicht ausreichend ○ n. b. ○

5.19 Outsourcing?

a Nutzt Ihr Haus Outsourcing? ja ○ nein ○

b falls ja: Welche Funktionen haben Sie ausgelagert?

- ☐ externer ISi-Beauftragter
- ☐ Überwachung, Kontrolle, Qualitätssicherung
- ☐ Managed Firewall/IDS/IPS
- ☐ Content Security/Virenabwehr
- ☐ E-Mail-Betrieb
- ☐ Netzwerk-Management
- ☐ Datensicherung, Backup-Lösungen
- ☐ Dokumentation, Archivierung
- ☐ Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung
- ☐ Betriebssystempflege/Administration
- ☐ gesamte(s) Rechenzentrum/IT
- ☐ Notfallvorsorge/Business Continuity
- ☐ Anwendungssysteme
- ☐ Datenbank-Systeme, Werkzeuge
- ☐ Haustechnik
- ☐ Datenschutz
- ☐ Vernichtung von Datenträgern (Papier, EDV)
- ☐ Wachschutz/Bewachung
- ☐ Sonstiges (bitte nennen): _____

c falls ja: Haben Sie Service-Level-Agreements/ vertragliche Vereinbarungen mit dem Outsourcer? ja ○ nein ○

- mit expliziten Anforderungen an die ISi? ja ○ nein ○
- mit expliziten Anforderungen an den Datenschutz? ja ○ nein ○

d falls ja: Kontrolle erfolgt ...

	regelmäßig	anlassbezogen	nie	n. b.
Haben Sie Service-Level-Agreements/ vertragliche Vereinbarungen mit dem Outsourcer?	○	○	○	○
mit expliziten Anforderungen an die ISi?	○	○	○	○
mit expliziten Anforderungen an den Datenschutz?	○	○	○	○

e falls ja: Bitte bewerten Sie die Outsourcingleistungen

sehr gut ○ gut ○ befriedigend ○ ausreichend ○ nicht ausreichend ○ n. b. ○

5.20 Versicherungen

a Haben Sie spezielle Versicherungen im Hinblick auf IT-Systeme oder Datenhaltung abgeschlossen (außer Feuerversicherung)? ja ○ nein ○

b falls ja: Haben Sie eine oder mehrere dieser Spezialversicherungen bereits in Anspruch genommen? ja ○ nein ○ n. b. ○

c *Mussten* Sie für den Abschluss mindestens einer Versicherung ein ISi-Audit durchlaufen oder ein anerkanntes ISi-Zertifikat vorlegen? ja ○ nein ○

d Bietet mindestens eine Ihrer abgeschlossenen Versicherungen für das Durchlaufen eines ISi-Audits oder die Vorlage eines anerkannten ISi-Zertifikats *günstigere Konditionen* an? ja ○ nein ○

5.21 Anbieter

a Hat Ihr Haus Produkte der folgenden Anbieter *im Einsatz?*

• IBM ☐ • Microsoft ☐ • SAP ☐ • Sun Microsystems ☐ • bel. Linux-System ☐

b Welche der folgenden Unternehmen sind Ihnen als Anbieter von Sicherheitsprodukten bzw. -dienstleistungen *bekannt?*

• Aladdin ☐	• it.sec ☐	• RSG ☐
• AVG Anti-Virus (Jakob Software) ☐	• itWatch ☐	• Safeboot ☐
• Cisco ☐	• Juniper ☐	• SAP ☐
• Defense ☐	• Kaspersky ☐	• Secaron ☐
• Design Institut München (DIM) ☐	• KPMG ☐	• secunet ☐
• Deutscher Sparkassen-Verlag ☐	• Lampertz ☐	• Siemens ☐
• D-Trust ☐	• Microsoft ☐	• SonicWALL ☐
• Entrada ☐	• modulan ☐	• Symantec ☐
• ESET/DATSEC ☐	• PGP ☐	• TESIS SYSware ☐
• Eurosec ☐	• phion ☐	• Trendmicro ☐
• F.-J. Lang ☐	• retarus ☐	• T-Systems ☐
• GeNUA ☐	• Rittal ☐	• Utimaco ☐
• giritech ☐	• ROG ☐	• Websense ☐
• Infinigate ☐	• Rohde & Schwarz SIT ☐	• es fehlen:
• Infodas ☐	• RSA ☐	

c Welchem Hersteller der IT-Branche trauen Sie am ehesten zu, durch technische Innovationen und organisatorische Maßnahmen die drängenden Sicherheitsprobleme effizient und kostengünstig in den Griff zu bekommen?

d Sind Ihnen die folgenden Aufgaben und Dienstleistungen des BSI bekannt?

	ja	nein		ja	nein
• IT-Sicherheitshandbuch	○	○	• kryptographische Grundlagenarbeit	○	○
• Schriften/Faltblätter zur IT-Sicherheit	○	○	• Beratung	○	○
• Leitfaden IT-Sicherheit	○	○	• Grundschutz-Hotline	○	○
• Studien-/Buch-Publikationen	○	○	• GSTOOL	○	○
• BSI-Standards	○	○	• Viren-Hotline	○	○
• Grundschutz-Kataloge	○	○	• Viren-Mailingliste	○	○
• Web-Angebot des BSI	○	○	• Informationsdienst (BSI-Forum in der <kes>)	○	○
• BSI-Newsletter (5-mal/Jahr)	○	○	• BSI-Kongress	○	○
• Zertifizierung	○	○	• Newsletter „sicher • informiert“ (14-tägig)	○	○
• CERT-Bund	○	○	• Angebot „BSI für Bürger“	○	○

Bitte vergessen Sie nicht, auf der nächsten Seite Ihren Absender anzugeben, damit wir Ihnen die Auswertung und Ihr Dankeschön-Geschenk zuschicken können.

So garantieren wir Vertraulichkeit:

- Dieser Abschnitt mit Ihrer Anschrift wird in der <kes>-Redaktion abgetrennt, bevor der Fragebogen zur Auswertung geht. Der Abschnitt dient dazu, den Teilnehmern nach der Auswertung das Ergebnis der <kes>/Microsoft-Sicherheitsstudie zuzusenden.

- Sie können diesen Abschnitt auch selbst abtrennen und getrennt vom anonymen Fragebogen einsenden. Dabei steht Vertrauen gegen Vertrauen: Die <kes>-Redaktion garantiert Ihnen, dass Fragebogen und Abschnitt streng getrennt bleiben. Sie garantieren uns, dass Sie nicht etwa nur den Abschnitt, sondern auch einen ausgefüllten Fragebogen abgeschickt haben.

Herrn Peter Hohl
– persönlich –
Redaktion <kes>
Postfach 1234
55205 Ingelheim

(Anschriftsfeld für Versand im C4-Fensterumschlag)

Ihre „Dankeschön-Prämien"

A

52 neue Wochensprüche „Ein Mittel gegen Einsamkeit . . ." von Peter Hohl

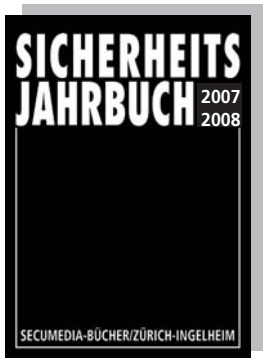
FlammEx Profi, fotoelektronischer Rauchmelder für Zuhause

A+B

Pfeffer-/Salzpumpen-Set – die Einhand-Mühlen von Zweibrüder

Zwei Sprüchebücher „Ein Mittel ..." und „Erfolg ist leicht"

Sicherheitsjahrbuch 2007/2008 – das umfassende Kompendium der Sicherheit



Jeder Teilnehmer der Studie erhält von Microsoft (solange Vorrat reicht) zusätzlich ein so genanntes TSA-Koffer-Schloss, das die US-amerikanische Transportation Security Administration (TSA) bei Kontrollen von aufgegebenem Gepäck mit einem Generalschlüssel zerstörungsfrei öffnen kann.

Ich bin Teilnehmer der <kes>/Microsoft-Sicherheitsstudie 2008

Soweit ich diesen Abschnitt gesondert einsende, versichere ich ehrenwörtlich, dass gleichzeitig ein ausgefüllter Fragebogen von mir eingeschickt wurde. Bitte schicken Sie die Auswertungen und mein Teilnahmegeschenk an folgende Anschrift:

A Ich konnte dieses Jahr leider nur Teil A ausfüllen – ich wünsche mir als Dankeschön

- ○ Rauchmelder für Zuhause
- ○ Buch „Ein Mittel gegen Einsamkeit"

A+B Ich habe den vollständigen Fragebogen ausgefüllt und möchte als Teilnahmegeschenk (bitte nur einen Gegenstand ankreuzen)

- ○ Pfeffer- und Salzmühle
- ○ Sicherheits-Jahrbuch 2007/2008
- ○ Sprüchebücher „Ein Mittel ..." und „Erfolg ist leicht "

Bitte einsenden an: Herrn Peter Hohl persönlich, Redaktion <kes>, Postfach 1234, 55205 Ingelheim

(vorherige Seite ist vorbereitet zum Versand im C4-Umschlag)

Firma / Behörde

Name, Vorname

Straße / Postfach

Land / PLZ / Wohnort

Datum Unterschrift