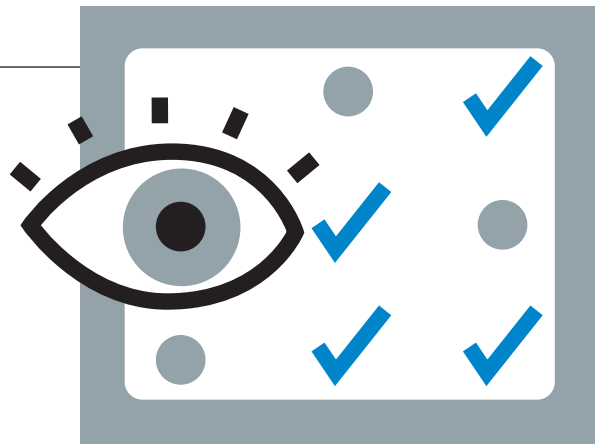


Checkliste zur Informations-Sicherheit



<kes> **Microsoft**
Sicherheitsstudie 2010

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.

Vermissten 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 vorigen 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 90).

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/studie2010/ 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: 15. Mai 2010

_____ **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.

_____ 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®



antispameurope®



itWatch

retarus:
messaging services



secunet



SOPHOS
und utimaco



•• T •• Systems•

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 2.04b: 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/studie2010/ werden wir zudem bei Bedarf eine FAQ-Sammlung pflegen.

Fragebogen für die <kes>/Microsoft-Sicherheitsstudie 2010

Im Folgenden bitten wir Sie um eine Reihe von Angaben zum Stand der Informationssicherheit (ISI).
 Wo 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.
 Sollten Ihnen Antwortoptionen fehlen, ergänzen Sie diese bitte als Randnotiz oder auf einem Beiblatt.

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 2008/2009 tatsächlich zu mittleren bis größeren Beeinträchtigungen geführt?				
	höchste Priorität	erhöhte	normale/ keine	abnehmend stark	gleich- bleibend	zunehmend etwas stark	ja	nein
• von Menschen direkt verursachte Gefahren								
– Irrtum und Nachlässigkeit eigener Mitarbeiter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– unbeabsichtigte Fehler von Externen (z. B. Wartungstechniker)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Manipulation zum Zweck der Bereicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– unbefugte Kenntnisnahme Informationsdiebstahl, Wirtschaftsspionage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Sabotage (inkl. DoS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Hacking (Vandalismus, Probing, Missbrauch, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Malware (Viren, Würmer, Trojanische Pferde usw.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• technische Defekte/Qualitätsmängel								
– hardwarebedingt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– softwarebedingt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Mängel der Dokumentation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• höhere Gewalt (Feuer, Wasser usw.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Sonstiges	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Server	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Clients/PCs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mobile Endgeräte (Net-/Notebooks, Smartphones, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Teleworking-PCs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Speichermedien (Tapes, CDs, USB-Speicher, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• IT-Netzwerk (kabelgebunden)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• IT-Netzwerk, drahtlos (WLAN/WiFi/UMTS, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• TK-Netzwerk (ggf. inkl. VoIP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Applikationen/Geschäftsanwendungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A

1.03 Vertraulichkeitsbrüche

a Haben Unbefugte 2008/2009 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, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Abhören von Kommunikation (E-Mail, FTP, VoIP, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verlust/Diebstahl mobiler Systeme (Notebook, Smartphone, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verlust/Diebstahl von Speichermedien (Backup, USB-Sticks, CDs ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Einbruch in Gebäude	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Missbrauch/bewusste Weitergabe durch Berechtigte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Social Engineering, Phishing, Unachtsamkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b Welche Konsequenzen hatten diese Vorfälle?

• Imageschaden <input type="checkbox"/>	• verlorene Kunden oder Aufträge <input type="checkbox"/>
• missbräuchliche Verwendung der Daten durch Dritte <input type="checkbox"/>	• externe Sanktionen gegenüber Ihrem Haus / Mitarbeiter <input type="checkbox"/>
• personelle Maßnahmen <input type="checkbox"/>	• techn./organisat. Maßnahmen <input type="checkbox"/>
• Strafanzeige gegen Verursacher / Unbekannt <input type="checkbox"/>	• Sonstige <input type="checkbox"/>
• Keine Konsequenzen <input type="checkbox"/>	

1.04 Malware-Vorfälle

a Hatte Ihr Haus 2009 Vorfälle mit Malware (Viren, Würmer, Trojaner, Spyware usw.)?	b falls ja: Welche Systeme waren betroffen?	c Tendenz
<input type="radio"/> ja	Server <input type="radio"/> häufig <input type="radio"/> selten <input type="radio"/> nie <input type="radio"/> n. b.	<input type="radio"/> weniger Vorfälle als 2008
<input type="radio"/> nein	Desktop-PCs/Clients <input type="radio"/> häufig <input type="radio"/> selten <input type="radio"/> nie <input type="radio"/> n. b.	<input type="radio"/> mehr Vorfälle als 2008
	Notebooks <input type="radio"/> häufig <input type="radio"/> selten <input type="radio"/> nie <input type="radio"/> n. b.	<input type="radio"/> n. b.
	Handys/Smartphones/PDAs <input type="radio"/> häufig <input type="radio"/> selten <input type="radio"/> nie <input type="radio"/> n. b.	

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

	häufig	selten	nie	n. b.
• Speichermedien (CDs, DVDs, USB-Speicher, Diskette, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mobile Endgeräte (Net-/Notebooks, Smartphones, PDAs)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• unerwünschte Anwendungen (Download, USB/U3, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• internes Netz / Intranet (Würmer)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Internet (Würmer)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• WWW-Seite (aktive Inhalte, Drive-by-Downloads)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• E-Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• unbekannte Herkunft	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.	_____ €
• Malware-Fehlalarm (unbegründete Fehlermeldung)	_____ mal/Jahr	_____ Std.	_____ €
• unbegründete Warnung (Hoax)	_____ mal/Jahr	_____ Std.	_____ €
• gezielter Angriff auf / über / mit IT	_____ 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 Schadenergebnis:

• auslösendes Ereignis _____	Wurden in der Folge des Vorfalles	ja	nein	n. b.
_____	• Angriffspunkte beseitigt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• betroffene Anwendung / Systeme _____	• Sicherheitsmechanismen neu eingerichtet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
_____	• bestehende Mechanismen verstärkt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Ausfallzeit _____ Std. • Kosten _____ €	• Produkt-/Anbieterwechsel vollzogen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	• organisatorische Konsequenzen gezogen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

(Anhaltspunkte für Ihre Schätzung können 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 <i>Strategie</i> für die Informationsverarbeitung	<input type="radio"/>	<input type="radio"/>
• eine schriftlich fixierte <i>Strategie</i> für die Informationssicherheit	<input type="radio"/>	<input type="radio"/>
• schriftlich fixierte spezifische <i>Isi-Konzepte/Richtlinien</i>		
– zur Handhabung sensibler/kritischer Daten	<input type="radio"/>	<input type="radio"/>
– zur Weitergabe/Bereitstellung von Daten an berechnete Dritte (Partner, Dienstleister, ...)	<input type="radio"/>	<input type="radio"/>
– zur Nutzung von Cloud-/Web-Services (inkl. SOA, SaaS, ...)	<input type="radio"/>	<input type="radio"/>
– zur E-Mail-Nutzung	<input type="radio"/>	<input type="radio"/>
– zur Nutzung von Web 2.0, Social Networks, ...	<input type="radio"/>	<input type="radio"/>
– zur Gestaltung/Nutzung von Passwörtern (Qualität, Wechsel, Mehrfachnutzung)	<input type="radio"/>	<input type="radio"/>
– zum Softwareeinsatz auf PCs	<input type="radio"/>	<input type="radio"/>
– zum Einsatz von Verschlüsselung/elektronischen Signaturen	<input type="radio"/>	<input type="radio"/>
– zur Nutzung mobiler Endgeräte (Net-/Notebooks, Smartphones, PDAs, ...)	<input type="radio"/>	<input type="radio"/>
– zur Nutzung mobiler Speicher und Plug&Play-Peripherie	<input type="radio"/>	<input type="radio"/>
– zur dienstlichen Nutzung privater IT-Systeme	<input type="radio"/>	<input type="radio"/>
– Sonstige: _____	<input type="radio"/>	<input type="radio"/>
• schriftlich formulierte <i>Isi-Maßnahmen</i>	<input type="radio"/>	<input type="radio"/>

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

a	ja, regelmäßig	<input type="radio"/>	b Diese Prüfung erfolgt ggf. mithilfe von ...
ja, anlassbezogen	<input type="radio"/>		• (erneuten) Risikoanalysen <input type="checkbox"/>
nein, nie	<input type="radio"/>		• (erneuten) Schwachstellenanalysen <input type="checkbox"/>
			• Simulationen oder Szenarien <input type="checkbox"/>
			• Übungen (Notfall, Wiederanlauf) <input type="checkbox"/>
			• Penetrationsversuchen <input type="checkbox"/>
			• Sonstigem (bitte nennen): _____ <input type="checkbox"/>

c Wie häufig wurde in den letzten Jahren im Mittel geprüft alle ____ Monate

d Welche Reichweite hatte die letzte Überprüfung?
 alle geschäftskritischen Systeme einzelne Systeme nicht bekannt

e Führte die letzte Überprüfung zur Aufdeckung von Schwachstellen?
 ja nein n. b.

2.03 Wie beurteilen Sie die Übereinstimmung der „gelebten“ Praxis (Ist-Zustand) mit den Konzepten/Richtlinien (Soll-Zustand)?

sehr gut gut befriedigend ausreichend nicht ausreichend n. b.

2.04 Wird die *Einhaltung* vorgesehener Maßnahmen/Richtlinien geprüft?

a	ja <input type="radio"/>	b falls ja: Durch wen erfolgt diese Prüfung?
nein <input type="radio"/>		• IT-Abteilung <input type="checkbox"/>
		• eigene Isi-Abteilung/CSO/CISO/IT-SiBe/ ... <input type="checkbox"/>
		• Datenschutzbeauftragter <input type="checkbox"/>
		• interne Revision <input type="checkbox"/>
		• Geschäftsführung <input type="checkbox"/>
		• externe Berater/Wirtschaftsprüfer <input type="checkbox"/>
		• Sonstige (bitte nennen): _____ <input type="checkbox"/>

c Nutzt Ihr Haus im Hinblick auf vorgesehene Maßnahmen/Richtlinien ...?

	umfassend	teilweise	nein	n.b.
• Software zur kontinuierlichen Überwachung (Policy-Monitoring)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Software zur kontinuierlichen Durchsetzung (Policy-Enforcement)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Kennzahlen, Key-Performance-Indikatoren o. Ä. zur Bewertung der Einhaltung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A

2.05 Risikobewertung

a Hat Ihr Haus seine Anwendungen / Systeme hinsichtlich ihrer Bedeutung für Geschäftsprozesse sowie bestehender Risiken klassifiziert?	b falls ja: Welche Methodik setzt Ihr Haus hierbei ein?
ja, für <i>alle</i> Anwendungen / Systeme <input type="radio"/>	<ul style="list-style-type: none"> <input type="checkbox"/> eigene Methodik/Software <input type="checkbox"/> standardisiertes Verfahren (Grundschutz, ISO, ...) <input type="checkbox"/> Verfahren eines Herstellers oder Beraters <input type="checkbox"/> Risikomanagement-Software <input type="checkbox"/> sonstige Methodik: <input type="checkbox"/> kein strikt methodisches Vorgehen
ja, für <i>einzelne</i> Anwendungen / Systeme <input type="radio"/>	
nein <input type="radio"/>	
c Ist das IT-Risikomanagement in Ihrem Hause in ein allgemeines Risikomanagement des (Gesamt-)Unternehmens eingebunden?	
ja <input type="radio"/> nein <input type="radio"/> n. b. <input type="radio"/>	

2.06 Wie wichtig sind die folgenden Risiken für die Klassifizierung von Anwendungen / Systemen in Ihrem Haus?

	sehr wichtig	wichtig	unwichtig	n. b.
• Verlust oder Schaden von oder an Hardware u. Ä.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verzögerung von Arbeitsabläufen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• indirekte finanzielle Verluste (z. B. Auftragsverlust)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Imageverlust	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verstöße gegen Gesetze / Vorschriften / Verträge	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verstöße gegen interne Regelungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Schaden bei Dritten / Haftungsansprüche	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.07 Stellenwert der ISi im Top-Management

ISi birgt Mehrwert für andere Bereiche (Rationalisierung, Business Enabler, ...)	<input type="radio"/>
ISi ist ein vorrangiges Ziel der Informationsverarbeitung	<input type="radio"/>
ISi ist ein gleichrangiges Ziel der Informationsverarbeitung	<input type="radio"/>
ISi ist eher ein „lästiges Übel“	<input type="radio"/>
n. b.	<input type="radio"/>

2.08 Kennen Sie die folgenden Kriterienwerke?

	a		b falls ja: Welche praktische Bedeutung haben diese Werke für Ihr Haus/Ihre Arbeit?			
	ja	nein	sehr wichtig	weniger wichtig	unwichtig	n. b.
• Common Criteria	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• FIPS 140	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• ITIL	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• COBIT	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• ISO 2700x	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• ISO 13335	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• IT-Grundschutz (nach BSI)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• ISO 900x	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

ja nein

d falls ja: nach welchen Kriterien?

2.09 Systemsicherheit

	ja	nein
a Setzt Ihr Haus zurzeit sicherheitszertifizierte Produkte ein?	<input type="radio"/>	<input type="radio"/>
b falls ja: Haben sich Ihre Erwartungen an Nutzen und Zuverlässigkeit erfüllt?	<input type="radio"/>	<input type="radio"/>
c Rechtfertigt ein zertifiziertes Produkt Ihrer Meinung nach einen höheren Preis?	<input type="radio"/>	<input type="radio"/>
d Werden Sie in Zukunft sicherheitszertifizierte Produkte bevorzugt einsetzen?	<input type="radio"/>	<input type="radio"/>
		noch unentschieden <input type="radio"/>
e Setzen Sie Systeme mit Trusted-Computing-Komponenten (TPM) bevorzugt ein?	<input type="radio"/>	<input type="radio"/>
f Sind Sicherheits-Aspekte für Ihr Haus bei der Beschaffung von IT-Systemen ...?	sehr wichtig <input type="radio"/> weniger wichtig <input type="radio"/> unwichtig <input type="radio"/>	
g Wird die Erfüllung von ISi-Anforderungen als Voraussetzung für die Inbetriebnahme verifiziert?	<input type="radio"/> ja	<input type="radio"/> nein

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

	a Kenntnis		b Relevanz		c Umsetzung		
	inhaltlich bekannt		bedeutsam		bereits erfolgt		
	ja	nein	ja	nein	umfassend	teilweise	gering
• BDSG	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• TKG/TKÜV	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• TMG	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• SigG/SigV	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• KonTraG	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• GDPdU	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Basel II	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• SOX	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• FRCP (E-Disolvency)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• branchenspez. Regularien	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

bitte nennen: _____

BDSG = Bundesdatenschutzgesetz, TKG = Telekommunikationsgesetz, TKÜV = Telekommunikationsüberwachungsverordnung, TMG = Telemediengesetz, SigG/SigV = Signaturgesetz/-Verordnung, KonTraG = Gesetz zur Kontrolle und Transparenz bei Aktiengesellschaften und publizitätspflichtigen Gesellschaften, GDPdU = Grundsätze zu Datenzugriff und Prüfbarkeit digitaler Unterlagen, Basel II = Baseler Akkord, Eigenkapitalvorschriften für das Kreditgewerbe, SOX = Sarbanes-Oxley Act, FRCP = US Federal Rules of Civil Procedure

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

	überzogen	angemessen	unzureichend	n. b.
• Datenschutz	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• TK-/Internet-Überwachung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Strafgesetze (bzgl. Computer-Kriminalität)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Signaturgesetz	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• E-Business (Verträge, Haftung, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Risikomanagement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

e Welche der folgenden Aussagen treffen im Hinblick auf die jüngste Novelle des deutschen Bundesdatenschutzgesetzes (BDSG) für Ihr Haus zu?

	ja	nein	n. b.
• Durch das neue BDSG müssen sich Unternehmen verstärkt vor Datenlecks schützen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Unser Haus hat bereits geeignete Sicherheitsmaßnahmen implementiert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• „Data Loss / Leakage Prevention“ (DLP) unterstützt Unternehmen bei der Einhaltung dieser Vorschriften	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Unser Haus ist über DLP-Lösungen ausreichend informiert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Unser Haus plant <i>keine</i> zusätzlichen Sicherheitsmaßnahmen aufgrund der BDSG-Novelle	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.11 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	<input type="checkbox"/>
• Es fehlt an Bewusstsein beim mittleren Management	<input type="checkbox"/>
• Es fehlt an Bewusstsein bei den Mitarbeitern	<input type="checkbox"/>
• Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	<input type="checkbox"/>
• Es fehlen realisierbare (Teil-)Konzepte	<input type="checkbox"/>
• Es fehlen geeignete Methoden und Werkzeuge	<input type="checkbox"/>
• Es fehlt an Möglichkeiten zur <i>Durchsetzung</i> sicherheitsrelevanter Maßnahmen	<input type="checkbox"/>
• Es fehlen verfügbare und kompetente Mitarbeiter	<input type="checkbox"/>
• Es fehlen geeignete Produkte	<input type="checkbox"/>
• Anwendungen sind nicht für Isi-Maßnahmen vorbereitet	<input type="checkbox"/>
• Es fehlt an praxisorientierten Sicherheitsberatern	<input type="checkbox"/>
• Es fehlt an Geld/Budget	<input type="checkbox"/>
• Die vorhandenen Konzepte werden nicht umgesetzt	<input type="checkbox"/>
• Die Kontrolle auf Einhaltung ist unzureichend	<input type="checkbox"/>
• Sonstiges (bitte nennen): _____	<input type="checkbox"/>
• keine	<input type="checkbox"/>

A

2.12 Wie beurteilen Sie den Kenntnisstand zur ISI in Ihrem Hause?

	sehr gut	gut	befriedigend	ausreichend	nicht austr.	n. b.
• Top-Management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mittleres Management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• IT-Sicherheitsfachleute	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Anwender in hochsensitiven Bereichen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Anwender in weniger sensitiven Bereichen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3 Statistische Angaben

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

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

3.02 Zu welcher Branche gehört Ihr Haus?

Energieversorgung <input type="radio"/>	Berater <input type="radio"/>
Handel <input type="radio"/>	Telekommunikationsdienstleister/Provider <input type="radio"/>
Handwerk <input type="radio"/>	Behörden/öffentliche Hand <input type="radio"/>
Transport/Verkehr <input type="radio"/>	Outsourcing-Dienstleister <input type="radio"/>
Kreditwirtschaft <input type="radio"/>	Wissenschaft/Forschung/Schulen <input type="radio"/>
Versicherungen <input type="radio"/>	chemische Industrie <input type="radio"/>
Verlage/Medien <input type="radio"/>	übrige Industrie <input type="radio"/>
Gesundheitswesen <input type="radio"/>	Sonstiges (bitte nennen): _____ <input type="radio"/>

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/CISO/CSO <input type="checkbox"/>	Leiter IT / DV / RZ <input type="checkbox"/>	Leiter Sicherheit/Werkschutz <input type="checkbox"/>	
ISI-Ausschuss (o. Ä.) <input type="checkbox"/>	IT / DV-Revision <input type="checkbox"/>	Administratoren <input type="checkbox"/>	
Datenschutzbeauftragter <input type="checkbox"/>	Leiter Organisation <input type="checkbox"/>	DV-orientierter Jurist <input type="checkbox"/>	

3.06 Welche Funktionsbezeichnung trifft auf Sie am ehesten zu?

Geschäftsführer <input type="radio"/>	RZ-/IT-Leiter <input type="radio"/>	IT-Mitarbeiter <input type="radio"/>
IT-Sicherheitsverantwortlicher/CISO <input type="radio"/>	DV-/Orga-Leiter <input type="radio"/>	Sonstiges: _____ <input type="radio"/>
IT-Sicherheitsadministrator <input type="radio"/>	Revisor <input type="radio"/>	
Datenschutzbeauftragter <input type="radio"/>	Administrator/Systemtechniker <input type="radio"/>	

3.07 Der Umsatz bzw. die Bilanzsumme Ihres Hauses betrug im letzten Wirtschafts-/Kalenderjahr

• _____ € Umsatz	• _____ € Bilanzsumme (nur Kreditinstitute/Versicherungen)
• nicht relevant, da Behörde oder Ähnliches (bitte ggf. ankreuzen) <input type="checkbox"/>	<input type="checkbox"/>

3.08 Budget

a Das Budget für Informationsverarbeitung (inkl. Personalkosten) umfasst im Jahr 2009 _____ €	geschätzt <input type="radio"/> ermittelt <input type="radio"/>
b Der Anteil für ISI-Maßnahmen (inkl. Personalkosten) an diesem Budget beträgt _____ %	geschätzt <input type="radio"/> ermittelt <input type="radio"/>

4 Informationsquellen und Schulung

4.01 Wen informiert/schult Ihr Haus zu Fragen der ISi?

	häufig/regelmäßig (min. 1x jährl.)	gelegentlich / zu speziellen Anlässen	nie	n. b.
• Benutzer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• freie/externe Mitarbeiter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• IT-/DV-Mitarbeiter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Datenschutzbeauftragte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• ISi-Beauftragte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Revisoren, Prüfer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• andere	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4.02 Welche Ausbildungsmethoden setzt Ihr Haus auf dem Gebiet der ISi bevorzugt ein?

a	häufig	gelegentlich	nie	n. b.
• interne Schulungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• externe Schulungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Materialien (Unterlagen, CDs/DVDs) zum Selbstlernen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Online-Trainings-Anwendungen/-Tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b Kennen Sie den Internet-Risk-Behaviour-Index (www.IRBI.de)?

ja nein

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, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• herstellerunabhängige Zertifikate zur Aus-/Weiterbildung (z. B. CISSP, CISM, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b Welche herstellerunabhängigen ISi-Zertifikate kennen Sie?

• CISA <input type="checkbox"/>	• CISSP <input type="checkbox"/>	• IT-Grundschutz-Auditor <input type="checkbox"/>
• CISM <input type="checkbox"/>	• SSCP <input type="checkbox"/>	• Sonstige (bitte ausschreiben):
• CISO <input type="checkbox"/>	• TISP <input type="checkbox"/>	_____

4.04 Wo informieren Sie sich über ISi?

• CeBIT <input type="checkbox"/>	• it-sa <input type="checkbox"/>	• Infosecurity <input type="checkbox"/>	• BSI-Kongress <input type="checkbox"/>	• ISSE <input type="checkbox"/>	• Security Essen <input type="checkbox"/>
• andere Messen / Konferenzen / Kongresse / Seminare	(welche?) _____				
• Zeitschriften / Magazine	(welche?) _____				
• Internetquellen / Security Communities	(welche?) _____				

4.05 Wo erhalten Sie Informationen über aktuelle Sicherheits-Updates?

a • aktiv vom Hersteller (push) <input type="checkbox"/>	• auf Informationsseiten des Herstellers (pull) <input type="checkbox"/>
• aktiv durch Anbieter (Systemhäuser, Händler ...)	• auf Informationsseiten von Dritten <input type="checkbox"/>
• aktiv durch Dritte (push, z. B. Mailingliste) <input type="checkbox"/>	

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

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

Sonstige: _____

4.06 Qualität von Hersteller-Advisories

	sehr gut	gut	befriedigend	ausreichend	nicht austr.	n. b.
a Umfang/Vollständigkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b Verständlichkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c Geschwindigkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d Bevorzugen Sie eine lokalisierte Fassung, auch wenn diese 1-2 Tage später erscheint?					<input type="radio"/> ja	<input type="radio"/> nein

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 vor- gesehen	realisiert	geplant	nicht vor- gesehen	realisiert	geplant	nicht vor- gesehen
• Firewalls	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Intrusion-Detection/Prevention-Systeme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Netzwerkzugangskontrolle (EAP, NAC/NAP, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Schnittstellenüberwachung/-schutz (USB, ser., par., Bluetooth, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Durchgängige Benutzerverwaltung (Identity-Lifecycle-Management)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Authentifizierung									
– Hardware-Token	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Passwort	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Chipkarte/Smartcard	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– biometrische Verfahren	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– SSL-Zertifikate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Security-Event-Management (Protokollierung/Auswertung)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• zentralisiertes Schwachstellen-Management (Vulnerability-Mgmt.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• zentralisiertes System-/Patch-Management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Virtualisierung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Malware-/Spyware-Abwehr	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Spam-Abwehr	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Content-Inspection/-Filtering (Adress-/Inhaltsfilter eingehend)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Data-Leakage/Loss-Prevention (DLP, Inhaltskontrolle abgehend)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Digital-/Enterprise-Rights-Management (DRM/ERM)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verschlüsselung/VPN									
– sensitive Dateien	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Festplatten / eingebaute Speicher (komplett/partitionsweise)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– mobile Speichermedien (USB, SDcard, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Archivdatenträger/Backups	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– LAN / Intranet-Verbindungen (VPN)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– WLAN-Verbindungen (WPA/VPN, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– WAN / Internet-Verbindungen (VPN)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– mobile Verbindungen (VPN via UMTS, Hotspots usw.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Telefon / Fax (Festnetz/GSM)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Voice over IP (VoIP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– E-Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Datensicherung (Backup)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Langzeit-Archivierung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• physische Sicherheit									
– Zutrittskontrolle, biometrisch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Zutrittskontrolle, sonstige	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Bewachung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Video-Überwachung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Einbruchmeldesysteme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Schutz von Glasflächen gegen Durchbruch / Durchwurf	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Sicherheitstüren	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Brandmeldesysteme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Löschanlagen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– andere Meldesysteme (z. B. Gas, Staub, Wasser)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Datensicherungsschränke/-räume	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
– Schutz gegen kompromittierende Abstrahlung (TEMPEST)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– sonstige Maßnahmen gegen Hardwarediebstahl	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• physikalisches Löschen von Datenträgern	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Klimatisierung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
• unterbrechungsfreie Stromversorgung (USV)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Überspannungsschutz für Stromleitungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Überspannungsschutz für Daten-/IT-Leitungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Reserve-Netzzugang (IT/TK) zur Ausfallüberbrückung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.02 Klassifizierung/Segmentierung

a Wie klassifiziert Ihr Haus Daten bezüglich ihrer Sensitivität (z. B. als geschäftskritisch, vertraulich, Verschlusssache usw.)?

automatisiert
 manuell
 gar nicht

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/gefährdete Systeme und Daten speziell abgeschottet?

ja, durch Netzwerkmechanismen (VLAN, NAC/NAP 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?

- für alle Mitarbeiter
- für spezielle Mitarbeiter/Abteilungen/Bereiche
- nur an ausgewählten Arbeitsplätzen
- generell nicht gestattet
- n. b.

a geschäftliche Nutzung von
 Multimedia, „Web 2.0“ WWW E-Mail

b private Nutzung gestattet

c Nutzt Ihr Haus ein Berechtigungskonzept für aktive Inhalte (JavaScript, ActiveX, Silverlight, 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 Endgeräte-Sicherheit (Device-/Application-Management)

Wie sichert sich Ihr Haus gegen unerwünschte Nutzung/Installation von ...?

- 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

a Schnittstellen

b Anwendungen

c Wie häufig werden Log-Files der Endgeräte zu Sicherheitszwecken ausgewertet?

regelmäßig: alle ____ Tage anlassbezogen nie n. b.

d Wie lange werden in Ihrem Haus Endgeräte-Log-Files (oder relevante Informationen daraus) aufbewahrt?

____ Monate

e Der Einsatz von Terminalservern ist ...?

realisiert geplant nicht vorgesehen

f In welchem Maße nutzt Ihr Haus Thin Clients als Arbeitsplatzsysteme?

ausschließlich bevorzugt gleichwertig nachrangig gar nicht

g Falls Thin Clients jetzt oder geplant im Einsatz sind: Von welchen Herstellern?

Igel HP Fujitsu Sun Wyse Sonstige

B

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

	h Aufschaltung gestattet			i technische Kontrolle		
	ja	nein	n. b.	umfassend	teilweise	keine
• Net-/Notebooks, Smartphones/PDAs usw. (LAN/WLAN-Zugang)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Smartphones/PDAs usw. (Synchronisation mit PCs)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mobile Speichermedien (USB, SDcards, Digitalkameras, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Netzwerkhardware (Switches, WLAN-APs, Modems ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• sonstige Peripherie (z. B. Drucker)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.05 Unified Threat-Management (UTM) / Multi-Vendor-Strategie

a Wie beurteilen Sie die Leistungsfähigkeit von Unified-Threat-Management-Systemen (UTM) im Vergleich zu Einzellösungen/Best-of-Breed-Ansätzen?

UTM ist ...	besser		gleich	schlechter		n. b.
	erheblich	etwas	gut	etwas	erheblich	
• Sicherheit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Skalierbarkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Umsetzung von Hochverfügbarkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Bedienbarkeit (Management-Oberfläche)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Anpassbarkeit an veränderte Anforderungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Kosten-Nutzen-Verhältnis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b Nutzen Sie aus Sicherheitsgründen auf verschiedenen Systemen oder Netzwerksegmenten Produkte mehrerer verschiedener Anbieter?

	Einsatz von Produkten			n. b.
	von nur einem	zweier Anbieter(n)	von drei oder mehr	
• Anti-Virus-Software*	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Firewalls	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Router/Netzwerkhardware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Server-Betriebssysteme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Web-Server	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Applikations-Server	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

c Der Einsatz eines zentralen Management-Tools zur Verwaltung heterogener Sicherheitssysteme ist ...

realisiert geplant nicht vorgesehen n. b.

d Wie oft ergeben sich in Ihrem Haus beim Einspielen von Updates oder neuen Anwendungen Inkompatibilitäten oder sonstige Probleme mit Sicherheits-Software auf Endgeräten?

häufig gelegentlich selten nie n. 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, häufig
- ja, selten
- nein, nie

c falls ja: Warum?

- aus Kostengründen
- aus Sicherheitsgründen
- bessere Funktionalität
- bessere Interoperabilität
- Sonstiges

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

	häufig	gelegentlich	nie	n. b.
• Prüfungen hinsichtlich der Sicherheit erfolgen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Prüfungen hinsichtlich funktionaler Aspekte erfolgen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Modifikationen/lokale Anpassungen erfolgen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.07 Content-Security (Malware, Spam, Filter)

a Welche Vorsorge gegen Malware hat Ihr Haus getroffen?

	ja	nein	b Update-Frequenz
• Einsatz von Viren-Scannern	<input type="radio"/>	<input type="radio"/>	_____ Std.
– an der Firewall/Internet-Gateway	<input type="radio"/>	<input type="radio"/>	_____ Std.
– auf dem Mail-/File-/Applikations-Server	<input type="radio"/>	<input type="radio"/>	_____ Std.
– auf den PCs/Workstations	<input type="radio"/>	<input type="radio"/>	_____ Std.
– auf mobilen Endgeräten	<input type="radio"/>	<input type="radio"/>	_____ Std.
• Stetige Schreib-/Leseprüfung (Virenwächter) auf PCs/Notebooks	<input type="radio"/>	<input type="radio"/>	
• Isolierte Testumgebung steht zur Verfügung	<input type="radio"/>	<input type="radio"/>	

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

• Virenschutz <input type="checkbox"/>	• Spyware-Schutz <input type="checkbox"/>	• Desktop/Client-Firewall <input type="checkbox"/>	• Prüfung von SSL-Übertragungen <input type="checkbox"/>
• Phishing-Abwehr <input type="checkbox"/>	• Spam-Abwehr <input type="checkbox"/>	• Inhaltsfilter <input type="checkbox"/>	• Applikationskontrolle <input type="checkbox"/>
• Reporting-Tools <input type="checkbox"/>	• Monitoring/Alerting <input type="checkbox"/>	• zentrale Administration <input type="checkbox"/>	

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	b Welchen Standard verwenden Sie dabei?
• für alle E-Mails	<input type="checkbox"/>	<input type="checkbox"/>	• S/MIME <input type="checkbox"/>
• für externe Kommunikation	<input type="checkbox"/>	<input type="checkbox"/>	• (Open)PGP/GPG <input type="checkbox"/>
• für sensitive Nachrichten	<input type="checkbox"/>	<input type="checkbox"/>	• Sonstige <input type="checkbox"/>
• nie	<input type="radio"/>	<input type="radio"/>	

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 vor-gesehen		realisiert	geplant	nicht vor-gesehen
• nur Software	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	• laut Signaturgesetz			
• Hardwaremodule (HSM)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	– fortgeschrittene Signatur	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Hardware-Token	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	– qualifizierte Signatur	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Chipkarten	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	– qualifizierte Signatur mit Anbieterakkreditierung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• elektronischer Personalausweis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>				

5.10 Identity-Management (IdM) / Public-Key-Infrastructures (PKI)

a Die Implementierung einer IdM-Lösung ist ...

realisiert geplant nicht vorgesehen n. b.

b Die Implementierung einer PKI ist ...

c Für welche Zwecke nutzen/planen Sie in Ihrem Haus eine PKI?

• allgemeine elektronische Signaturen (E-Mail, Dateien usw.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Code-Signaturen (Software)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verschlüsselung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Authentifizierung (VPN, SSL, Web-/Remote-Access usw.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Autorisierung (Zugriffsrechte, Single-Sign-on usw.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

B

d Sind Sie über die Funktionen und Möglichkeiten des neuen deutschen Personalausweises (z. B. Internetausweis und qual. elektr. Signatur) informiert? umfassend teilweise nein

e Plant Ihr Haus, diese neuen elektronischen Ausweisfunktionen für seine Geschäftsprozesse zu nutzen? ja nein

f Sind Sie der Meinung, dass der elektronische Geschäftsverkehr durch den neuen Personalausweis für Bürger und Unternehmen interessanter wird? ja nein n. b.

5.11 Notfallvorsorge

a Besteht ein IT-Notfall/-Wiederanlaufkonzept?	b falls ja: Wurde dieses Konzept schriftlich fixiert?
ja <input type="radio"/>	<input type="radio"/> ja
nein <input type="radio"/>	<input type="radio"/> nein
	<input type="radio"/> n. b.

c falls ja: Berücksichtigt dieses Konzept explizit die speziellen Anforderungen für/bei ...? ja nein

• Hochverfügbarkeit des E-Business		<input type="radio"/>	<input type="radio"/>
• Hardware-Ausfall/-Wiederbeschaffung		<input type="radio"/>	<input type="radio"/>
• Software-Sicherheitsvorfälle (Bekanntwerden von Schwachstellen o. Ä.)		<input type="radio"/>	<input type="radio"/>
• Viren/Würmer/Exploit-„Epidemien“		<input type="radio"/>	<input type="radio"/>
• Denial-of-Service-Attacken		<input type="radio"/>	<input type="radio"/>
• gezielte Angriffe durch Einzeltäter (Hacker, Spionage, ...)		<input type="radio"/>	<input type="radio"/>
• physische Einwirkungen (Brand, Naturkatastrophen, Terror, ...)		<input type="radio"/>	<input type="radio"/>
• Zusammenbruch externer Infrastrukturen		<input type="radio"/>	<input type="radio"/>

d Liegen unternehmenswichtige Daten an räumlich unabhängigen Standorten vor (z. B. Auslagerung/Spiegelung an Zweigstellen oder bei Kooperationspartnern/Dienstleistern) ja nein n. b.

Was hat Ihr Haus für längere Ausfälle bereitgestellt?	e Unternehmens-server/Mainframe			f Abt.-Rechner/Arbeitsplätze PC, LAN		
	realisiert	geplant	nicht vor-gesehen	realisiert	geplant	nicht vor-gesehen
• Räume („kalte Lösung“ bzw. „empty shell“)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Räume mit (wichtiger) Hardware („warme Lösung“)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Cluster/Load-Balancing/dynamische Büros (mit entspr. Kapazität)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• laufende Systeme („heiße Lösung“)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• konfigurationsidentische Netze	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Virtualisierungslösung mit redundanter Datenhaltung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Nutzung von Cloud-/SaaS-Diensten	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verträge mit externen Dienstleistern/Partnern						
– über die Nutzung von deren Ressourcen (stationäres Ausweich-RZ)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– über die Nutzung von kurzfristig verfügbaren Containern	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verträge über die schnelle Lieferung von Hardware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Versicherung abgeschlossen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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)		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• onlinegestütztes Handbuch		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Online-Anwendung		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

i Wie oft wird die Dokumentation aktualisiert? alle ___ Tage anlassbezogen nie n. b.

j Werden „abgearbeitete“ Pläne zu Revisionszwecken archiviert und können jederzeit wieder eingesehen werden? ja nein n. b.

5.12 Computer-Forensik

a Wurde in Ihrem Haus 2008/2009 ein Sicherheitsvorfall rechtlich verfolgt?	b falls nein: Warum?
ja <input type="radio"/>	weil kein Vorfall <input type="radio"/>
nein <input type="radio"/>	mangels Verfolgungsinteresse <input type="radio"/>
	mangels Wissen um Ermittlungsmöglichkeiten <input type="radio"/>
	n. b. <input type="radio"/>

c Wen würde Ihr Haus im Bedarfsfall für forensische Analysen ansprechen?

	auf jeden Fall	bevorzugt	normalerweise	nachrangig	keinesfalls	n. b.
• eigene IT-Abteilung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• eigene Revision	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• eigene Rechtsabteilung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• externer Rechtsbeistand	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• externe Wirtschaftsberatung/-prüfer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• externer, bereits bekannter IT-Dienstleister	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Fachdienstleister für Computer-Forensik	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• externes CERT/CSIRT	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• BSI	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Strafverfolgung (Polizei, Staatsanwaltschaften)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.13 CERT/CSIRT

a Unterhält Ihr Haus ein eigenes Computer Emergency oder 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? _____

5.14 ISi-Beratung

a Nutzt Ihr Haus externe ISi-Beratung?	b falls ja: in welcher Form?
ja, häufig <input type="radio"/>	• Strategie- und Managementberatung <input type="checkbox"/>
ja, gelegentlich <input type="radio"/>	• Durchführung von Inhouse-Schulungen <input type="checkbox"/>
nein, nie <input type="radio"/>	• Durchführung von Risikoanalysen und Konzeptentwicklung <input type="checkbox"/>
	• Durchführung von Schwachstellenanalysen <input type="checkbox"/>
	• Durchführung von Penetrationstests <input type="checkbox"/>
	• Umsetzung von Konzepten und Maßnahmen <input type="checkbox"/>
	• Kontrolle vorhandener Konzepte auf Eignung und Einhaltung <input type="checkbox"/>
	• Produktberatung und Kaufunterstützung <input type="checkbox"/>
	• Prozess-Entwicklung und -Optimierung <input type="checkbox"/>
	• Sonstiges (bitte nennen): <input type="checkbox"/>

c falls ja: Bitte benoten Sie die Beratungsleistungen sehr gut gut befriedigend ausreichend nicht ausreichend n. b.

5.15 Outsourcing/Managed-Security- (MSS) und Cloud-Services?

a Nutzt Ihr Haus Outsourcing? ja nein

b falls ja: Welche Funktionen haben Sie ausgelagert?

• externer ISi-Beauftragter	<input type="checkbox"/>	• gesamte(s) Rechenzentrum/IT	<input type="checkbox"/>
• Überwachung, Kontrolle, Qualitätssicherung	<input type="checkbox"/>	• Notfallvorsorge/Business-Continuity	<input type="checkbox"/>
• Managed Firewall/IDS/IPS	<input type="checkbox"/>	• Anwendungssysteme	<input type="checkbox"/>
• Content-Security/Virenabwehr	<input type="checkbox"/>	• Customer-Relationship-Management (CRM)	<input type="checkbox"/>
• Spamabwehr	<input type="checkbox"/>	• Datenbank-Systeme, Werkzeuge	<input type="checkbox"/>
• E-Mail-Betrieb	<input type="checkbox"/>	• Haustechnik	<input type="checkbox"/>
• Netzwerk-Management	<input type="checkbox"/>	• Datenschutz	<input type="checkbox"/>
• Datensicherung, Backup-Lösungen	<input type="checkbox"/>	• Vernichtung von Datenträgern (Papier, IT)	<input type="checkbox"/>
• Archivierung, Dokumentation,	<input type="checkbox"/>	• Wachschatz/Bewachung	<input type="checkbox"/>
• Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung	<input type="checkbox"/>	• Sonstiges (bitte nennen):	<input type="checkbox"/>
• Betriebssystempflege/Administration	<input type="checkbox"/>		

c falls ja: Bitte bewerten Sie die Outsourcingleistungen sehr gut gut befriedigend ausreichend nicht ausreichend n. b.

B

**d falls ja: Haben Sie Service-Level-Agreements/
vertragliche Vereinbarungen
mit dem Outsourcer?**

- mit expliziten Anforderungen an die ISI? ja nein
- mit expliziten Anforderungen an den Datenschutz? ja nein
- mit Regelungen zu Haftungsübernahme oder Schadensersatz? ja nein

e falls ja: Kontrolle erfolgt ...

regelmäßig anlassbezogen nie n. b.

-
-
-

**f Welche Informationen/Kriterien sind Ihnen beim Auslagern
von Security-Services wichtig?**

sehr wichtig weniger wichtig unwichtig n. b.

- Verfügbarkeit der Dienste
- Unabhängige Zertifizierung des Anbieters / der Dienste
- Performance (Durchlauf-/Wartezeiten)
- Bereitstellung statistischer Daten
(z. B. über Spam-/Virenaufkommen)
- Sicherheitsrelevante Detailinformationen
(z. B. über gestoppte Angriffe/Viren)
- detaillierte Statusinformationen
(z. B. bearbeitete Mails/Verbindungen)

g Wie häufig erwarten Sie entsprechende Statusberichte bzw. aktualisierte Daten?

- in Echtzeit stündlich täglich wöchentlich monatlich n. b.

**h Wie beurteilen Sie die Leistungsfähigkeit externer Dienste (Outsourcing/MSS/Cloud-Services)
im Vergleich zu Inhouse-Lösungen**

ext. Dienste sind ... besser gleich schlechter n. b.

erheblich etwas gut etwas erheblich

- Sicherheit
- Datenschutz
- Skalierbarkeit
- Anpassbarkeit an veränderte Anforderungen
- Kosten-Nutzen-Verhältnis
- Transparenz/Kontrollierbarkeit

**i Nutzt Ihr Haus Applikationen oder Sicherheitssysteme, die auf Cloud-/Web-Services zurückgreifen
(z. B. bei Viren-/Spamabwehr am Endgerät)?**

- ja (gesicherte Erkenntnis) vermutlich ja vermutlich nicht nein (gesicherte Erkenntnis) n. b.
-

**j falls ja: Sind die damit verbundene Kommunikation dieser Anwendungen sowie die Weitergabe von Daten
an den Dienstleister für Ihr Haus hinreichend transparent nachvollziehbar?**

- ja nein n. b.

5.16 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

5.17 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?

• antispameurope	<input type="checkbox"/>	• GeNUA	<input type="checkbox"/>	• Rittal/Lampertz	<input type="checkbox"/>
• art of defence	<input type="checkbox"/>	• IBM	<input type="checkbox"/>	• ROG	<input type="checkbox"/>
• Astaro	<input type="checkbox"/>	• INFINIGATE	<input type="checkbox"/>	• Rohde & Schwarz	<input type="checkbox"/>
• Avira	<input type="checkbox"/>	• INFODAS	<input type="checkbox"/>	• Safenet/Aladdin	<input type="checkbox"/>
• Axway	<input type="checkbox"/>	• itWatch	<input type="checkbox"/>	• SAP	<input type="checkbox"/>
• Barracuda	<input type="checkbox"/>	• Juniper	<input type="checkbox"/>	• Secude	<input type="checkbox"/>
• Blue Coat	<input type="checkbox"/>	• Jürgen Jakob Software	<input type="checkbox"/>	• Secaron	<input type="checkbox"/>
• Bundesdruckerei/D-Trust	<input type="checkbox"/>	• Kaspersky	<input type="checkbox"/>	• secunet	<input type="checkbox"/>
• Checkpoint	<input type="checkbox"/>	• KPMG	<input type="checkbox"/>	• Siemens	<input type="checkbox"/>
• CenterTools	<input type="checkbox"/>	• mabunta	<input type="checkbox"/>	• SOPHOS	<input type="checkbox"/>
• Cisco	<input type="checkbox"/>	• McAfee	<input type="checkbox"/>	• Symantec	<input type="checkbox"/>
• CROCODIAL	<input type="checkbox"/>	• Microsoft	<input type="checkbox"/>	• Thales	<input type="checkbox"/>
• DATSEC/eset	<input type="checkbox"/>	• ODN	<input type="checkbox"/>	• Utimaco	<input type="checkbox"/>
• Dehn+Söhne	<input type="checkbox"/>	• OPTIMAL Systemberatung	<input type="checkbox"/>	• UIMC	<input type="checkbox"/>
• DeviceLock	<input type="checkbox"/>	• PAV Panda Security	<input type="checkbox"/>	• TREND MICRO	<input type="checkbox"/>
• DIM	<input type="checkbox"/>	• PGP	<input type="checkbox"/>	• T-Systems	<input type="checkbox"/>
• eleven	<input type="checkbox"/>	• phion	<input type="checkbox"/>	• Verbatim	<input type="checkbox"/>
• entrada	<input type="checkbox"/>	• retarus	<input type="checkbox"/>	• es fehlen: _____	<input type="checkbox"/>

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	<input type="radio"/>	<input type="radio"/>	• kryptografische Grundlagenarbeit	<input type="radio"/>	<input type="radio"/>
• Schriften/Faltblätter zur IT-Sicherheit	<input type="radio"/>	<input type="radio"/>	• Beratung	<input type="radio"/>	<input type="radio"/>
• Leitfaden IT-Sicherheit	<input type="radio"/>	<input type="radio"/>	• Grundschatz-Hotline	<input type="radio"/>	<input type="radio"/>
• Studien-/Buch-Publikationen	<input type="radio"/>	<input type="radio"/>	• GSTOOL	<input type="radio"/>	<input type="radio"/>
• BSI-Standards	<input type="radio"/>	<input type="radio"/>	• Viren-Hotline	<input type="radio"/>	<input type="radio"/>
• Grundschatz-Kataloge	<input type="radio"/>	<input type="radio"/>	• Viren-Mailingliste	<input type="radio"/>	<input type="radio"/>
• Web-Angebot des BSI	<input type="radio"/>	<input type="radio"/>	• Informationsdienst (BSI-Forum in der <kes>)	<input type="radio"/>	<input type="radio"/>
• BSI-Newsletter (5-mal/Jahr)	<input type="radio"/>	<input type="radio"/>	• BSI-Kongress	<input type="radio"/>	<input type="radio"/>
• Zertifizierung	<input type="radio"/>	<input type="radio"/>	• Newsletter „sicher • informiert“ (14-tägig)	<input type="radio"/>	<input type="radio"/>
• CERT-Bund	<input type="radio"/>	<input type="radio"/>	• Angebot „BSI für Bürger“	<input type="radio"/>	<input type="radio"/>

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.

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

(Anschriftsfeld für Versand im C4-Fensterumschlag)

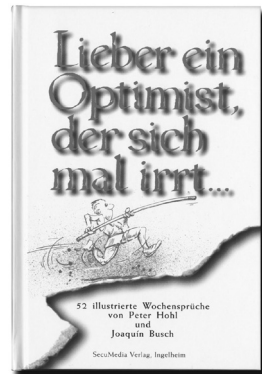
Ihre „Dankeschön-Prämien“

A



V9 Micro-Lenser, die „Taschenlampe am Schlüsselbund“ von Zweibrüder Optoelectronics

Wochensprüche
„Lieber ein Optimist“
von Peter Hohl



A+B

Kopflampe von
Zweibrüder Optoelectronics
(Abb. ähnlich)



Zwei Sprüchebücher
„Lieber ein Optimist“ und
„Direkt nach vorn“

Sicherheitsjahrbuch
2009/2010 –
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 2010

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*

- Taschenlampe am Schlüsselbund
- Buch „Lieber ein Optimist“

A+B Ich habe den vollständigen Fragebogen ausgefüllt
und möchte als Teilnahmegeschenk*

- Kopflampe
 - Sicherheits-Jahrbuch 2009/2010
 - Sprüchebücher „Lieber ein Optimist“ und
„Direkt nach vorn“
- *(bitte nur einen Gegenstand ankreuzen)

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