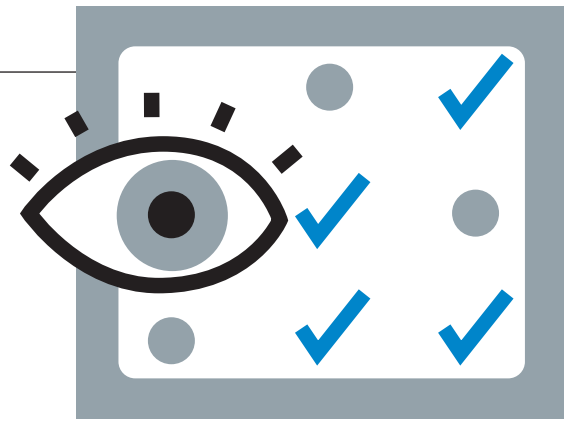


Checkliste zur Informations-Sicherheit



<kes> **Microsoft**
Sicherheitsstudie 2014

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.

Mit dem vorliegenden Fragebogen möchten wir und die Sponsoren die Grundlage für die nächste <kes>-Studie legen und schon jetzt jedem Ausfüller eine Arbeitshilfe zur Reflexion und Evaluierung seiner eigenen Sicherheitslage an die Hand geben – natürlich wurde die „Checkliste zur Informations-Sicherheit“ auch in diesem Jahr wieder aktualisiert. Und wie immer freuen wir uns schon jetzt darauf, im kommenden Jahr mit den Ergebnissen Ihrer und unserer Arbeit wieder belastbare Zahlen und Fakten zur Lage der Informations-Sicherheit zu liefern.

Zum zweiten Mal steht Ihnen der Fragebogen darüber hinaus nicht mehr nur in der gedruckten Version und als PDF-Datei zur Verfügung. Auch dieses Jahr können Sie die Fragen direkt online beantworten (natürlich mit der Möglichkeit zum Zwischenspeichern). Das Bremer Unternehmen OTARIS Interactive Services GmbH hat unsere Checkliste dazu in seiner „ProAUDIT Suite“ modelliert und hostet die Online-Version des Fragebogens auf seinen Webservern.

Für die Fragebögen per Post garantiert seit jeher <kes>-Herausgeber Peter Hohl mit seinem Namen (s. Kasten) – für die Onlineversion verbürgt sich nun gleichermaßen OTARIS-Geschäftsführer Mehmet Kus, dass bei der Speicherung sowie Datenverarbeitung und -aufbereitung umfassende Maßnahmen für Sicherheit, Datenschutz und Ihre Anonymität sorgen. Näheres dazu sowie den Zugang zum Online-Fragebogen finden Sie auf www.kes.info/studie2014.

Sowohl online als auch offline ist der Fragebogen 2014 erneut in zwei Segmente gegliedert: Wer keine Möglichkeit hat, sich mit allen Antworten zu beteiligen, kann sich wieder 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 18).

So gehts

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

_____ Sollten Sie die Studie weiterempfehlen mögen: Auf www.kes.info/studie2014/ liegt diese 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.

_____ Einsendetermin: 3. März 2014

_____ **Ich garantiere mit meinem Namen absolute Vertraulichkeit aller Einsendungen an SecuMedia.** 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



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 überhaupt erst ein sinnvolles Gesamtbild entstehen lassen.



Für technisch-organisatorische Unterstützung bedanken wir uns bei der OTARIS Interactive Services GmbH (Hosting von Onlinefragebogen und Erfassung) sowie der humanIT Software GmbH (Software für Auswertung und Grafikerstellung).



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 2.05 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/studie2014/ werden wir zudem bei Bedarf eine FAQ-Sammlung pflegen.

Fragebogen für die <kes>/Microsoft-Sicherheitsstudie 2014

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.

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.	Priorität			b Wie schätzen Sie die zukünftige Entwicklung der Risiken in diesen Gefahrenbereichen für Ihr Haus ein?				c Haben diese Gefahren in Ihrem Haus 2012/2013 tatsächlich zu mittleren bis größeren Beeinträchtigungen geführt?	
	höchste	erhöhte	normale/ keine	abnehmend stark	etwas	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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>
• Notebooks/Netbooks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Smartphones/Tablets	<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 (USB-Speicher, CDs/DVDs, Tapes, ...)	<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"/>
• Prozess-, Automations- und Leittechnik (Industrial IT)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A

1.03 Vertraulichkeitsbrüche/Datenlecks

a Haben Unbefugte 2012/2013 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"/>
• Datenlecks/Probleme bei Dienstleistern oder Partnern	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b falls es Vertraulichkeitsbrüche gab: 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="radio"/>

c Sind Ihrer Meinung nach für die meisten Datenlecks eigene Mitarbeiter (mit-) verantwortlich?

☐ ja
☐ nein

d falls ja: Was sind die Gründe dafür?

	ja	nein	n. b.
• Mitarbeiter verstehen die Systeme nicht (Datenschutz-/Sicherheitslösungen zu kompliziert)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Mitarbeitern sind die Konsequenzen nicht bewusst	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Mitarbeiter kennen die Firmen-Policies nicht	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Mitarbeiter wollen dem Unternehmen schaden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

e Wie oft nutzen Mitarbeiter in Ihrem Haus Filesharing-Dienste, die auf den privaten Gebrauch zugeschnitten sind (z.B. Dropbox), um dienstliche Dokumente auszutauschen oder zu speichern?

häufig ☐ selten ☐ nie ☐ n. b. ☐

f Ist eine solche Nutzung in Ihrem Hause explizit verboten?

ja ☐ nein ☐ n. b. ☐

1.04 Malware-Vorfälle

a Hatte Ihr Haus 2013 Vorfälle mit Malware (Viren, Würmer, Trojaner, Spyware usw.)?

☐ ja
☐ nein

b falls ja: Welche Systeme waren betroffen?

	häufig	selten	nie	n. b.
Server	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Desktop-PCs/Clients	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Notebooks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Smartphones/Handys	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

c Tendenz

☐ weniger Vorfälle als 2012
☐ mehr Vorfälle als 2012
☐ n. b.

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

	häufig	selten	nie	n. b.
• Speichermedien (CDs, DVDs, USB-Speicher, SD-Cards, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mobile Endgeräte (Net-/Notebooks, Tablets, Smartphones)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• unerwünschte Anwendungen (Download, USB, ...)	<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"/>

e Wäre ein nennenswerter Teil der Malware-Vorfälle durch abweichendes (besseres) Nutzer-Verhalten vermeidbar gewesen?

ja ☐ nein ☐ n. b. ☐

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, Hinweis durch Mitarbeiter)	_____ 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 Schadenereignis:

• 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.	• Produkt-/Anbieterwechsel vollzogen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Kosten _____ €	• organisatorische Konsequenzen gezogen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2 Isi-Strategie und -Management

2.01 Gibt es in Ihrem Haus ...?

	ja	nein
• eine schriftlich fixierte <i>Strategie</i> für die Informationsverarbeitung (IT-Betrieb)	<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 berechtigte 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, Tablets, Smartphones, ...)	<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. ☐

A

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.
a organisatorisch (Mitarbeiterverhalten, Kommunikation, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b technisch (Abdeckung, Implementierung, Konfiguration, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.04 Wird die Umsetzung und Einhaltung vorgesehener Maßnahmen/Richtlinien geprüft?

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

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"/>

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"/>	• eigene Methodik/Software <input type="checkbox"/>
ja, für <i>einzelne</i> Anwendungen / Systeme <input type="radio"/>	• standardisiertes Verfahren (Grundschutz, ISO, ...) <input type="checkbox"/>
nein <input type="radio"/>	• Verfahren eines Herstellers oder Beraters <input type="checkbox"/>
c Ist das IT-Risikomanagement (RM) in Ihrem Hause in ein allgemeines Risikomanagement des (Gesamt-)Unternehmens eingebunden?	• Risikomanagement-Software <input type="checkbox"/>
ja <input type="radio"/> nein <input type="radio"/> n. b. <input type="radio"/>	• sonstige Methodik: <input type="checkbox"/>
	• kein strikt methodisches Vorgehen <input type="checkbox"/>

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 (z. B. durch Manipulation/Transaktionen)	<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"/>
• Verzögerung von Arbeitsabläufen	<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"/>

2.08 Kennen Sie die folgenden Kriterienwerke?

	a ja	nein	b falls ja: Welche praktische Bedeutung haben diese Werke für Ihr Haus/Ihre Arbeit?
			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"/>
• 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 2700 (ISMS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
• ISO 22301 (BCM)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
• ISO 31000 (RM)	<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"/>
• PCI DSS	<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 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/III	<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-Discovery)	<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/III = 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"/>

2.10 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"/>
• Die Komplexität heutiger IT-Landschaften ist nicht mehr beherrschbar	<input type="checkbox"/>
• Die Menge der verarbeiteten Daten ist nicht mehr beherrschbar	<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

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

	sehr gut	gut	befriedigend	ausreichend	nicht ausr.	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/Tablets	_____	• 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"/>	CIO	<input type="radio"/>	Administrator/Systemtechniker	<input type="radio"/>
IT-Sicherheitsverantwortlicher/CISO	<input type="radio"/>	RZ-/IT-Leiter	<input type="radio"/>	IT-Mitarbeiter	<input type="radio"/>
IT-Sicherheitsadministrator	<input type="radio"/>	Orga-Leiter	<input type="radio"/>	Sonstiges: _____	<input type="radio"/>
Datenschutzbeauftragter	<input type="radio"/>	Revisor	<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"/>

3.08 Budget

a Das Budget für Informationsverarbeitung (inkl. Personalkosten) umfasste im Jahr 2013 _____ €	geschätzt <input type="radio"/> ermittelt <input type="radio"/>
b Der Anteil für ISI-Maßnahmen (inkl. Personalkosten) an diesem Budget betrug _____ %	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?

	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"/>

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"/>	• T.I.S.P. <input type="checkbox"/>
• CISM <input type="checkbox"/>	• SSCP <input type="checkbox"/>	• ISO 27000 Lead Auditor <input type="checkbox"/>
• CISO <input type="checkbox"/>	• CCFP <input type="checkbox"/>	• IT-Grundschutz-Auditor <input type="checkbox"/>
• CGEIT <input type="checkbox"/>	• CSSLP <input type="checkbox"/>	• Sonstige (bitte ausschreiben):
• CRISC <input type="checkbox"/>	• CPP <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"/>	• RSA Conference <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 ausr.	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"/>

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, Tablets)		
	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 (IDS/IPS)	<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"/>
• Identity- und Access-Management-Lösung (IAM)	<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-/TLS-/X.509-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-Information- und -Event-Management (SIEM)	<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"/>
• Application-Management (Schutz vor Installation/Nutzung unerw. App.)	<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"/>
• Public-Key-Infrastructure (PKI)	<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/WPA2, 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 ...)	<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"/>			
– 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"/>
• 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 Vertraulichkeitsanforderungen (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 innerhalb Ihres Hauses 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 Systemsicherheit/Anbieters Auswahl

Bei der Auswahl von IT-Systemen und -Lösungen sind für Ihr Haus ...

a allgemeine IT

sehr wichtig weniger wichtig unwichtig

b Sicherheitssysteme

sehr wichtig weniger wichtig unwichtig

• Sicherheitsaspekte generell

☐ ☐ ☐

☐ ☐ ☐

• Sicherheits-Zertifikate

☐ ☐ ☐

☐ ☐ ☐

• Trusted-Computing-Technologie (TPM, ...)

☐ ☐ ☐

☐ ☐ ☐

• Hauptsitz des Anbieters im deutschsprachigen Raum

☐ ☐ ☐

☐ ☐ ☐

• Hauptsitz des Anbieters in der EU

☐ ☐ ☐

☐ ☐ ☐

• Entwicklung aus deutscher Hand („made in Germany“)

☐ ☐ ☐

☐ ☐ ☐

• Anpassbarkeit an eigene Anforderungen (Customizing)

☐ ☐ ☐

☐ ☐ ☐

• Preis

☐ ☐ ☐

☐ ☐ ☐

• Unternehmensgröße/Bedeutung im Markt

☐ ☐ ☐

☐ ☐ ☐

• Referenzen

☐ ☐ ☐

☐ ☐ ☐

• Direktsupport durch den Hersteller

☐ ☐ ☐

☐ ☐ ☐

• Support in deutscher Sprache

☐ ☐ ☐

☐ ☐ ☐

• persönliche Ansprechbarkeit/feste Ansprechpartner

☐ ☐ ☐

☐ ☐ ☐

• regelmäßige Infos/Newsletter

☐ ☐ ☐

☐ ☐ ☐

Sind höhere Preise gerechtfertigt für Produkte/Lösungen ...

ja nein n. b.

c mit Sicherheits-Zertifikat?

☐ ☐ ☐

d „made in Germany“?

☐ ☐ ☐

e Wird die Erfüllung von ISi-Anforderungen als

Voraussetzung für die Inbetriebnahme verifiziert?

☐ ☐ ☐

5.04 Angriffserkennung/Lagebild

a Welche Maßnahmen zu Lagebild und „situational Awareness“ sind in Ihrem Hause ...?

realisiert geplant nicht vorgesehen

• zentrales Speichern aller Log-Informationen

☐ ☐ ☐

• zentrales, regelmäßiges Auswerten aller Log-Informationen

☐ ☐ ☐

• zentrales Echtzeit-Monitoring der Logs

☐ ☐ ☐

• zentrales Korrelieren der Logs

☐ ☐ ☐

• Integration von Helpdesk-Information in das zentrale Logging

☐ ☐ ☐

• zentrales Compliance-Reporting

☐ ☐ ☐

• firmenweites Security-Dashboard

☐ ☐ ☐

• Nutzung externer Dienste zur Früherkennung neuer Bedrohungen

☐ ☐ ☐

• Melden eigener Informationen an solche Dienste oder an Behörden zur Verbesserung des Lagebilds

☐ ☐ ☐

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

regelmäßig: alle ___ Tage ☐ anlassbezogen ☐ nie ☐

B

5.05 Netzwerksicherheit

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

e Aufschaltung gestattet

ja ☐ nein ☐ n. b. ☐

f technische Kontrolle

umfassend ☐ teilweise ☐ keine ☐

• Notebooks, Smartphones/Tablets usw. (LAN/WLAN-Zugang)

• Smartphones usw. (Synchronisation mit PCs)

• mobile Speichermedien (USB, SDcards, Digitalkameras, ...)

• Netzwerkhardware (Switches, WLAN-APs, Modems ...)

• sonstige Peripherie (z. B. Drucker)

Sind Ihre Netzwerk- und Sicherheitssysteme bereit für den Einsatz von ...?

ja ☐ nein ☐ n. b. ☐

g DNSSEC

h IPv6

i Haben Sie IPv6 bereits im Einsatz?

Pilotbetrieb ☐intern ☐extern ☐nein ☐

5.06 Content-Security (Malware, Spam, Filter)

a Welche Funktionen erwarten Sie von einer Endpoint-Security-Lösung?

• Virenschutz ☐• Spyware-Schutz ☐• Desktop/Client-Firewall ☐• SSL/TLS-Übertragungen prüfen ☐• Phishing-Abwehr ☐• Spam-Abwehr ☐• Inhaltsfilter ☐• Applikationskontrolle ☐• Verschlüsselung ☐• Data-Leak-/Loss-Prev. ☐• Intrusion Detection/Prev. ☐• Device-/Schnittstellenkontrolle ☐• Reporting-Tools ☐• Monitoring/Alerting ☐• zentrale Administration ☐

b Welche Vorsorge gegen Malware hat Ihr Haus getroffen?

• Einsatz von Viren-Scannern

ja ☐ nein ☐

c Update-Frequenz

– an der Firewall/Internet-Gateway

☐

_____ Std.

– auf dem Mail-/File-/Applikations-Server

☐

_____ Std.

– auf den PCs/Workstations

☐

_____ Std.

– auf mobilen Endgeräten

☐

_____ Std.

• stetige Schreib-/Leseprüfung (Virenwächter) auf PCs/Notebooks/Tablets

☐

• isolierte Testumgebung steht zur Verfügung

☐

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 ☐

5.07 Server-based Computing

a Der Einsatz von Terminalservern ist ...?

realisiert ☐geplant ☐nicht vorgesehen ☐

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

ausschließlich ☐bevorzugt ☐gleichwertig ☐nachrangig ☐gar nicht ☐

5.08 Smartphones/Tablets

Sind für Smartphones/Tablets von Mitarbeitern oder Partnern Ihres Hauses ...?

	realisiert	geplant	nicht vorgesehen
a Online-Zugriff auf schutzwürdige Unternehmensdaten	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b Speicherung schutzwürdiger Daten auf dem Gerät	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c Verschlüsselung gespeicherter Daten	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d Verschlüsselung von Sprachkommunikation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e Security-Suite (Virenschutz, Personal-Firewall, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f zentrales Management (Apps, Patches, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

g Welche Smartphone-Betriebssysteme sind in Ihrem Haus im Einsatz?

- ☐ Android
 ☐ BlackBerry
 ☐ iOS
 ☐ Symbian
 ☐ Windows Mobile
☐ Windows Phone
 ☐ Sonstige: _____

5.09 Unified Threat-Management (UTM) / Single- versus 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 erheblich	etwas	gleich gut	schlechter etwas	erheblich	n. b.
• 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 von nur einem	zweier Anbieter(n)	von drei oder mehr	n. b.
• Anti-Virus-Software (Multi-Engines bitte wie Multi-Vendor angeben)	<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"/>

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

- realisiert ☐
 geplant ☐
 nicht vorgesehen ☐
 n. b. ☐

5.10 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"/>

B

5.11 E-Mail-Sicherheit/Datenaustausch

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

	Signaturen	Verschlüsselung
• für alle E-Mails	<input type="checkbox"/>	<input type="checkbox"/>
• für externe Kommunikation	<input type="checkbox"/>	<input type="checkbox"/>
• für sensitive Nachrichten	<input type="checkbox"/>	<input type="checkbox"/>
• nie	<input type="checkbox"/>	<input type="checkbox"/>

b Welchen Standard verwenden Sie dabei?

• S/MIME	<input type="checkbox"/>
• (Open)PGP/GPG	<input type="checkbox"/>
• Sonstige	<input type="checkbox"/>

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

realisiert ☐ geplant ☐ nicht vorgesehen ☐

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

geschätzt ☐ ermittelt ☐ _____ % Spam

5.12 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			
• elektronischer Personalausweis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	mit Anbieterakkreditierung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

umfassend ☐ teilweise ☐ nein ☐

c Plant Ihr Haus, diese neuen elektronischen Ausweisfunktionen für seine Geschäftsprozesse zu nutzen?

ja ☐ nein ☐

d Sind Sie der Meinung, dass der elektronische Geschäftsverkehr durch den neuen Personalausweis für Bürger und Unternehmen interessanter wird?

ja ☐ nein ☐ n. b. ☐

5.13 Notfallvorsorge

a Besteht ein IT-Notfall/-Wiederanlaufkonzept?

ja ☐
nein ☐

b falls ja: Wurde dieses Konzept schriftlich fixiert?

☐ ja
☐ 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-Attacks
- gezielte Angriffe durch Einzeltäter (Hacker, Spionage, ...)
- physische Einwirkungen (Brand, Naturkatastrophen, Terror, ...)
- Zusammenbruch externer Infrastrukturen

☐ ☐
☐ ☐
☐ ☐
☐ ☐
☐ ☐
☐ ☐
☐ ☐
☐ ☐

d Liegen unternehmenswichtige Daten an räumlich unabhängigen Standorten vor

(z. B. Auslagerung/Spiegelung an Zweigstellen oder bei Kooperationspartnern/Dienstleistern)

ja ☐ nein ☐ n. b. ☐

e falls Sie einen Recovery-Vertrag haben:

Wie oft mussten Sie diesen 2012/2013 in Anspruch nehmen?

mehrmals ☐ einmal ☐ nie ☐ n. b. ☐

Was hat Ihr Haus für längere Ausfälle bereitgestellt?

	f Unternehmens-server/Mainframe			g Abt.-Rechner/Arbeitsplätze PC, LAN		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
• 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"/>

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 diese Dokumentation aktualisiert?

alle ____ Tage ☐ anlassbezogen ☐ nie ☐ n. b. ☐

5.14 Datenverluste/-rettung

a Hatte Ihr Haus 2012/2013 nennenswerte Probleme mit (zumindest zeitweise) un verfügbaren oder verlorenen Daten?

ja ☐ nein ☐ n. b. ☐

b falls ja: Was war(en) die Ursache(n)?

* PCs, Notebooks, Speichermedien, ...

Diebstahl/Verlust von Hardware*	<input type="checkbox"/>
Defekte von Hardware*	<input type="checkbox"/>
Softwarefehler	<input type="checkbox"/>
Bedienfehler	<input type="checkbox"/>
höhere Gewalt	<input type="checkbox"/>
Sonstiges	<input type="checkbox"/>

c falls ja: War eine Wiederherstellung aller Daten möglich?

	ja	nein
durch Rekonstruktion aus dem Backup	<input type="checkbox"/>	<input type="checkbox"/>
durch manuelle Neuerfassung	<input type="checkbox"/>	<input type="checkbox"/>
mit Datenrettungs-Tools durch eigene Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
Datenrettung durch Externe	<input type="checkbox"/>	<input type="checkbox"/>
durch Sonstiges	<input type="checkbox"/>	<input type="checkbox"/>

d 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.)

5.15 Computer-Forensik

a Wurde in Ihrem Haus 2012/2013 ein Sicherheits-vorfall rechtlich verfolgt?

ja ☐
nein ☐

b falls nein: Warum?

weil kein Vorfall	<input type="radio"/>
mangels Verfolgungsinteresse	<input type="radio"/>
mangels Wissen um Ermittlungsmöglichkeiten	<input type="radio"/>
n. b.	<input type="radio"/>

5.16 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?

B

5.17 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"/>

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

d Welche Aussagen zur Auswahl vertrauenswürdiger Partner im IT-Sicherheitsumfeld treffen auf Ihr Haus zu?

	ja	nein	n. b.
• Wir konzentrieren die Zusammenarbeit auf einen Partner, der uns umfassend in allen ISi-Fragen beraten kann.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Für uns sind Reputation und Leistungsspektrum eines Partners besonders wichtig.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Wir bevorzugen kurzfristige Partnerschaften, die sich nach dem Best-Price-Prinzip ergeben.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Wir wechseln häufig die Partner, um möglichst viele verschiedene Meinungen zu erfahren.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.18 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"/>	• Betriebssystempflege/Administration	<input type="checkbox"/>
• Managed Firewall/IDS/IPS	<input type="checkbox"/>	• gesamte(s) Rechenzentrum/IT	<input type="checkbox"/>
• Content-Security/Virenabwehr	<input type="checkbox"/>	• Notfallvorsorge/Business-Continuity	<input type="checkbox"/>
• Spamabwehr	<input type="checkbox"/>	• Anwendungssysteme	<input type="checkbox"/>
• E-Mail-Betrieb	<input type="checkbox"/>	• Datenbank-Systeme, Werkzeuge	<input type="checkbox"/>
• Netzwerk-Management	<input type="checkbox"/>	• Haustechnik	<input type="checkbox"/>
• Datensicherung, Backup-Lösungen	<input type="checkbox"/>	• Datenschutz	<input type="checkbox"/>
• Archivierung, Dokumentation	<input type="checkbox"/>	• Vernichtung von Datenträgern (Papier, IT)	<input type="checkbox"/>
• Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung	<input type="checkbox"/>	• Wachschutz/Bewachung	<input type="checkbox"/>

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

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

	ja	nein	regelmäßig	anlassbezogen	nie	n. b.
• mit expliziten Anforderungen an die ISi?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mit expliziten Anforderungen an den Datenschutz?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mit Regelungen zu Haftungsübernahme oder Schadensersatz?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

e falls ja: Kontrolle erfolgt ...

f 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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Datenschutz	<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"/>
• 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"/>
• Transparenz/Kontrollierbarkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

g 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.
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

h 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.
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

i Welche Cloud-Plattformen/Infrastruktur-Services nutzt Ihr Haus in nennenswertem Umfang oder plant dies in den kommenden zwei Jahren?

	realisiert	geplant	nicht vorgesehen		realisiert	geplant	nicht vorgesehen
Amazon Web Services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	VMWare Hybrid Cloud/vCloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Rackspace Cloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Red Hat Cloud Infrastructure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Open Stack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	IBM Smart Cloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Microsoft Azure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Google Computer Engine	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Citrix Cloud Platform/Stack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Sonstige	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.19 Versicherungen

a Hat Ihr Haus hinsichtlich IT-Risiken eine Spezialversicherung (z. B. Datenlöschung/-diebstahl, Betriebsunterbrechung durch Malware/Angriffe, Imageschäden, Spionage o. Ä.) abgeschlossen? ja ☐ nein ☐

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

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

5.20 Anbieter

a 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?

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

	ja	nein		ja	nein
• kryptografische Grundlagenarbeit	<input type="radio"/>	<input type="radio"/>	• Technische Richtlinien	<input type="radio"/>	<input type="radio"/>
• IT-Sicherheitsberatung	<input type="radio"/>	<input type="radio"/>	• Deutscher IT-Sicherheitskongress	<input type="radio"/>	<input type="radio"/>
• Zertifizierung	<input type="radio"/>	<input type="radio"/>	• Hotline für Bürger (z.B. zu Malware)	<input type="radio"/>	<input type="radio"/>
• Allianz für Cyber-Sicherheit	<input type="radio"/>	<input type="radio"/>	• Web-Angebot www.bsi.bund.de	<input type="radio"/>	<input type="radio"/>
• CERT-Bund	<input type="radio"/>	<input type="radio"/>	• Website „BSI für Bürger“	<input type="radio"/>	<input type="radio"/>
• IT-Grundschutz-Kataloge	<input type="radio"/>	<input type="radio"/>	• BSI-Newsletter	<input type="radio"/>	<input type="radio"/>
• IT-Grundschutz-Hotline	<input type="radio"/>	<input type="radio"/>	• Informationsangebote des Bürger-CERT	<input type="radio"/>	<input type="radio"/>
• Leitfaden IT-Sicherheit	<input type="radio"/>	<input type="radio"/>	• BSI-Auftritt auf Facebook	<input type="radio"/>	<input type="radio"/>
• Studien-/Buch-Publikationen	<input type="radio"/>	<input type="radio"/>	• BSI-Auftritt auf Xing	<input type="radio"/>	<input type="radio"/>
• BSI-Standards	<input type="radio"/>	<input type="radio"/>	• BSI-Forum in der <kes>	<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 —
<kes> Redaktion
Postfach 1234
55205 Ingelheim

(Anschriftsfeld für Versand im C4-Fensterumschlag)

Ihre „Dankeschön-Prämien“

A

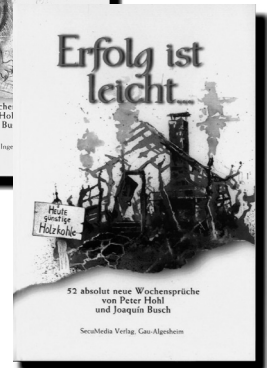
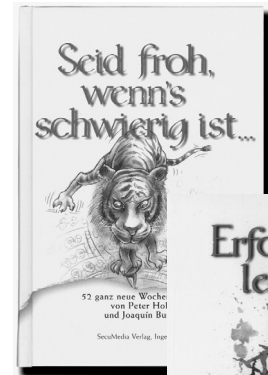


V9 Micro-Lenser, die „Taschenlampe am Schlüsselbund“ von Zweibrüder Optoelectronics

A+B



Kopflampe SEO5 von LED Lenser



zwei Sprüchebücher von Peter Hohl



Notebook-Tasche von Digittrade – das robuste Außenmaterial und Innenpolster bieten einen Rund-um-Schutz für Laptops

Leatherman Tool
SQUIRT PS4



Alle Prämien verfügbar solange Vorrat reicht.

Ich bin Teilnehmer der <kes>/Microsoft-Sicherheitsstudie 2014

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
- ☐ zwei Sprüchebücher

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

- ☐ Kopflampe
- ☐ Leatherman Multi-Tool
- ☐ Notebook-Tasche

Bitte Tasche aussuchen unter www.kes.info/studie-geschenk und hier eintragen:

.....
Größe (Zoll) Name der Tasche

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

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

* (bitte bevorzugtes Präsent mit „1“ ankreuzen
falls vergriffen, bitte Alternative mit „2“ und/oder „3“ markieren)

Firma / Behörde

Name, Vorname

Straße / Postfach

Land / PLZ / Wohnort

Datum

Unterschrift