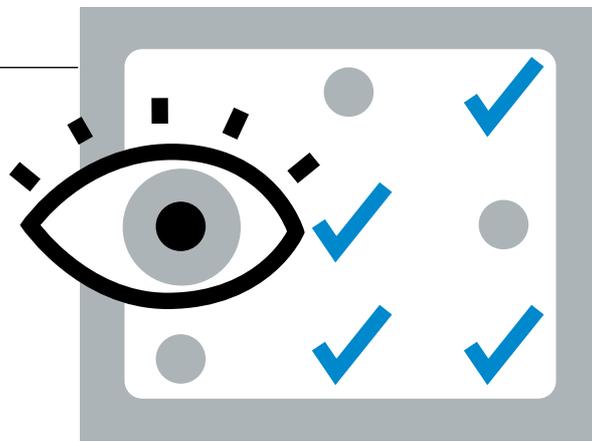


Checkliste zur Informations-Sicherheit



<kes> **Microsoft**
Sicherheitsstudie

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.

Normalerweise finden Sie in der <kes> vor allem Antworten. Alle zwei Jahre gibt es allerdings etliche Seiten, die (vordergründig) nur voller Fragen stecken. Einerseits bereiten wir damit natürlich den Weg für einen ausführlichen Lagebericht zur Informationssicherheit (ISI) im deutschsprachigen Raum. Gleichzeitig handelt es sich bei dem Fragenkatalog aber um eine Checkliste, deren Beantwortung jedem Ausfüller unmittelbar wertvolle Einblicke in die Sicherheitslage des eigenen Hauses geben dürfte.

Als Teilnehmer der <kes>/Microsoft-Sicherheitsstudie gewinnen Sie daher gleich vierfach: Zunächst einmal sofort durch die „Selbst-Einschätzung“ im Zuge der Beschäftigung mit dem Fragebogen – später dann durch das Gesamtbild der Sicherheit, das die <kes> nach der Auswertung aller Einsendungen publiziert und das durch Ihre wertvollen Angaben erst möglich wird.

Neben der veröffentlichten Auswertung erhalten alle Teilnehmer der Studie – Vorteil Nr. 3 – exklusiven Online-Zugriff auf die tabellarische Detailauswertung *aller* Fragen, sodass Ihnen ein noch umfassenderer Vergleich der eigenen Sicherheitssituation mit den kumulierten Daten des Teilnehmerfelds möglich ist.

Und last, not least – Gewinn Nr. 4 – erhalten Sie als Einsender eines ausgefüllten Fragebogens als Bonus für Ihre persönlichen Bemühungen ein Dankeschön-Geschenk vom SecuMedia-Verlag. Dabei haben Sie die Wahl zwischen drei fachlichen Publikationen (Webserver-Sicherheitsstudien des BSI und Sicherheits-Kompendium), einer „LED-Mikro-Taschenlampe“ oder – zum Regenerieren der kleinen grauen Zellen – einem Sammelband mit den neuesten Aphorismen von Peter Hohl (vgl. www.wochensprueche.de). Näheres hierzu finden Sie auf Seite 66.

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/studie2004/ 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 2004

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

_____ Sollten Sie die Anonymität selbst sicherstellen wollen, können Sie Coupon und Fragebogen auch getrennt einsenden. Bitte beachten Sie dazu die Hinweise auf den Seiten 65 und 66.

_____ 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

Vielen Dank für freundliche Unterstützung

Die folgenden Unternehmen fördern die Durchführung unserer aktuellen Sicherheitsstudie:

Microsoft®

Aladdin®
SECURING THE GLOBAL VILLAGE
Aladdin.de



CLEARSWIFT™

DIM

entrada
IT-Security

GROUP
TECHNOLOGIES



INFOAG

NOKIA
CONNECTING PEOPLE



ROG



SOLSOFT

SOPHOS

UIMC[®]
DR. VOSSBEIN
GmbH & Co KG

T · Systems

Für zusätzliche Anregungen und Hinweise bedanken wir uns beim Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie bei der Hans-Joachim Gaebert Unternehmensberatung. 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

Der diesjährige Fragebogen kommt in völlig neuer Aufmachung daher. 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 Notensstufe 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 1.04: eine oder mehrere „ja-Antworten“ schließen „nein“ und „n. b.“ aus).

Für weitere Fragen zu den Fragen oder Antwortmöglichkeiten haben wir die spezielle Mail-Adresse checkliste2004@kes.info eingerichtet. Auf www.kes.info/studie2004/ werden wir zudem eine FAQ-Sammlung pflegen.

1.03 Welche Internetnutzung gestattet Ihr Unternehmen den Mitarbeitern?

	a geschäftliche Nutzung von			b private Nutzung gestattet
	Multimedia-Diensten	WWW	E-Mail	
• für alle Mitarbeiter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• für spezielle Mitarbeiter/Abteilungen/Bereiche	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• nur an ausgewählten Arbeitsplätzen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Zugang generell nicht gestattet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• n. b.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

1.04 Wurde in Ihrem Unternehmen bereits versucht, über das Internet ...? ja nein

• Rechner zu hacken	<input type="checkbox"/>	<input type="checkbox"/>
• Daten unbefugt zu lesen	<input type="checkbox"/>	<input type="checkbox"/>
• Daten zu verändern	<input type="checkbox"/>	<input type="checkbox"/>
• Verbindungsdaten abzuhören	<input type="checkbox"/>	<input type="checkbox"/>
• die Verfügbarkeit zu beeinträchtigen	<input type="checkbox"/>	<input type="checkbox"/>
• nichts von alledem	<input type="checkbox"/>	<input type="checkbox"/>
• n. b. oder „kein Internetzugang“	<input type="checkbox"/>	<input type="checkbox"/>

1.05 Ist bereits der Versuch unternommen worden, auf Ihrem WWW-Server ...? ja nein

• Seiten zu verändern (Vandalismus)	<input type="checkbox"/>	<input type="checkbox"/>
• Daten auszuspionieren	<input type="checkbox"/>	<input type="checkbox"/>
• Daten zu löschen	<input type="checkbox"/>	<input type="checkbox"/>
• Daten in betrügerischer Absicht zu manipulieren	<input type="checkbox"/>	<input type="checkbox"/>
• Angebote lahmzulegen (Denial of Service)	<input type="checkbox"/>	<input type="checkbox"/>
• nichts von alledem	<input type="checkbox"/>	<input type="checkbox"/>
• n. b. oder „kein Webserver“	<input type="checkbox"/>	<input type="checkbox"/>

1.06 Hatten Sie 2003 Vorfälle mit Malware?

	File-Viren	Boot-Viren	Makro-Viren	Würmer	Troj. Pferde/Backdoors
a • ja, und zwar über	<input type="radio"/>				
- Datenträger (CD-ROM, Diskette, ...)	<input type="checkbox"/>				
- internes Netz	<input type="checkbox"/>				
- E-Mail	<input type="checkbox"/>				
- Internet-Download	<input type="checkbox"/>				
- Internet (autom. Verbreitung)	<input type="checkbox"/>				
- WWW-Seite (aktive Inhalte)	<input type="checkbox"/>				
- unbekannte Herkunft	<input type="checkbox"/>				
• nein	<input type="radio"/>				
• n. b. oder nicht registriert	<input type="radio"/>				
b • im Vergleich zu 2002: weniger Fälle	<input type="radio"/>				
• im Vergleich zu 2002: mehr Fälle	<input type="radio"/>				

1.07 Aufwand durch Malware-Infektion/Fehlalarm

Wie hoch schätzen Sie in Ihrem Haus verursacht durch eine einzelne:	a Ausfallzeit	b Kosten	c Häufigkeit des Auftretens
• Virus-/Wurm-Infektion	_____ Std.	_____ €	_____ mal/Jahr
• Fehlalarm (unbegründete Fehlermeldung)	_____ Std.	_____ €	_____ mal/Jahr
• unbegründete Warnung (Hoax)	_____ Std.	_____ €	_____ mal/Jahr

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

1.08 Gab es 2002 oder 2003 durch die folgende Malware nennenswerte Beeinträchtigungen

in Ihrem Unternehmen	ja	nein	n. b. oder keine Daten verfügbar
• Klez	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Bugbear	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Slammer/SQLExp	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Blaster/Lovsan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Sobig.F	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

• auslösendes Ereignis _____

• betroffene Anwendung / Systeme _____

• Ausfallzeit _____ Std. • direkte Kosten _____ € • Rekonstruktionsaufwand _____ €

• Konsequenzen für den Unternehmenserfolg bzw. die Aufgabenerfüllung _____

2.00 Management und Organisation der ISi

2.01 Welchen Stellenwert hat die ISi für Ihr Top-Management?

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

2.02 Aufgabenverteilung/Verantwortlichkeit

a Gibt es in Ihrem Unternehmen

b Wer ist verantwortlich für:

	<input type="checkbox"/> zentraler ISi-Beauftragter	<input type="checkbox"/> dezentraler ISi-Beauftragter	<input type="checkbox"/> zentraler Datenschutzbeauftragter	<input type="checkbox"/> dezentraler Datenschutzbeauftragter	<input type="checkbox"/> ISi-Ausschuss (o. ä.)	<input type="checkbox"/> Leiter IV / DV / RZ	<input type="checkbox"/> IV / DV-Revision	<input type="checkbox"/> Leiter Organisation	<input type="checkbox"/> Leiter Sicherheit/Werkschutz	<input type="checkbox"/> Administratoren	<input type="checkbox"/> Benutzerservice	<input type="checkbox"/> DV-orientierter Jurist	<input type="checkbox"/> Top-Management	<input type="checkbox"/> Einkauf/Beschaffung	<input type="checkbox"/> jeweilige Fachabteilung	<input type="checkbox"/> andere
• Formulierung der ISi-Strategie (Ziele, Rahmenbed., Ressourcen)	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Sensibilisierung / Schulung der Nutzer	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Durchführung von Risikoanalysen/Sicherheitsanalysen	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Erstellung von Konzepten, Richtlinien	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Beschaffung und Betrieb von																
- Servern	<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"/>	<input type="radio"/>	<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"/>	<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"/>	<input type="radio"/>
- mobilen Endgeräten	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
- technischer Infrastruktur (z. B. Klimaanlage, Gefahrenmeldeanl.)	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
- Software (inkl. Lizenzverwaltung)	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Wirtschaftlichkeit der IT-Sicherheit	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Notfall- und Eskalationsmaßnahmen/Business Continuity	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Prüfung/Einhaltung gesetzlicher Vorgaben	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.03 Wie beurteilen Sie den Kenntnisstand zur ISi in Ihrem Unternehmen?

	sehr gut	gut	mittel	eher schlecht	n. b.
• Top-Management	<input type="radio"/>				
• Mittelmanagement	<input type="radio"/>				
• IT-Sicherheitsfachleute	<input type="radio"/>				
• Anwender in hochsensitiven Bereichen	<input type="radio"/>				
• Anwender in weniger sensitiven Bereichen	<input type="radio"/>				

2.04 Wen informieren/schulen Sie über Fragen der ISi?

	gar nicht	regelmäßig (min. 1xjähr.)	gelegentlich / zu speziellen Anlässen	n. b.
• Benutzer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• IV-/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"/>

2.05 Welche Ausbildungsmethoden setzt Ihr Unternehmen auf dem Gebiet der ISi bevorzugt ein?

	häufig	gelegentlich	nie	n. b.
• interne Schulungen durch Frontalunterricht, möglichst flächendeckend	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• interne Schulungen durch Frontalunterricht für Spezialgruppen	<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 (Schulungsunterlagen) zum Selbstlernen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• (Multimediale) Lern-CDs zum Selbstlernen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Online-Trainings-Anwendungen/-Tools (Intranet)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.06 Wo informieren Sie sich über ISi?

- CeBIT IT-SecurityArea (SYSTEMS) infosecurity BSI-Kongress ISSE Security Essen
- Konferenzen / Kongresse / Seminare (welche?) _____
- Zeitschriften / Magazine (welche?) _____
- Mailinglisten (welche?) _____
- Internet / WWW
(bitte nennen Sie die URLs Ihrer wichtigsten Informationsquellen) _____

2.07 Wo erhalten Sie Informationen über aktuelle Sicherheits-Updates?

- a • aktiv vom Hersteller (push) (s. u.)
 - durch Dritte (push, z. B. Mailingliste) (welche? _____)
 - auf Informationsseiten des Herstellers (pull)
 - auf Informationsseiten von Dritten
(bitte nennen Sie die wichtigsten URLs) _____
- b • In welcher Frequenz prüfen Sie passive Kanäle?
 - täglich wöchentlich monatlich quartalsweise
 - seltener/unregelmäßig gar nicht
- c • Welche Hersteller-Bulletins haben Sie abonniert?
 - IBM Microsoft SOPHOS Symantec
 - Sonstige: _____

2.08 Wie verwalten Sie (in nennenswertem Umfang) Ihre Systeme?

	Netzwerk-Systeme		Host/PC-Systeme	
	ja	nein	ja	nein
• manuell	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mit Managementlösungen der jeweiligen Hersteller nämlich _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• mit zentralen Managementlösungen nämlich _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.09 CERT/CSiRT

- a Unterhält Ihr Unternehmen ein eigenes Computer Emergency oder Incident Response Team (CERT/CSiRT)?
 - ja nein
- b Nutzt Ihr Unternehmen Dienstleistungen eines externen CERT/CSiRT?
 - ja, kostenpflichtig ja, kostenlos nein
- c Falls ja: Von welchem CERT/CSiRT? _____

2.10 Outsourcing?

- a Betreibt Ihr Unternehmen Outsourcing
 - ja nein
- b Falls ja: Welche Funktionen haben Sie ausgelagert?

• Auftragsentwurf, Arbeitsvorbereitung, Operating	<input type="checkbox"/>	• gesamtes Rechenzentrum	<input type="checkbox"/>
• Überwachung, Kontrolle, Qualitätssicherung	<input type="checkbox"/>	• Notfallvorsorge/Business Continuity	<input type="checkbox"/>
• Managed Firewall/IDS	<input type="checkbox"/>	• Online-Anwendungssysteme	<input type="checkbox"/>
• Netzwerk-Management	<input type="checkbox"/>	• Datenbank-Systeme, Werkzeuge	<input type="checkbox"/>
• Datensicherung, Backup-Lösungen	<input type="checkbox"/>	• Haustechnik	<input type="checkbox"/>
• Verwaltung, Dokumentation, Archivierung	<input type="checkbox"/>	• Datenschutz gemäß BDSG	<input type="checkbox"/>
• Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung	<input type="checkbox"/>	• Entsorgung von Datenträgern (Papier, EDV)	<input type="checkbox"/>
• Betriebssystempflege	<input type="checkbox"/>	• Sonstiges (bitte nennen):	<input type="checkbox"/>
- c Falls ja: Haben Sie Service-Level-Agreements/vertragliche Vereinbarungen mit dem Outsourcer?

	ja, mit regelmäßiger Kontrolle	ja, mit anlassbezogener Kontrolle	ja, aber keine Kontrolle	nein
• mit expliziten Anforderungen an die ISi?	<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"/>

2.11 ISi-Beratung

a Nutzt Ihr Haus externe ISi-Beratung ... ?

- ja, regelmäßig
- ja, gelegentlich
- nein

b Falls Ja: in welcher Form?

- Strategie- und Managementberatung
- Durchführung von Risikoanalysen und Konzeptentwicklung
- Durchführung von Schwachstellenanalysen
- Durchführung von Penetrationstests
- Umsetzung von Konzepten und Maßnahmen
- Kontrolle vorhandener Konzepte auf Eignung und Einhaltung
- Sonstiges (bitte nennen): _____

c Waren Sie mit der Beratung zufrieden?

- ja
- ja, mit Einschränkungen
- nein

2.12 Versicherungen

a Welche Versicherungen aus dem Bereich ISi haben Sie abgeschlossen / bereits in Anspruch genommen?

	abge- schlossen		ja und in Anspruch genommen			abge- schlossen		ja und in Anspruch genommen	
	nein	ja	nein	ja		nein	ja	nein	ja
• Elektronikversicherung					• Feuerversicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
- Sachversicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	• „Technologie-Police“ o. ä. (Kombination von Elektronik- u. Maschinenversicherung)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
- Datenversicherung/Softwareversicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	• Vertrauensschaden-Versicherung				
- Erweiterte Datenversicherung (inkl. Schäden durch Viren, fehlerhaftes Programmieren, versehentliches Löschen)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	- Computermisbrauch-Versicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
- Mehrkostenversicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	- Datenmissbrauch-Versicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
- Elektronik-Betriebsunterbrechungs- versicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	• Datenschutzversicherung				
• Sonstige _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	- Datenhaftpflicht-Versicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
					- Datenrechtsschutz-Versicherung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
					• keine	<input type="radio"/>			

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

3.00 ISi-Strategie und -Konzept

3.01 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"/>
• ein umfassendes, integriertes Sicherheitshandbuch	<input type="radio"/>	<input type="radio"/>
• schriftlich fixierte spezifische ISi- <i>Konzepte/Richtlinien</i>		
- zum Einsatz von Verschlüsselung	<input type="radio"/>	<input type="radio"/>
- zur Handhabung sensibler/kritischer Daten	<input type="radio"/>	<input type="radio"/>
- zur Nutzung von Internet, E-Mail, ...	<input type="radio"/>	<input type="radio"/>
- zum Softwareeinsatz auf PCs	<input type="radio"/>	<input type="radio"/>
- zur Nutzung mobiler Endgeräte (Notebook, PDA, ...)	<input type="radio"/>	<input type="radio"/>
- Sonstige _____	<input type="radio"/>	<input type="radio"/>
• schriftlich formulierte <i>Maßnahmen</i>	<input type="radio"/>	<input type="radio"/>

3.02 Wird die *Einhaltung* der vorgesehenen Maßnahmen geprüft?

- ja, durch die Revision
- ja, durch externe Sicherheitsberater
- ja, durch die eigene Sicherheitsabteilung
- ja, durch _____
- nein, sie wird nicht geprüft

3.03 Die (fortdauernde) *Eignung* der Konzepte / Richtlinien

a wird überprüft mithilfe von ...

	ja	nein
• (erneuten) Risikoanalysen	<input type="checkbox"/>	
• (erneuten) Schwachstellenanalysen	<input type="checkbox"/>	
• Simulationen oder Szenarien	<input type="checkbox"/>	
• Übungen (Notfall, Wiederanlauf)	<input type="checkbox"/>	
• Penetrationsversuchen	<input type="checkbox"/>	
• Sonstiges (bitte nennen) _____	<input type="checkbox"/>	
• Es erfolgt keine Überprüfung	<input type="checkbox"/>	<input type="radio"/>

b Die letzte Überprüfung fand statt (Monat und Jahr): _____

c Welche Reichweite hatte diese Überprüfung? alle geschäftskritischen Systeme einzelne Systeme nicht bekannt

d Führt die letzte Überprüfung zur Aufdeckung von Schwachstellen? ja nein

e Falls Ja:

• Die Schwachstellen wurden inzwischen beseitigt	<input type="radio"/>	
• Die Beseitigung dauert noch an	<input type="radio"/>	
• Es wurden keine Aktivitäten ergriffen	<input type="radio"/>	<input type="radio"/> nicht bekannt

3.04 Krisenplanung

a Besteht ein EDV-Notfall/-Wiederanlaufkonzept ... ?

• ja, schriftlich fixiert, verifiziert, validiert und freigegeben	<input type="radio"/>
• ja, schriftlich fixiert	<input type="radio"/>
• ja, aber nicht schriftlich	<input type="radio"/>
• nein	<input type="radio"/>

b 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"/>
• gezieltes Eindringen 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"/>

3.05 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	<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"/>

3.06 Beschaffung / Inbetriebnahme

a Sind Sicherheits-Aspekte für Ihr Haus bei der Beschaffung von IV-Systemen ... ?
ein Hauptkriterium eher zweitrangig eher unbedeutend

b Wird die Erfüllung von ISI-Anforderungen als Voraussetzung für die Inbetriebnahme verifiziert? ja nein

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

	a Kenntnis		b Relevanz		c Umsetzung		
	inhaltlich bekannt		relevant		bereits erfolgt		
	ja	nein	ja	nein	umfassend	teilweise	gering
• BDSG	<input type="radio"/>						
• TKG/TDSV/TKÜV	<input type="radio"/>						
• TDG/TDDSG	<input type="radio"/>						
• ZKDSG	<input type="radio"/>						
• SigG/SigV	<input type="radio"/>						
• KonTraG	<input type="radio"/>						
• GDPdU	<input type="radio"/>						
• Basel II	<input type="radio"/>						

- Basel II = Baseler Akkord, Eigenkapitalvorschriften für das Kreditgewerbe
 BDSG = Bundesdatenschutzgesetz
 TKG = Telekommunikationsgesetz, TDSV = Telekommunikationsdienstleistungsunternehmen-Datenschutzverordnung
 TKÜV = Telekommunikationsüberwachungsverordnung
 TDG = Teledienstgesetz, TDDSG = Teledienstschutzgesetz
 SigG/SigV = Signaturgesetz/-Verordnung
 KonTraG = Gesetz zur Kontrolle und Transparenz bei Aktiengesellschaften und publizitätspflichtigen Gesellschaften
 GDPdU = Grundsätze zu Datenzugriff und Prüfbarkeit digitaler Unterlagen
 ZKDSG = Zugangskontrolldiensteschutzgesetz

4.00 Methoden und Instrumente

4.01 Risikobewertung

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

- ja, für *alle* Anwendungen / Systeme b Falls ja: Welcher Prozentanteil der Anwendungen / Systeme hat einen sehr hohen Schutzbedarf bzw. ein sehr hohes Risiko? _____ %
 • ja, für *einzelne* Anwendungen / Systeme
 • nein

4.02 Wie wichtig sind die folgenden Kriterien für die Klassifizierung von

Anwendungen / Systemen in Ihrem Haus?	sehr wichtig	wichtig	unwichtig	n. b.
• direkter finanzieller Schaden an Hardware u. ä.	<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"/>
• Sonstiges (bitte nennen): _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4.03 Die folgenden methodischen Vorgehensweisen und Software-Tools...

	sind bereits im Einsatz	Einsatz ist geplant	Einsatz ist nicht vorgesehen	n. b. oder unbekannt
• Verfahren nach dem IT-Grundschriftbuch des BSI	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verfahren nach dem IT-Sicherheitshandbuch des BSI	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• checklistengetützte Schwachstellenanalyse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Sicherheitshandbuch von Softwarehersteller (Name): _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• softwaregestützte Standardmethode (Name): _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Softwareanalysetool	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Verfahren eines Beraters	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• selbstentwickeltes Verfahren	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Sonstiges (bitte nennen): _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• keine der genannten methodischen Vorgehensweisen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4.04 Im Rahmen von Prüfungen (z. B. durch interne Revision, Wirtschaftsprüfer) werden unter ISi-Aspekten geprüft:

• Konzeption und Zielsetzung	<input type="checkbox"/>	• Änderungshistorie (Change Management)	<input type="checkbox"/>
• Aufbauorganisation	<input type="checkbox"/>	• Virenschutz	<input type="checkbox"/>
• Ablauforganisation (z. B. für einzelne Vorgänge, Verfahren)	<input type="checkbox"/>	• Berechtigungskonzept	<input type="checkbox"/>
• Software (Korrektheit, Fehlerfreiheit usw.)	<input type="checkbox"/>	• Notfallkonzept	<input type="checkbox"/>
• Software-Entwicklung (inkl. Test- und Freigabeverfahren)	<input type="checkbox"/>	• physische Sicherheit	<input type="checkbox"/>
• Software-Einsatz	<input type="checkbox"/>	• Netzwerkstrategie/Firewalls	<input type="checkbox"/>
• Übereinstimmung der System-Konfiguration mit Vorgaben	<input type="checkbox"/>	• Sonstiges (bitte nennen): _____	<input type="checkbox"/>
• Datenklassifizierung und Zugriffsrechte	<input type="checkbox"/>	• nichts Derartiges	<input type="radio"/>

5.00 Sonstige ISi-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"/>
• Virenschutzmechanismen	<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"/>
• Intrusion Detection Systems	<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"/>
• Benutzerverzeichnis mit Security-Policy	<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"/>
• Authentisierung									
- 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	<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"/>
• Protokollierung unberechtigter Zugriffe	<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)	<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"/>
• 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 (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"/>
- 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	<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	<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	<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	<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"/>
- Fax	<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"/>
• 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"/>
- 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	<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"/>			
• Rückrufautomatik bei Modemzugriff	<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 Wie wichtig bewerten Sie folgende Komponenten eines unternehmensweiten Security-Managements?

	sehr wichtig	wichtig	unwichtig	n. b.
• plattformübergreifende Benutzerverwaltung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Single-Sign-On	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• zentrale Überwachung der eingesetzten Security-Systeme (z. B. Firewall, Applikations-Security-Systeme)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Alarm- und Eskalationssystem	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Intrusion Detection Systems (IDS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Kontrolle und Überwachung von Internet-Missbrauch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Virtual Private Networks (VPN)	<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"/>
• andere _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.03 Heterogenität/OpenSource

a Nutzen Sie aus Sicherheitsgründen auf verschiedenen Systemen oder Netzwerksegmenten Produkte mehrerer verschiedener Anbieter?	Einsatz von Produkten			
	nur einem	zweier Anbieter	von drei und und mehr	n. b.
• 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	<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"/>
• Sonstiges _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

c Setzt Ihr Unternehmen OpenSource Software ein? ja, aus Kostengründen ja, aus Sicherheitsgründen nein
ja, wegen: _____

5.04 Content Security (Malware, Spam, Filter)

a Haben Sie Vorsorge gegen Malware getroffen?	ja	nein	b Update-Frequenz
• nein	<input type="radio"/>	<input type="radio"/>	
• ja, wir benutzen Viren-Scanner	<input type="checkbox"/>	<input type="checkbox"/>	_____ Std.
- an der Firewall/Internet-Gateway	<input type="checkbox"/>	<input type="checkbox"/>	_____ Std.
- auf dem Mail-/File-/Applikationsserver	<input type="checkbox"/>	<input type="checkbox"/>	_____ Std.
- auf den PCs/Workstations	<input type="checkbox"/>	<input type="checkbox"/>	_____ Std.
- auf mobilen Systemen	<input type="checkbox"/>	<input type="checkbox"/>	_____ Std.
• ja, wir nutzen Prüfsummenprogramme	<input type="checkbox"/>	<input type="checkbox"/>	
• ja, wir nutzen online-Virenwächter auf PCs	<input type="checkbox"/>	<input type="checkbox"/>	
• isolierte Testumgebung steht zur Verfügung	<input type="checkbox"/>	<input type="checkbox"/>	
• andere Methode (bitte nennen): _____	<input type="checkbox"/>	<input type="checkbox"/>	

c Ist sichergestellt, dass Ihre Maßnahmen auch wirken ... ja nein nicht festgestellt

• gegen Makroviren bei Office-Dokumenten

• gegen online übertragene Schadsoftware (E-Mail-Anhang, Downloads)

d Haben Sie über eine reine Viren-Muster-Erkennung hinaus Content-Security-Komponenten im Einsatz	Gateway		Desktop	
	ja	nein	ja	nein
• für E-Mails (SMTP-Scan)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• für Web-Seiten (HTTP-Scan)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• für Downloads (FTP-Scan)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• für sonstige Applikationen (Instant + Messaging, P2P usw.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

e Wurde Ihre Content-Security-Lösung in Kombination mit einer Firewall installiert? ja nein

f Falls ja: Mit welcher Firewall? Check Point Cisco Netscreen Sonstige: _____

g Wie wichtig sind folgende Argumente für den Einsatz einer Content-Security-Lösung?
(1 = trifft voll zu ... 5 = trifft überhaupt nicht zu)

	1	2	3	4	5	n. b.
• Schutz der Netzwerk-Infrastruktur gegen Virus-Attacken usw.	<input type="radio"/>					
• Vermeidung rechtlicher Risiken aus der Nutzung von Internet/E-Mail	<input type="radio"/>					
• Erhalten der Netzwerkbandbreite	<input type="radio"/>					
• Erhöhte Mitarbeiterproduktivität durch eingeschränkte private E-Mail-/Web-Nutzung	<input type="radio"/>					

• Sonstiges: _____

h Wie wichtig sind die folgenden Kriterien für die Auswahl einer Content-Security-Lösung?
(1 = besonders wichtig ... 5 = unwichtig)

	1	2	3	4	5	n. b.
• Kosten	<input type="radio"/>					
• Funktionsumfang	<input type="radio"/>					
• zentrale Administrationsarbeit	<input type="radio"/>					
• „Marke“ (Image)	<input type="radio"/>					
• Hersteller-Support	<input type="radio"/>					
• Beratung/Service (Lieferant)	<input type="radio"/>					
• Return-on-Investment (ROI)	<input type="radio"/>					

i Welche Funktionen erwarten Sie von einer Content-Security-Lösung?
 Virenschutz Spam-Abwehr Inhaltsfilter Reporting-Tools Monitoring/Alerting

j Auf welchem Server-Betriebssystem sollte die Lösung arbeiten?
 Windows Linux Unix andere

k Wie hoch ist in Ihrem Unternehmen der Spam-Anteil bei E-Mails?
 geschätzt ermittelt ____% Spam

5.05 E-Mail-Verschlüsselung

a Nutzen Sie in Ihrem Unternehmen E-Mail-Verschlüsselung – sofern der Kommunikationspartner über einen Kryptoschlüssel verfügt?	b Welchen Standard verwenden Sie dabei?
• für alle E-Mails <input type="checkbox"/>	• S/MIME <input type="checkbox"/>
• für externe Kommunikation <input type="checkbox"/>	• (Open)PGP/GPG <input type="checkbox"/>
• für sensitive Nachrichten <input type="checkbox"/>	• sonstigen (bitte nennen)
• nie <input type="radio"/>	

5.06 Digitale Signaturen

a Nutzen Sie in Ihrem Unternehmen digitale/elektronische Signaturen?

	E-Mail	WWW (SSL)	Applikationen	nein
• zur Authentifizierung interner Kommunikation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
• bei B2B-Kommunikation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
• bei B2C-Kommunikation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
• im E-Government?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
• Sonstiges: _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b Welche Infrastruktur nutzen Sie für digitale/elektronische Signaturen?

	B2B-Server			B2C-Server			Client/PC			mobile Endgeräte		
	realisiert	geplant	nicht vor-gesehen									
• nur Software	<input type="radio"/>											
• Hardwaremodule	<input type="radio"/>											
• Hardware-Token	<input type="radio"/>											
• Chipkarten	<input type="radio"/>											
• „Klasse-2“-Chipkartenterminal (sichere PIN-Eingabe)	<input type="radio"/>											
• „Klasse-3“-Chipkartenterminal (mit eigenem Display)	<input type="radio"/>											
• lt. SigG												
– fortgeschrittene Signatur	<input type="radio"/>											
– qualifizierte Signatur	<input type="radio"/>											
– qualifizierte Signatur mit Anbieterakkreditierung	<input type="radio"/>											
• Sonstiges: _____	<input type="radio"/>											
• nichts von alledem	<input type="radio"/>	<input type="radio"/>										

5.07 Public Key Infrastructure (PKI)

a Planen Sie die Implementierung einer PKI? ja nein

b Für welche Zwecke nutzen Sie in Ihrem Unternehmen eine PKI?

	realisiert	geplant	nicht vorgesehen
• E-Mail-Verschlüsselung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Dateiverschlüsselung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Zugriffsrechte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Single-Sign-On	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Virtual Private Networks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Telearbeitsplätze/Remote Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Web-Zugriff (Portale, Intranet, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Sonstiges: _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5.08 Angriffserkennung

a Welche Logdaten wertet Ihr Unternehmen aus?

	Internet				Intranet/LAN			
	Auswertung min. 2 x pro Woche	Auswertung seltener, aber regelmäßig	Auswertung erfolgt anlassbezogen	keine Auswertung oder Protokollierung	Auswertung min. 2 x pro Woche	Auswertung seltener, aber regelmäßig	Auswertung erfolgt anlassbezogen	keine Auswertung oder Protokollierung
• Anti-Virus-Lösungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Firewall(s)	<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 Systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Netzkomponenten (Router, Switches etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Betriebssysteme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Web-/E-Commerce-Applikationen	<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 Applikationen: _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b Setzen Sie ein System ein, das Angriffe gegen Ihr Netzwerk erkennt und Sie davor schützt?

• ja, wir setzen ein *netzwerkbasiertes* Intrusion Detection System (IDS) ein

• ja, wir setzen ein *hostbasiertes* Intrusion Detection System (IDS) ein

• nein, wir setzen Virens Scanner und Firewalls ein

• nein

c Falls Sie bislang *kein* netzwerkbasiertes IDS einsetzen: Planen sie den Einsatz eines solchen Systems?

ja, in den nächsten 12 Monaten ja, in den nächsten 24 Monaten nein

d Falls Sie zukünftig den Einsatz eines netzwerkbasierten IDS planen:

Welches Budget steht dafür zur Verfügung? _____ €

e Hat Ihr Unternehmen in den letzten 12 Monaten einen Penetrationstest in Auftrag gegeben?

• ja, auf

– die Internet-Infrastruktur

– kritische Systeme von innen

– Sonstiges _____

• nein

5.09 Notfallvorsorge

a Halten Sie wesentliche Komponenten Ihrer Informationsverarbeitung an verschiedenen Orten vor?

	Auslagerungsarchiv	Roboter-Systeme	gespiegelte Daten	zus. Rechner/Cluster
• ja, in einem getrennten Brandabschnitt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– in einem anderen Gebäude	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– bei einem Kooperationspartner	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– bei einem externen Anbieter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• nein	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

b Was haben Sie für längere Ausfälle bereitgestellt?

	Unternehmensserver/Mainframe			Abt.-Rechner 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 (mit Überkapazität)	<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"/>
• Ersatzräume für Personal (mit installierter Infrastruktur)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Ersatzräume für Personal (ohne installierte Infrastruktur)	<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"/>
• nichts	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	

c Halten Sie es für notwendig, vor einer Entscheidung über Recovery-Maßnahmen ein strategisches Konzept zu erstellen?

	Haben Sie ein solches Konzept?
• ja, und zwar	<input type="radio"/>
– Durchführung mit eigenen Kräften	<input type="radio"/>
– mit externer Beratung	<input type="radio"/>
– mit Einbindung der Geschäftsführung in diese konzeptionelle Arbeit	<input type="radio"/>
• nein	<input type="radio"/>

d Falls Sie einen Recovery-Vertrag haben:

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

e Existiert in Ihrem Hause eine Notfalldokumentation?	ja	in Arbeit	geplant	nein
• manuelles Handbuch (PC-Textsystem, Host-Texte)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• online gestütztes Handbuch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• online-Anwendung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

f Was umfasst Ihre Dokumentation?	ja	teilweise	nein
• Aktionspläne für den K-Fall	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Recovery Units mit			
– Aktionsplan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Benötigte Ressourcen (HW, SW, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Aktionspläne Störungen im Tagesbetrieb	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• IT-Dokumentation (Arbeitsanweisungen)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Allgemeine Dokumentationen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Inventarisierung			
– Hardware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Software	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
– Infrastruktur (Klima, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

g Welches Produkt setzen Sie dafür ein? _____

h Ist das eingesetzte Notfall-Produkt in folgenden Varianten verfügbar?	ja	nein
• Browser basierend	<input type="radio"/>	<input type="radio"/>
• Client/Server basierend	<input type="radio"/>	<input type="radio"/>
• Mobil (auf USB-Speicher)	<input type="radio"/>	<input type="radio"/>
• Datenbank gestützt (Oracle, DB2, etc.)	<input type="radio"/>	<input type="radio"/>
• Mandantenfähig	<input type="radio"/>	<input type="radio"/>

i Das eingesetzte Produkt benötigt zum Einsatz andere Produkte?	ja	teilweise	nein
• Textverarbeitungssoftware (z. B. Word)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Planungssoftware (z. B. MS-Projekt)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Drucksoftware (z. B. Word, Crystal Report)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

j Wie oft wird die Dokumentation aktualisiert alle _____ Tage anlassbezogen nie

k Deckt das eingesetzte Produkt die Anforderungen nach ITIL/BSI-Grundschutzhandbuch ab? ITIL BSI nein n. b.

l Werden „abgearbeitete“ Pläne zu Revisionszwecken archiviert und können jederzeit wieder eingesehen werden? ja nein

m Glauben Sie, dass eine gesicherte Aktualität der gesamten Dokumentation durch den Einsatz im Tagesbetrieb erreichbar oder verbesserbar ist?

n Glauben Sie, dass durch den täglichen/regelmäßigen Umgang mit dem Tool die Nutzung/Handhabung im K-Fall vereinfacht wird?

o Werden die Notfallübungen anhand der Dokumentation durchgeführt?

p Wird die Dokumentation hierbei auf Aktualität und Vollständigkeit überprüft?

q Wurden bereits Störfälle auf Basis der Dokumentation bearbeitet?

5.10 Überspannungsschutz

a Ist Ihre EDV mit Überspannungsschutzbausteinen ausgerüstet? ja nein

- in 230/400 V Versorgungsleitungen
- in Daten-, Telefon- und Modemleitungen
- kein Überspannungsschutz

b Wenn *kein* Überspannungsschutz vorhanden ist: Was sind die Gründe?

- zu teuer
- zu kompliziert
- wir haben LWL
- Risiko erscheint uns nicht gravierend
- Überspannungsschutz ist geplant

5.11 Anbieter

a Welche der folgenden Unternehmen, die Sicherheitsprodukte anbieten, sind Ihnen bekannt?

- | | |
|--|--|
| <input type="checkbox"/> Aladdin | <input type="checkbox"/> Lampertz |
| <input type="checkbox"/> Adolphs | <input type="checkbox"/> Litcos |
| <input type="checkbox"/> Allasso | <input type="checkbox"/> Network Associates (NAI) |
| <input type="checkbox"/> Clearswift | <input type="checkbox"/> Nokia |
| <input type="checkbox"/> Computer Links | <input type="checkbox"/> Norman Data Defense Systems |
| <input type="checkbox"/> Design Institut München (DIM) | <input type="checkbox"/> Packet Alarm (VarySys Technologies) |
| <input type="checkbox"/> Entrada | <input type="checkbox"/> Pegatec |
| <input type="checkbox"/> eSeSiX | <input type="checkbox"/> Rainbow |
| <input type="checkbox"/> Eurosec | <input type="checkbox"/> ROG |
| <input type="checkbox"/> F-Secure | <input type="checkbox"/> Rohde & Schwarz SIT |
| <input type="checkbox"/> GeNUA | <input type="checkbox"/> Secaron |
| <input type="checkbox"/> Group Technologies | <input type="checkbox"/> Solsoft |
| <input type="checkbox"/> HiSolutions | <input type="checkbox"/> Sophos |
| <input type="checkbox"/> ICON (jetzt NOXS) | <input type="checkbox"/> Symantec |
| <input type="checkbox"/> Info AG | <input type="checkbox"/> Trend Micro |
| <input type="checkbox"/> Kroll Ontrack | <input type="checkbox"/> es fehlen: _____ |

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

6.00 BSI

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

	ja	nein		ja	nein
• IT-Sicherheitshandbuch	<input type="radio"/>	<input type="radio"/>	• kryptographische Grundlagenarbeit	<input type="radio"/>	<input type="radio"/>
• IT-Grundschutzhandbuch	<input type="radio"/>	<input type="radio"/>	• Beratung	<input type="radio"/>	<input type="radio"/>
• Schriften/Faltblätter zur IT-Sicherheit	<input type="radio"/>	<input type="radio"/>	• Viren-Hotline	<input type="radio"/>	<input type="radio"/>
• Leitfaden IT-Sicherheit	<input type="radio"/>	<input type="radio"/>	• Viren-Newsletter	<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"/>
• Zertifizierung	<input type="radio"/>	<input type="radio"/>	• BSI-Kongress	<input type="radio"/>	<input type="radio"/>

6.02 Haben Sie sich bereits mit den folgenden internationalen ISi-Kriterien befasst?

	ja	nein	nicht bekannt
• ITSEC	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Common Criteria	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• BS 7799 / ISO IEC 17799	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• Fips 140	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• ITIL	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
• COBIT	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6.03 Zertifizierte Sicherheitsprodukte

	ja	nein
a Setzen Sie zur Zeit zertifizierte 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 nach Ihrer Meinung einen höheren Preis?	<input type="radio"/>	<input type="radio"/>
d Werden Sie in Zukunft zertifizierte (Sicherheits-)Produkte bevorzugt einsetzen?	<input type="radio"/>	<input type="radio"/>

noch unentschieden

7.00 Statistische Angaben

7.01 Bitte geben Sie uns einige Informationen zur Hardware-Ausstattung Ihres Hauses (ggf. bitte schätzen):

	Stück		Stück
• Mainframe	_____	• Server	_____
• Clients/PCs	_____	• mobile Endgeräte (Notebooks, PDAs, ...)	_____
• LAN / PC-Netze	_____	• WAN (inkl. VPN und gemietete Netze)	_____
• WLAN	_____	• Heim-/Telearbeitsplätze (auch Teilzeit)	_____

7.02 Zu welcher Branche gehört Ihr Haus?

Bitte nur eine Nennung; ggf. entscheiden Sie sich bitte für die wichtigste.

• Energieversorgung	<input type="radio"/>	• Berater	<input type="radio"/>
• Handel	<input type="radio"/>	• Telekommunikationsdienstleister/Provider	<input type="radio"/>
• Handwerk	<input type="radio"/>	• Behörden	<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"/>
		• Sonstiges (Bitte nennen): _____	<input type="radio"/>

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

• Deutschland	<input type="radio"/>	• Schweiz	<input type="radio"/>	• Österreich	<input type="radio"/>	• Sonstiges (Bitte nennen): _____	<input type="radio"/>
---------------	-----------------------	-----------	-----------------------	--------------	-----------------------	-----------------------------------	-----------------------

7.04 Mitarbeiterzahl

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

7.05 Welche Funktionsbezeichnung trifft auf Sie am ehesten zu?

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

7.06 Der Umsatz bzw. die Bilanzsumme Ihres Hauses betrug im Jahr 2003 ...
(falls nicht bekannt, bitte Angabe für 2002 bzw. das letzte Wirtschaftsjahr)

- _____ € Umsatz
- _____ € Bilanzsumme (nur für Kreditinstitute / Versicherungen)
- nicht relevant, da Behörde oder ähnliches *(Bitte ankreuzen)*

7.07 Budget

- a Das Budget für Informationsverarbeitung (inkl. Personalkosten) umfasst im Jahr 2004 _____ €
- | | | |
|--|-----------------------|-----------------------|
| | geschätzt | ermittelt |
| | <input type="radio"/> | <input type="radio"/> |
- b Der Anteil für ISi-Maßnahmen (inkl. Personalkosten) an diesem Budget beträgt _____ %
- | | | |
|--|-----------------------|-----------------------|
| | <input type="radio"/> | <input type="radio"/> |
|--|-----------------------|-----------------------|
- c Von den Projekt- und Betriebsbudgets entfallen für die IT-Sicherheit von Anwendungen mit _____ Schutzbedarf
- | | | | |
|------------|---------|---------|---------|
| | hoch | mittel | niedrig |
| • Projekte | _____ % | _____ % | _____ % |
| • Betrieb | _____ % | _____ % | _____ % |

7.08 Bitte schätzen Sie: Wenn in Ihrem Haus alle elektronisch gespeicherten Daten vernichtet würden, wie hoch würden Sie den Verlust beziffern?

Geschätzter Betrag: _____ €

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

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

So garantieren wir Vertraulichkeit:

- Dieser Abschnitt mit Ihrer Anschrift wird in der <kes>-Redaktion abgetrennt, bevor der Fragebogen zur Auswertung geht. Der Abschnitt dient dazu, den Teilnehmern nach der Auswertung das Ergebnis der <kes>/Microsoft-Sicherheitsstudie zuzusenden.
- Sie können diesen Abschnitt auch selbst abtrennen und getrennt vom anonymen Fragebogen einsenden. Dabei steht Vertrauen gegen Vertrauen: Die <kes>-Redaktion garantiert Ihnen, dass Fragebogen und Abschnitt streng getrennt bleiben. Sie garantieren uns, dass Sie nicht etwa nur den Abschnitt, sondern auch einen ausgefüllten Fragebogen abgeschickt haben.

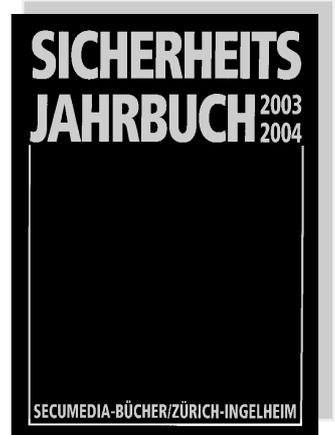
Herrn Peter Hohl
- persönlich -
Redaktion <kes>
Postfach 1234
55205 Ingelheim

Ihre „Dankeschön-Prämien“



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

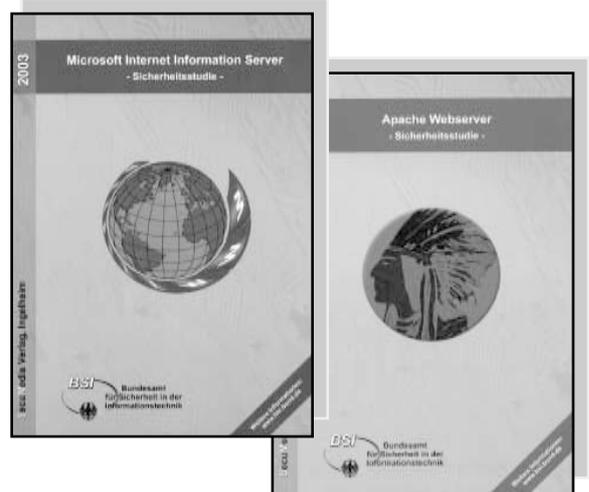
Sicherheitsjahrbuch 2003/2004
Das umfassende Compendium
der Sicherheit



52 völlig neue Wochensprüche – Der Nachfolger des erfolgreichen
„Lieber ein Optimist der sich mal irrt . . .“ von Peter Hohl



BSI-Studie zur Webserver-
Sicherheit: entweder für
IIS oder Apache



Ich bin Teilnehmer der <kes>/Microsoft-Sicherheitsstudie 2004

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

Als Teilnahme Geschenk wünsche ich mir
(bitte nur einen Gegenstand ankreuzen)

- Sicherheits-Jahrbuch 2003/2004
- BSI-Studie IIS-Sicherheit
- BSI-Studie Apache-Sicherheit
- Buch Direkt nach vorn ...
- V9 Micro-Lenser

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