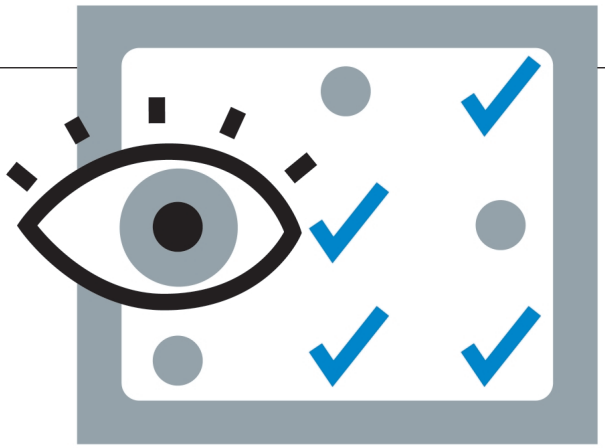


<kes> Microsoft®
Sicherheitsstudie 2006

# Checkliste zur Informations-Sicherheit

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

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 zwei fachlichen Publikationen (RFID-Sicherheitsstudie des BSI und Sicherheits-Kompendium), einer „LED-Mikro-Taschenlampe" oder – zum Regenerieren der kleinen grauen Zellen – einem Sammelband mit Aphorismen von Peter Hohl (vgl. www.wochensprueche.de). Näheres hierzu finden Sie auf Seite 114.

## 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/studie2006/ liegt eine PDF-Version des Fragebogens zum Download bereit.

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

_____ Einsendeschluss: 1. Mai 2006

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

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

Peter Hohl, <kes>-Herausgeber

**Vielen Dank für freundliche Unterstützung unserer Studie**

Microsoft

ASTRUM IT

itWatch GmbH

ROG

BorderWare™

Jürgen Jakob Software-Entwicklung

AVG Anti-Virus

SAP

TRUST

PGP

»|secaron e.security solutions

entrada IT-Security

phion

SONICWALL

ibas Datenrettung Datenlöschung Computer Forensics

proRZ professioneller Rechenzentrumsbau

TESIS SYSware

it.sec security for your information

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

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 2.03 b: eine oder mehrere „eingesetzte Methodiken" schließen „keine Methodik" aus).

Für weitere Fragen zu den Fragen oder Antwortmöglichkeiten haben wir die spezielle Mail-Adresse checkliste2006@kes.info eingerichtet. Auf www.kes.info/studie2006/ werden wir zudem eine FAQ-Sammlung pflegen.

# Fragebogen für die <kes>/Microsoft-Sicherheitsstudie 2006

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

## 1 Aktuelle Risikosituation

1.01 Gefahrenbereiche

| | a Nennen Sie bitte die Gefahrenbereiche, die aus Ihrer Sicht für Ihr Haus die höchste Bedeutung haben. (Vergeben Sie dazu bitte insgesamt sechs Prioritätspunkte, maximal drei pro Eintrag) | insges. 6 Kreuze | b Wie schätzen Sie die zukünftige Entwicklung der Risiken in diesen Gefahrenbereichen für Ihr Haus ein? (Bitte ankreuzen) | | | | | c Haben diese Gefahrenbereiche in Ihrem Haus in den vergangenen beiden Jahren tatsächlich zu mittleren bis größeren Beeinträchtigungen geführt? (Bitte ankreuzen) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | nehmen zu stark | nehmen zu etwas | bleiben gleich | nehmen ab etwas | nehmen ab stark | ja | nein |
| • | von Menschen direkt verursachte Gefahren | | | | | | | | |
| – | Irrtum und Nachlässigkeit eigener Mitarbeiter | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| – | unbeabsichtigte Fehler von Externen (z. B. Wartungstechniker) | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| – | Manipulation zum Zweck der Bereicherung | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| – | unbefugte Kenntnisnahme Informationsdiebstahl, Wirtschaftsspionage | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| – | Sabotage (inkl. DoS) | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| – | Hacking (Vandalismus, Probing, Missbrauch, ...) | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| • | Malware (Viren, Würmer, Trojanische Pferde usw.) | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| • | technische Defekte/ Qualitätsmängel | | | | | | | | |
| – | hardwarebedingt | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| – | softwarebedingt | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| – | Mängel der Dokumentation | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| • | höhere Gewalt (Feuer, Wasser usw.) | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| • | Sonstiges | ◇ ◇ ◇ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

(bitte nennen):

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

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

| 1.03 Welche Internetnutzung gestattet Ihr Haus den Mitarbeitern? | a geschäftliche Nutzung von: Multimedia-Diensten | WWW | E-Mail | b private Nutzung gestattet |
|---|---|---|---|---|
| • für alle Mitarbeiter | ○ | ○ | ○ | ○ |
| • für spezielle Mitarbeiter/Abteilungen/Bereiche | ○ | ○ | ○ | ○ |
| • nur an ausgewählten Arbeitsplätzen | ○ | ○ | ○ | ○ |
| • generell nicht gestattet | ○ | ○ | ○ | ○ |
| • n. b. | ○ | ○ | ○ | ○ |

1.04 Private Systeme

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

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

1.05 Vertraulichkeitsbrüche

a **Haben Unbefugte 2004/2005 über die folgenden Wege Zugriff auf schutzwürdige Daten erlangt?**

| | ja (gesicherte Erkenntnis) | vermutlich ja | vermutlich nicht | nein (gesicherte Erkenntnis) | n. b. |
|---|---|---|---|---|---|
| • Online-Angriff (Hacking, Systemeinbruch, ...) | ○ | ○ | ○ | ○ | ○ |
| • Abhören von Kommunikation (E-Mail, FTP, VoIP, ...) | ○ | ○ | ○ | ○ | ○ |
| • Verlust oder Diebstahl mobiler Systeme (Notebook, PDAs, ...) | ○ | ○ | ○ | ○ | ○ |
| • Verlust oder Diebstahl von Speichermedien (Backup-Tapes, USB-Speicher, ...) | ○ | ○ | ○ | ○ | ○ |
| • Einbruch in Gebäude | ○ | ○ | ○ | ○ | ○ |
| • Missbrauch/Weitergabe durch Berechtigte | ○ | ○ | ○ | ○ | ○ |
| • sonstiger Weg: _____ | ○ | ○ | ○ | ○ | ○ |

b **Welche Konsequenzen hatten diese Vorfälle?**

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

| 1.06 Hatte Ihr Haus 2005 Vorfälle mit Malware? | | File-Viren | Boot-Viren | Makro-Viren | Würmer | Troj. Pferde/Backdoors | Spyware |
|---|---|---|---|---|---|---|---|
| a | • ja, und zwar durch ... | ○ | ○ | ○ | ○ | ○ | ○ |
| | • nein | ○ | ○ | ○ | ○ | ○ | ○ |
| | • n. b. oder nicht registriert | ○ | ○ | ○ | ○ | ○ | ○ |
| b | • weniger Fälle als 2004 | ○ | ○ | ○ | ○ | ○ | ○ |
| | • mehr Vorfälle als 2004 | ○ | ○ | ○ | ○ | ○ | ○ |

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

| | häufig | selten | nie | n. b. |
|---|---|---|---|---|
| • Datenträger (CD-ROM, Diskette, ...) | ○ | ○ | ○ | ○ |
| • internes Netz | ○ | ○ | ○ | ○ |
| • E-Mail | ○ | ○ | ○ | ○ |
| • Internet-Download | ○ | ○ | ○ | ○ |
| • Internet (autom. Verbreitung) | ○ | ○ | ○ | ○ |
| • WWW-Seite (aktive Inhalte) | ○ | ○ | ○ | ○ |
| • unbekannte Herkunft | ○ | ○ | ○ | ○ |

1.07 Häufigkeit und Aufwand von Sicherheitsvorfällen/Fehlalarm

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

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

1.08 Gab es 2004 oder 2005 durch die folgende Malware nennenswerte Beeinträchtigungen in Ihrem Hause?

| | ja | nein | n. b. oder keine Daten verfügbar |
|---|---|---|---|
| • Bagle/Beagle | ○ | ○ | ○ |
| • Mytob | ○ | ○ | ○ |
| • Netsky | ○ | ○ | ○ |
| • Sasser | ○ | ○ | ○ |
| • Sober | ○ | ○ | ○ |

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 ISi-Strategie und -Management

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

2.02 Krisenplanung

| a Besteht ein EDV-Notfall/-Wiederanlaufkonzept? | ja | nein |
|---|---|---|
| • ja, schriftlich fixiert, verifiziert, validiert und freigegeben | ○ | |
| ja, schriftlich fixiert | ○ | |
| ja, aber nicht schriftlich | ○ | |
| • nein | | ○ |

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

## 2.03 Risikobewertung

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

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

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

- eigene Methodik/Software ☐
- standardisiertes Verfahren (GSHB, BS 7799, ...) ☐
- Verfahren eines Herstellers oder Beraters ☐
- Risikomanagement-Software ☐
- sonstige Methodik: _____ ☐
- kein strikt methodisches Vorgehen ○

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

- ja ○
- nein ○
- n. b. ○

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

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

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

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

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

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

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

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

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

2.07 Stellenwert der ISi

a 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. ○

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

ein Hauptkriterium ○ eher zweitrangig ○ eher unbedeutend ○

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

d Planen Sie künftig bevorzugt Systeme mit Trusted-Computing-Komponenten einzusetzen?

ja ○ nein ○ noch unentschieden ○

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

a ja ○ / nein ○

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

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

c Wie lange liegt die letzte Prüfung zurück? _____ Monate

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

e Führte die letzte Überprüfung zur Aufdeckung von Schwachstellen? ○ ja ○ nein

2.09 Wird die *Einhaltung* vorgesehener Maßnahmen geprüft?

a ja ○ / nein ○

b falls ja: Durch wen erfolgt diese Prüfung?

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

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

- Aufbauorganisation ☐
- Ablauforganisation (z. B. für einzelne Vorgänge, Verfahren) ☐
- Software-Entwicklung (inkl. Test- und Freigabeverfahren) ☐
- Software-Einsatz (angemessen, korrekt usw.) ☐
- Übereinstimmung der System-Konfiguration mit Vorgaben ☐
- Datenklassifizierung und Zugriffsrechte ☐
- Änderungshistorie (Change Management) ☐
- Virenschutz ☐
- Berechtigungskonzept ☐
- Notfallkonzept ☐
- physische Sicherheit ☐
- Netzwerkstrategie/Firewalls ☐
- Sonstiges (bitte nennen): _____ ☐
- nichts Derartiges ○

## 2.11 Welche Probleme behindern Sie am meisten bei der Verbesserung der ISi?

(Bitte alle zutreffenden Aussagen ankreuzen)

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

## 2.12 Aufgabenverteilung/Verantwortlichkeit

| a Gibt es in Ihrem Hause ...? / b Wer ist verantwortlich für ...? | ☐ ISi-Beauftragter | ☐ Datenschutzbeauftragter | ☐ ISi-Ausschuss (o. Ä.) | ☐ Leiter IT / DV / RZ | ☐ IT / DV-Revision | ☐ Leiter Organisation | ☐ Leiter Sicherheit/Werkschutz | ☐ Administratoren | ☐ Benutzerservice | ☐ DV-orientierter Jurist | ☐ Top-Management | ☐ Einkauf/Beschaffung | ☐ jeweilige Fachabteilung | ☐ andere |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| • Formulierung der ISi-Strategie (Ziele, Rahmenbed., Ressourcen) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| • Sensibilisierung und Schulung der Nutzer | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| • Durchführung von Risikoanalysen/Sicherheitsanalysen | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| • Erstellung von Konzepten und Richtlinien | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| • Beschaffung und Betrieb von | | | | | | | | | | | | | | |
| – Servern | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| – Clients/PCs | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| – mobilen Endgeräten | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| – technischer Infrastruktur (z. B. Klimaanlage, Gefahrenmeldeanl.) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| – Software (inkl. Lizenzverwaltung) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| • Wirtschaftlichkeit der IT-Sicherheit | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| • Notfall- und Eskalationsmaßnahmen/Business Continuity | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| • Prüfung/Einhaltung gesetzlicher Vorgaben | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

## 2.13 CERT/CSIRT

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

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

c falls ja: Von welchem CERT/CSIRT? _____

## 2.14 ISi-Beratung

a Nutzt Ihr Haus externe ISi-Beratung?

- ja, regelmäßig ○
- ja, gelegentlich ○
- nein ○

c falls ja: waren Sie mit der Beratung zufrieden?

- ja, uneingeschränkt ○
- ja, mit Einschränkungen ○
- nein ○
- n. b. ○

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 ☐
- Produktberatung und Kaufunterstützung ☐
- Prozess-Entwicklung und -Optimierung ☐
- Sonstiges (bitte nennen): _____

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

- ja, auf
  - – die Internet-Infrastruktur ☐
  - – kritische Systeme von innen ☐
  - – Sonstiges _____ ☐
- nein ○

2.15 Outsourcing?

a Betreibt Ihr Haus Outsourcing? ja ○ nein ○

b falls ja: Welche Funktionen haben Sie ausgelagert?

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

| c falls ja: Haben Sie Service-Level-Agreements/ vertragliche Vereinbarungen | ja, mit regelmäßiger Kontrolle | ja, mit anlassbezogener Kontrolle | ja, aber keine Kontrolle | nein |
|---|---|---|---|---|
| mit dem Outsourcer? | ○ | ○ | ○ | ○ |
| • mit expliziten Anforderungen an die ISi? | ○ | ○ | ○ | ○ |
| • mit expliziten Anforderungen an den Datenschutz? | ○ | ○ | ○ | ○ |

d Sind Sie mit dem Outsourcing zufrieden?

○ ja, uneingeschränkt ○ ja, mit Einschränkungen ○ nein ○ n. b.

2.16 Versicherungen

a Welche Versicherungen aus dem Bereich ISi hat Ihr Haus abgeschlossen / bereits in Anspruch genommen?

| | abgeschlossen ja | abgeschlossen nein | falls ja: bereits in Anspruch genommen | | abgeschlossen ja | abgeschlossen nein | falls ja: bereits in Anspruch genommen |
|---|---|---|---|---|---|---|---|
| • Elektronik-/IT-Sachversicherung | ○ | ○ | ○ | • Feuerversicherung | ○ | ○ | ○ |
| • Datenversicherung/Softwareversicherung | ○ | ○ | ○ | • Datenhaftpflicht-Versicherung | ○ | ○ | ○ |
| • Elektronik-/IT-Betriebsunterbrechungsversicherung | ○ | ○ | ○ | • Datenrechtsschutz-Versicherung | ○ | ○ | ○ |
| Sonstige _____ | ○ | ○ | ○ | • keine mit ISi-Bezug | ○ | | |

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 Informationsquellen und Schulung

| 3.01 Wen informieren/schult Ihr Haus über Fragen der ISi? | häufig/regelmäßig (min. 1xjährl.) | gelegentlich / zu speziellen Anlässen | nie | n. b. |
|---|---|---|---|---|
| • Benutzer | ○ | ○ | ○ | ○ |
| • freie/externe Mitarbeiter | ○ | ○ | ○ | ○ |
| • IV-/DV-Mitarbeiter | ○ | ○ | ○ | ○ |
| • Datenschutzbeauftragte | ○ | ○ | ○ | ○ |
| • ISi-Beauftragte | ○ | ○ | ○ | ○ |
| • Revisoren, Prüfer | ○ | ○ | ○ | ○ |
| • Management | ○ | ○ | ○ | ○ |
| • andere | ○ | ○ | ○ | ○ |

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

| | häufig | gelegentlich | nie | n. b. |
|---|---|---|---|---|
| • interne Schulungen durch Frontalunterricht, möglichst flächendeckend | ○ | ○ | ○ | ○ |
| • interne Schulungen durch Frontalunterricht für Spezialgruppen | ○ | ○ | ○ | ○ |
| • externe Schulungen | ○ | ○ | ○ | ○ |
| • Materialien (Schulungsunterlagen) zum Selbstlernen | ○ | ○ | ○ | ○ |
| • (Multimediale) Lern-CDs zum Selbstlernen | ○ | ○ | ○ | ○ |
| • Online-Trainings-Anwendungen/-Tools | ○ | ○ | ○ | ○ |

3.03 Berufszertifikate

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

b Welche herstellerunabhängigen ISi-Zertifikate kennen Sie?

| | | | | |
|---|---|---|---|---|
| • CISA | ❑ | • CISSP | ❑ | • sonstige (bitte ausschreiben): |
| • CISM | ❑ | • SSCP | ❑ | _____ |
| • CISO | ❑ | • TISP | ❑ | _____ |

3.04 Wo informieren Sie sich über ISi?

• CeBIT ❑ IT-SecurityArea (SYSTEMS) ❑ infosecurity ❑ BSI-Kongress ❑ ISSE ❑ Security Essen ❑

• Konferenzen / Kongresse / Seminare (welche?) _____

• Zeitschriften / Magazine (welche?) _____

• Hersteller-/Anbieter-Dokus (White Paper, Guidelines, ...) (welche?) _____

• Mailinglisten (welche?) _____

• Internet / WWW
(bitte nennen Sie die URLs _____
Ihrer wichtigsten Informationsquellen) _____

3.05 Wo erhalten Sie Informationen über aktuelle Sicherheits-Updates?

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

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

c • Welche ISi-Bulletins haben Sie abonniert? ❑ Microsoft ❑ Symantec ❑ CERT-Bund ❑ US-CERT.gov ❑ SANS.org ❑ heisec.de
Sonstige: _____

3.06 Qualität von Herstellerinformationen

| Wie beurteilen Sie die Informationsdienste der Anbieter von ... | **a Umfang/Vollständigkeit** gut befriedigend schlecht | **b Verständlichkeit** gut befriedigend schlecht | **c Geschwindigkeit** gut befriedigend schlecht |
|---|---|---|---|
| • Betriebssystemen | ○ ○ ○ | ○ ○ ○ | ○ ○ ○ |
| • Anwendungen | ○ ○ ○ | ○ ○ ○ | ○ ○ ○ |
| • Netzwerksystemen | ○ ○ ○ | ○ ○ ○ | ○ ○ ○ |
| • Sicherheitssystemen | ○ ○ ○ | ○ ○ ○ | ○ ○ ○ |

## 4 Methoden und Maßnahmen

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

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

4.02 Wie wichtig bewerten Sie folgende Komponenten eines unternehmensweiten Security-Managements?

| | sehr wichtig | wichtig | unwichtig | n. b. |
|---|---|---|---|---|
| • plattformübergreifende Benutzerverwaltung | ○ | ○ | ○ | ○ |
| • Single-Sign-on (SSO) | ○ | ○ | ○ | ○ |
| • zentrale Überwachung der eingesetzten Security-Systeme (z. B. Firewall, Applikations-Security-Systeme) | ○ | ○ | ○ | ○ |
| • Alarm- und Eskalationssystem | ○ | ○ | ○ | ○ |
| • Intrusion Detection/Prevention Systems (IDS/IPS) | ○ | ○ | ○ | ○ |
| • Kontrolle und Überwachung von Internet-Missbrauch | ○ | ○ | ○ | ○ |
| • Virtual Private Networks (VPN) | ○ | ○ | ○ | ○ |
| • Public Key Infrastructure (PKI) / Identity-Management-System | ○ | ○ | ○ | ○ |
| • andere _____ | ○ | ○ | ○ | ○ |

4.03 Multi-Vendor-Strategie

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

4.04 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, aus Kostengründen ☐ • nein ○
ja, aus Sicherheitsgründen ☐
ja, wegen: _____

4.05 Content Security (Malware, Spam, Filter)

a Welche Vorsorge gegen Malware hat Ihr Haus getroffen?

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

c Welche Funktionen erwarten Sie von einer Content-Security-Lösung?
Virenschutz ☐ Spyware-Schutz ☐ Spam-Abwehr ☐ Phishing-Abwehr ☐
Inhaltsfilter ☐ Reporting-Tools ☐ Monitoring/Alerting ☐

d Wie hoch ist in Ihrem Unternehmen der Spam-Anteil bei E-Mails?
geschätzt ○ ermittelt ○ _____% Spam

4.06 E-Mail-Verschlüsselung

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

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

b Welchen Standard verwenden Sie dabei?

| | |
|---|---|
| • S/MIME | ☐ |
| • (Open)PGP/GPG | ☐ |
| • sonstigen (bitte nennen) | |

c Der Einsatz einer „virtuellen Poststelle“ (Ver-/Entschlüsselung am Gateway/Server)
**ist ...** realisiert ○ geplant ○ nicht vorgesehen ○

## 4.07 Welche Infrastruktur nutzt Ihr Haus für digitale/elektronische Signaturen?

| | realisiert | geplant | nicht vorgesehen |
|---|---|---|---|
| • nur Software | ○ | ○ | ○ |
| • Hardwaremodule (HSM) | ○ | ○ | ○ |
| • Hardware-Token | ○ | ○ | ○ |
| • Chipkarten | ○ | ○ | ○ |
| • „Klasse-2"-Chipkartenterminal (sichere PIN-Eingabe) | ○ | ○ | ○ |
| • „Klasse-3"-Chipkartenterminal (mit eigenem Display) | ○ | ○ | ○ |

| | realisiert | geplant | nicht vorgesehen |
|---|---|---|---|
| • laut Signaturgesetz | | | |
| – fortgeschrittene Signatur | ○ | ○ | ○ |
| – qualifizierte Signatur | ○ | ○ | ○ |
| – qualifizierte Signatur mit Anbieterakkreditierung | ○ | ○ | ○ |
| • Sonstiges: _____ | ○ | ○ | |
| • nichts von alledem | ○ | ○ | |

## 4.08 Virtual Private Networks (VPNs)

a Welche VPN-Verfahren nutzt Ihr Haus?

| | realisiert | geplant | nicht vorgesehen | n. b. |
|---|---|---|---|---|
| • IPsec | ○ | ○ | ○ | ○ |
| • SSL | ○ | ○ | ○ | ○ |
| • MLPS | ○ | ○ | ○ | ○ |
| • sonstige _____ | ○ | ○ | ○ | ○ |

b Was spricht Ihrer Meinung nach *gegen* den Einsatz von SSL-VPNs?

- ☐ Kosten
- ☐ passende Lösung nicht verfügbar
- ☐ deckt sich nicht mit unseren Anforderungen
- ○ nichts
- • Sonstiges: _____

## 4.09 Public Key Infrastructure (PKI)

| | realisiert | geplant | nicht vorgesehen | n. b. |
|---|---|---|---|---|
| a Die Implementierung einer PKI ist ... | ○ | ○ | ○ | |
| b Für welche Zwecke nutzen/planen Sie in Ihrem Haus eine PKI? | | | | |
| • E-Mail-Verschlüsselung | ○ | ○ | ○ | ○ |
| • Dateiverschlüsselung | ○ | ○ | ○ | ○ |
| • Zugriffsrechte | ○ | ○ | ○ | ○ |
| • Single-Sign-On (SSO) | ○ | ○ | ○ | ○ |
| • Virtual Private Networks (VPN) | ○ | ○ | ○ | ○ |
| • Telearbeitsplätze / Remote Access | ○ | ○ | ○ | ○ |
| • Web-Zugriff (Portale, Intranet, ...) | ○ | ○ | ○ | ○ |
| • Sonstiges: _____ | ○ | ○ | | |

## 4.10 Identity Management (IdM)

| | realisiert | geplant | nicht vorgesehen | |
|---|---|---|---|---|
| a Die Implementierung einer IdM-Lösung ist ... | ○ | ○ | ○ | |
| b Welchen Nutzen versprechen Sie sich vom Einsatz einer IdM-Lösung? | sehr wichtig | wichtig | unwichtig | n. b. |
| • Kostenersparnis (ROI) | ○ | ○ | ○ | ○ |
| • Steigerung der Unternehmenssicherheit (Policy Enforcement) | ○ | ○ | ○ | ○ |
| • Realisierung einer konsistenten Rechtevergabe | ○ | ○ | ○ | ○ |
| • delegierte Administration | ○ | ○ | ○ | ○ |
| • hoher Automatisierungsgrad | ○ | ○ | ○ | ○ |
| • Compliance | ○ | ○ | ○ | ○ |
| • Nachvollziehbarkeit (Revisionierbarkeit) | ○ | ○ | ○ | ○ |
| • Sonstiges: _____ | ○ | ○ | | |

| c Welche Hemmnisse sehen Sie für den Einsatz einer IdM-Lösung? | sehr problematisch | problematisch | unproblematisch | n. b. |
|---|---|---|---|---|
| • technische Komplexität/aufwändige Einführung | ○ | ○ | ○ | ○ |
| • organisatorische Komplexität/aufwändige Einführung | ○ | ○ | ○ | ○ |
| • hohe Produktkosten | ○ | ○ | ○ | ○ |
| • hohe Betriebskosten | ○ | ○ | ○ | ○ |
| • Herstellerabhängigkeit | ○ | ○ | ○ | ○ |
| • ROI schwer berechenbar/nachvollziehbar | ○ | ○ | ○ | ○ |
| • Sonstiges: _____ | ○ | ○ | ○ | |

4.11 Welche Log-Daten wertet Ihr Haus aus?

| | Auswertung min. 2 x pro Woche | Auswertung seltener, aber regelmäßig | Auswertung erfolgt anlassbezogen | keine Auswertung oder Protokollierung |
|---|---|---|---|---|
| • Anti-Virus-Lösungen | ○ | ○ | ○ | ○ |
| • Firewall(s) | ○ | ○ | ○ | ○ |
| • Intrusion Detection/Prevention Systems | ○ | ○ | ○ | ○ |
| • Netzkomponenten (Router, Switches etc.) | ○ | ○ | ○ | ○ |
| • Betriebssysteme | ○ | ○ | ○ | ○ |
| • Web-/E-Commerce-Applikationen | ○ | ○ | ○ | ○ |
| • sonstige Applikationen: _____ | ○ | ○ | ○ | |

4.12 Device Management

a Welche Bedeutung hat die Nutzung von Plug&Play-Peripherie (z. B. USB-Speicher, Digitalkameras, Bluetooth, ...) für die Wertschöpfungskette bzw. Arbeitsabläufe Ihres Hauses?

groß ○ gering ○ vernachlässigbar ○ keine Nutzung ○ untersagt ○ n. b. ○

b Ist für 2006 eine intensivere Nutzung als bislang geplant?

ja ○ nein ○

c Wie sichert Ihr Haus Schnittstellen gegen unerwünschte Nutzung?

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

4.13 Wie verwaltet Ihr Haus (in nennenswertem Umfang) seine Systeme?

| | **a Netzwerk-Systeme** ja | nein | **b Host/PC-Systeme** ja | nein |
|---|---|---|---|---|
| • manuell | ○ | ○ | ○ | ○ |
| • mit Managementlösungen der jeweiligen Hersteller | ○ | ○ | ○ | ○ |
| • mit zentralen Managementlösungen | ○ | ○ | ○ | ○ |

4.14 Notfallvorsorge

a Hält Ihr Haus wesentliche Komponenten seiner Informationsverarbeitung an verschiedenen Orten vor?

| | Auslagerungsarchiv | Roboter-Systeme | gespiegelte Daten | zus. Rechner/ Cluster |
|---|---|---|---|---|
| • ja, in einem getrennten Brandabschnitt | ○ | ○ | ○ | ○ |
| – in einem anderen Gebäude | ○ | ○ | ○ | ○ |
| – bei einem Kooperationspartner | ○ | ○ | ○ | ○ |
| – bei einem externen Anbieter | ○ | ○ | ○ | ○ |
| • nein | ○ | ○ | ○ | ○ |

b Was hat Ihr Haus für längere Ausfälle bereitgestellt?

| | Unternehmensserver/Mainframe realisiert | geplant | nicht vorgesehen | Abt.-Rechner PC, LAN realisiert | geplant | nicht vorgesehen |
|---|---|---|---|---|---|---|
| • Räume („kalte Lösung“ bzw. „empty shell“) | ○ | ○ | ○ | ○ | ○ | ○ |
| • Räume mit (wichtiger) Hardware („warme Lösung“) | ○ | ○ | ○ | ○ | ○ | ○ |
| • Cluster/Load Balancing (mit Überkapazität) | ○ | ○ | ○ | ○ | ○ | ○ |
| • laufende Systeme („heiße Lösung“) | ○ | ○ | ○ | ○ | ○ | ○ |
| • konfigurationsidentische Netze | ○ | ○ | ○ | ○ | ○ | ○ |
| • Ersatzräume für Personal (mit installierter Infrastruktur) | ○ | ○ | ○ | ○ | ○ | ○ |
| • Ersatzräume für Personal (ohne installierte Infrastruktur) | ○ | ○ | ○ | ○ | ○ | ○ |
| • Verträge mit externen Dienstleistern/Partnern | | | | | | |
| – über die Nutzung von deren Ressourcen (stationäres Ausweich-RZ) | ○ | ○ | ○ | ○ | ○ | ○ |
| – über die Nutzung von kurzfristig verfügbaren Containern | ○ | ○ | ○ | ○ | ○ | ○ |
| • Verträge über die schnelle Lieferung von Hardware | ○ | ○ | ○ | ○ | ○ | ○ |
| • Versicherung abgeschlossen | ○ | ○ | ○ | ○ | ○ | ○ |
| • nichts | ○ | ○ | | ○ | ○ | |

c falls Sie einen Recovery-Vertrag haben:

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

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

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

f Welches Produkt setzen Sie dafür ein? _____

g Wie oft wird die Dokumentation aktualisiert? ○ alle____ Tage ○ anlassbezogen ○ nie

| h Deckt das eingesetzte Produkt die Anforderungen nach ITIL/BSI-Grundschutzhandbuch ab? | ITIL | BSI | nein | n. b. |
|---|---|---|---|---|
| | ☐ | ☐ | ○ | ○ |

| i Werden „abgearbeitete“ Pläne zu Revisonszwecken archiviert und können jederzeit wieder eingesehen werden? | ja | nein |
|---|---|---|
| | ○ | ○ |

## 4.15 System-Recovery

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

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

## 4.16 Computer-Forensik

a Wurde in Ihrem Haus 2005 ein Sicherheitsvorfall rechtlich verfolgt?

- ja ○
- nein, weil kein Vorfall ○
- nein, mangels Verfolgungsinteresse ○
- nein, mangels Wissen um Ermittlungsmöglichkeiten ○

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

4.17 Anbieter

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

IBM ❑ Microsoft ❑ SAP ❑ Sun Microsystems ❑ bel. Linux-System ❑

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

| | | |
|---|---|---|
| • Aladdin ❑ | • I.T.E.N.O.S. ❑ | • Safeboot ❑ |
| • Allasso ❑ | • Ibas ❑ | • SAP ❑ |
| • Astrum IT ❑ | • Infinigate ❑ | • Secaron ❑ |
| • AVG Anti-Virus (Jakob Software) ❑ | • it.sec ❑ | • Secunet ❑ |
| • BalaBit ❑ | • itWatch ❑ | • Siemens ❑ |
| • Borderware ❑ | • Juniper ❑ | • SonicWALL ❑ |
| • Defense ❑ | • Microsoft ❑ | • Sophos ❑ |
| • Design Institut München (DIM) ❑ | • Lampertz ❑ | • SurfControl ❑ |
| • Deutscher Sparkassen-Verlag ❑ | • PGP ❑ | • Symantec ❑ |
| • Entrada ❑ | • phion ❑ | • TESIS SYSware ❑ |
| • eSeSiX ❑ | • proRZ ❑ | • Trendmicro ❑ |
| • ESET/DATSEC ❑ | • retarus ❑ | • T-Systems ❑ |
| • F-Secure ❑ | • Rittal ❑ | • Websense ❑ |
| • GeNUA ❑ | • ROG ❑ | • es fehlen: |
| • Gerling Versicherungsgruppe ❑ | • Rohde & Schwarz SIT ❑ | _____ |
| • HiSolutions ❑ | • RSA ❑ | _____ |

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

## 5 Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

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

5.02 Kennen Sie die folgenden ISi-Kriterien?

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

| | a ja | nein | hoch | gering | keine | n. b. |
|---|---|---|---|---|---|---|
| • ITSEC | ○ | ○ | ○ | ○ | ○ | ○ |
| • Common Criteria | ○ | ○ | ○ | ○ | ○ | ○ |
| • FIPS 140 | ○ | ○ | ○ | ○ | ○ | ○ |
| • ITIL | ○ | ○ | ○ | ○ | ○ | ○ |
| • COBIT | ○ | ○ | ○ | ○ | ○ | ○ |
| • ISO 27001 | ○ | ○ | ○ | ○ | ○ | ○ |
| • BS 7799 / ISO IEC 17799 | ○ | ○ | ○ | ○ | ○ | ○ |
| • ISO 13335 | ○ | ○ | ○ | ○ | ○ | ○ |
| • IT-Grundschutz | ○ | ○ | ○ | ○ | ○ | ○ |

5.03 Zertifizierte Sicherheitsprodukte

| | ja | nein | |
|---|---|---|---|
| a Setzt Ihr Haus zurzeit zertifizierte Produkte ein? | ○ | ○ | |
| b falls ja: Haben sich Ihre Erwartungen an Nutzen und Zuverlässigkeit erfüllt? | ○ | ○ | |
| c Rechtfertigt ein zertifiziertes Produkt nach Ihrer Meinung einen höheren Preis? | ○ | ○ | |
| d Werden Sie in Zukunft zertifizierte (Sicherheits-)Produkte bevorzugt einsetzen? | ○ | ○ | ○ noch unentschieden |

## 6 Statistische Angaben

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

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

6.02 Zu welcher Branche gehört Ihr Haus?

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

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

• Deutschland ❍ • Schweiz ❍ • Österreich ❍ • Sonstiges (bitte nennen): _____ ❍

6.04 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 |

6.05 Welche Funktionsbezeichnung trifft auf Sie am ehesten zu?

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

6.06 Der Umsatz bzw. die Bilanzsumme Ihres Hauses betrug im Jahr 2005 ...

(falls nicht bekannt, bitte Angabe für 2004 bzw. das letzte Wirtschaftsjahr)

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

• nicht relevant, da Behörde oder ähnliches *(Bitte ankreuzen)* ❑

6.07 Budget

| | | geschätzt | ermittelt |
|---|---|---|---|
| a Das Budget für Informationsverarbeitung (inkl. Personalkosten) umfasst im Jahr 2005 | _____ € | ❍ | ❍ |
| b Der Anteil für ISi-Maßnahmen (inkl. Personalkosten) an diesem Budget beträgt | _____ % | ❍ | ❍ |

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

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

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

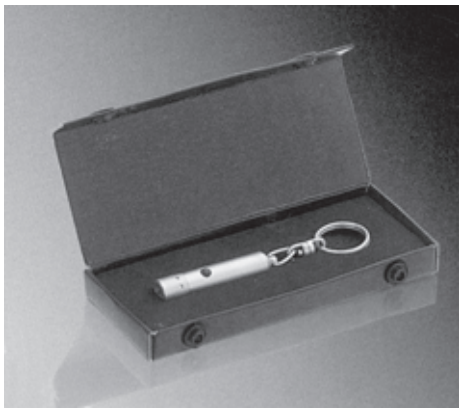
# So garantieren wir Vertraulichkeit:

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

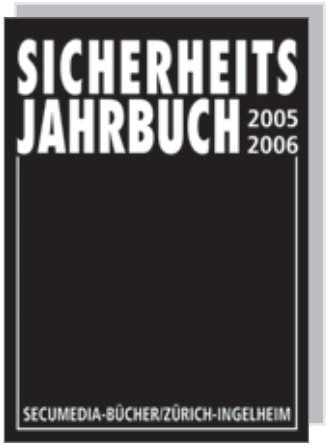
Herrn Peter Hohl
– persönlich –
Redaktion <kes>
Postfach 1234
55205 Ingelheim

(Anschriftsfeld für Versand im C4-Fensterumschlag)

# Ihre „Dankeschön-Prämien"

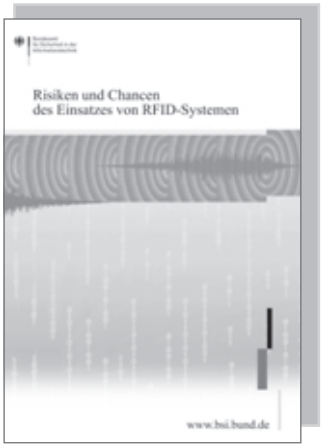


*V9 Micro-Lenser, die „Taschenlampe am Schlüsselbund" von Zweibrüder Optoelectronics*




*Sicherheitsjahrbuch 2005/2006 – das umfassende Kompendium der Sicherheit*


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




*BSI-Studie „Risiken und Chancen des Einsatzes von RFID-Systemen"*

## Ich bin Teilnehmer der <kes>/Microsoft-Sicherheitsstudie 2006

Bitte schicken Sie die Auswertungen und mein Teilnahmegeschenk an folgende Anschrift:

Als Teilnahmegeschenk wünsche ich mir
(bitte nur einen Gegenstand ankreuzen)

- ○ Sicherheits-Jahrbuch 2005/2006
- ○ BSI-Studie RFID-Systeme
- ○ Buch „Ein Mittel ..."
- ○ 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