Lagebericht zur Informations-Sicherheit (2)

Verlässliche Zahlen zur Informations-Sicherheit (ISi) findet man nur selten. Noch seltener sind konkrete Angaben zu Schäden und Budgets sowie selbstkritische Bestandsaufnahmen zur Sicherheitslage. In diesem Jahr haben erneut über 160 Teilnehmer den <kes>-Fragebogen als Checkliste für ihre eigene Sicherheit genutzt und damit gleichzeitig wertvolle Daten geliefert.

Die vertrauensvollen und umfassenden Antworten der Teilnehmer und die Unterstützung der Sponsoren und Partner machen diese Studie möglich – dafür zunächst vielmals Dankeschön! In diesem Jahr sind 163 ausgefüllte Fragebögen eingegangen. Dabei war auch eine erfreulich hohe Beteiligung durch kleine und mittelständische Unternehmen (KMU) mit bis zu 500 Mitarbeitern zu verzeichnen. Der erste Teil der Ergebnisse ist bereits in <kes> 2006#4 erschienen; wichtige Kernpunkte dieses zweiten Teils der Auswertung lauten:

- Schriftliche Strategien zur Informations-Sicherheit sind weiter auf dem Vormarsch: 64 % der Teilnehmer haben derart fixierte Policies.
- „Verstöße gegen Gesetze, Vorschriften und Verträge“ bleiben wichtigstes Kriterium zur Risikobewertung – „Verzögerungen von Arbeitsabläufen“ erhalten höhere Beachtung.
- Jeder siebte Sicherheitsvorfall wird mangels Wissen um Ermittlungsmöglichkeiten der Computer-Forensik nicht rechtlich verfolgt.
- Regulatorische Compliance verbessert – vor allem deutlich höhere Bekanntheit und Akzeptanz des KonTraG.
- Sicherheitskenntnisse im Management weiterhin schwach – knapp 40 % attestieren Top- und Mittelmanagement unbefriedigendes Wissen.

Gibt es im Unternehmen... ?	ja	eingegrenzt auf Unternehmen mit ISi-Strategie	ohne ISi-Strategie
Strategie für die Informations-Verarbeitung	53%	75%	16%
Strategie für die Informations-Sicherheit	64%	100%	0%
umfassendes, integriertes Sicherheitshandbuch	38%	56%	4%
spezifische ISi-Konzepte/Richtlinien...			
... zum Einsatz von Verschlüsselung	38%	47%	25%
... zur Handhabung sensitiver/kritischer Daten	60%	83%	20%
... zur Nutzung von Internet, E-Mail, ...	79%	99%	41%
... zum Softwareeinsatz auf PCs	75%	94%	43%
... zur Nutzung mobiler Endgeräte	54%	75%	18%
... zur Nutzung mobiler Speicher und Plug&Play-Peripherie	43%	60%	14%
... sonstige	32%	56%	10%
Eignung von Konzepten/Richtlinien wird überprüft	*66%*	*84%*	*34%*
schriftlich formulierte ISi-Maßnahmen	57%	79%	21%
Einhaltung vorgesehener Maßnahmen wird überprüft	*82%*	*95%*	*61%*

Basis: Ø 159 Antworten (exist. Maßnahmen: 126), Ø 159 (Prüfung)

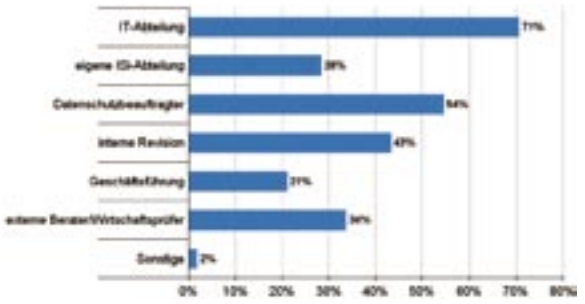
Tabelle 1: Strategien, Richtlinien und Konzepte

Konzepte

Erfreulicherweise gibt es erneut einen Zuwachs an Unternehmen und Behörden mit klaren Policies: Der Anteil der Teilnehmer mit schriftlich fixierter Strategie zur Informations-Sicherheit (ISi) stieg um vier Prozentpunkte auf heuer 64 %. Bei den spezifischen Konzepten und Richtlinien waren ebenfalls wieder Steigerungen zu verzeichnen (s. Tab. 1). Die Bereitschaft, auch Maßnahmen festzuschreiben, ist hingegen weiter gesunken: Gaben 2002 noch 71 % der Befragten an, Sicherheits-Maßnahmen schriftlich zu fixieren, so sank dieser Anteil 2004 bereits auf 65 % und liegt nunmehr bei nur noch 57 %.

Trotz dieser Zurückhaltung haben wieder erheblich mehr Studien-Teilnehmer als vor zwei Jahren eine Überprüfung der Einhaltung vorgesehener Maßnahmen bejaht: Nur 18 % verzichten auf derartige Prüfungen. Betrachtet man nur die befragten Häuser mit schriftlicher

ISi-Policy, so bleiben sogar nur 5 %, die „blind" auf die Einhaltung der Maßnahmen vertrauen (dort liegt auch die generelle Bereitschaft für weitere schriftliche Festlegungen deutlich höher als im Durchschnitt – vgl. Tab. 1). Die Durchführung der Prüfungen obliegt dabei vorrangig den IT-Abteilungen (s. Abb. 1).



Basis: Ø 133 Antworten

Abbildung 1: Wer prüft die Einhaltung vorgesehener ISi-Maßnahmen?

E-Mail und Web gehören am Arbeitsplatz heute selbstverständlich dazu – 88 % beziehungsweise 71 % gestatten eine entsprechende geschäftliche Nutzung allen Mitarbeitern. Beschränkungen der Freigabe für bestimmte Mitarbeiter, Abteilungen oder Arbeitsplätze gibt es bei 27 % fürs Web, bei 11 % bezüglich E-Mails; ein generelles Verbot ist hier praktisch nicht mehr zu beobachten. Deutlichere Restriktionen bestehen allerdings für Multimedia-Dienste: Nur 46 % der Befragten geben diese für alle Mitarbeiter frei, 22 % nur speziellen Bereichen, 15 % an ausgewählten Arbeitsplätzen – immerhin 17 % verbieten generell eine geschäftliche Multimedia-Nutzung.

Der Anteil der Studienteilnehmer, in deren Häuser die private Nutzung des Internets am Arbeitsplatz generell *nicht* gestattet ist, stieg im Vergleich zu 2004 deutlich um zehn Prozentpunkte auf 23 %. Noch knapp zwei Drittel erlauben allen Mitarbeitern jedoch auch private Nutzung, 13 % haben teilweise Beschränkungen vorgesehen. Das Aufschalten privater Systeme ist hingegen überwiegend untersagt (Abb. 2). Die größte Toleranz gibt es hier bezüglich mobiler Speichermedien (32 %) und der Synchronisation privater Smartphones und PDAs mit dem Arbeits-PC (29 %). Eine technische Kontrolle dieser Beschränkungen erfolgt jedoch nur selten in umfassender Manier (s. Abb. 2).

Ein Notfall-/Wiederanlaufkonzept liegt bei 78 % vor, allerdings nur bei knapp drei Viertel dieser Teilnehmer in schriftlicher Form (vgl. Abb. 3). Besondere Berücksichtigung erfahren dabei vor allem die spezifischen Anforderungen von Hardware-Ausfall und -Wiederbeschaffung (bei 79 % gegenüber 95 % in 2004) sowie physischen Einwirkungen (Brand, Naturkatastrophen, Terror – 77 %). Ferner berücksichtigt werden Software-Sicherheitsvorfälle (58 %), Malware-Epidemien (57 % gegenüber 74 % in 2004), das Zusammenbrechen externer Infrastrukturen (44 %), Hochverfügbarkeitsansprüche des E-Business (43 %) sowie Besonderheiten beim gezielten Eindringen von Einzeltätern (37 %) und Denial-of-Service-Angriffen (36 %).

Prüfungen

Eine fortdauernde Prüfung von Konzepten und Richtlinien auf ihre Eignung erfolgt weiterhin nur zögerlich: Wie schon vor zwei Jahren haben nur zwei Drittel aller Teilnehmer ein solches regelmäßiges Audit vorgesehen – von den Häusern mit schriftlicher ISi-Strategie allerdings immerhin 84 % (vgl. Tab. 1). Im Schnitt lag im Teilnehmerfeld die letzte solche Prüfung 8 Monate zurück und führte beim 69 % zur Aufdeckung von Schwachstellen. Zur Reichweite gaben 41 % an, dass alle geschäftskritischen Systeme geprüft wurden – 59 % prüften hingegen nur einzelne Systeme.

Die bevorzugten Methodiken zur Prüfung von Konzepten und Richtlinien sind erneute Schwachstellen- und Risikoanalysen (bei 79 % bzw. 78 % der Befragten). Übungen (Notfall/Wiederanlauf) halfen 62 % beim Audit, 54 % nutzten Penetrationsversuche. Simulationen oder Szenarien kamen hingegen nur bei 34 % zum Einsatz.

Im Rahmen sonstiger Prüfungen (z. B. durch interne Revision, Wirtschaftsprüfer, Berater oder Geschäftsführung) werden unter ISi-Aspekten vor allem Virenschutz (bei 76 %) und Berechtigungskonzept (71 %) geprüft; doch auch weitere Themenfelder werden hierbei verbreitet berücksichtigt (s. Tab. 2).

Inhouse vs. extern

Einen expliziten Beauftragten für die Informations-Sicherheit haben von der gesamten Stichprobe 46 %, wobei größere Organisationen naheliegenderweise eher eine solche Position vorsehen: Von den Unternehmen und Behörden ab 500 Mitarbeitern haben 79 % einen ISi-Beauftragten, von kleinen und mittleren Unternehmen nur 29 %. Weitere vorhandene Positionen zeigt Tabelle 3.

Prüfung unter ISi-Aspekten von...	ja
Virenschutz	76%
Berechtigungskonzept	71%
physische Sicherheit	64%
Netzwerkstrategie/Firewalls	64%
Notfallkonzept	62%
Datenklassifizierung und Zugriffsrechte	55%
Ablauforganisation (z. B. für einzelne Vorgänge, Verfahren)	52%
Software-Einsatz (angemessen, korrekt usw.)	50%
Aufbauorganisation	43%
Änderungshistorie (Change Management)	43%
Übereinstimmung der System-Konfiguration mit Vorgaben	42%
Software-Entwicklung (inkl. Test- und Freigabeverfahren)	41%
Sonstiges	6%
nichts Derartiges	13%

Basis: 154 Antworten

Tabelle 2: Prüfung unter ISi-Aspekten

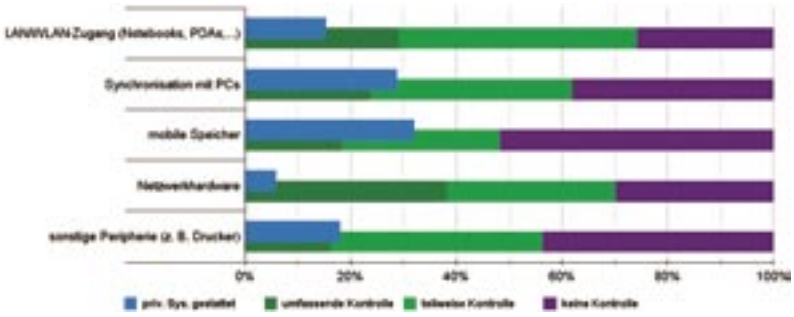


Abbildung 2: Gestattete Aufschaltung und Kontrolle privater Systeme

Basis: Ø 156 Antworten (Aufschaltung), Ø 147 (Kontrolle)

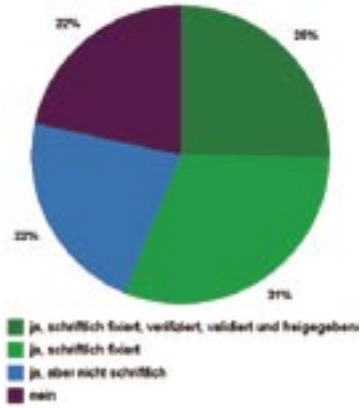


Abbildung 3: Vorhandensein eines IT-Notfall-/ Wiederanlaufkonzepts

Basis: 162 Antworten

Gibt es im Hause... ?	ja, bei
ISi-Beauftragter	46%
Datenschutzbeauftragter	75%
ISi-Ausschuss (o. Ä.)	13%
Leiter IT/DV/RZ	83%
IT/DV-Revision	33%
Leiter Organisation	36%
Leiter Sicherheit/Werkschutz	26%
Administratoren	88%
Benutzerservice	59%
DV-orientierter Jurist	13%

Tabelle 3: Vorhandene Positionen

Basis: 109 Antworten

Genutzte Berater-Funktionen	ja, bei
Risikoanalysen und Konzeptentwicklung	68%
Schwachstellenanalysen	57%
Penetrationstests	46%
Strategie- u. Managementberatung	41%
Produktberatung und Kaufunterstützung	41%
Prozess-Entwicklung und -Optimierung	39%
Umsetzung von Konzepten und Maßnahmen	36%
Kontrolle vorhandener Konzepte	35%
Sonstiges	5%

Tabelle 4: Genutzte Berater-Funktionen

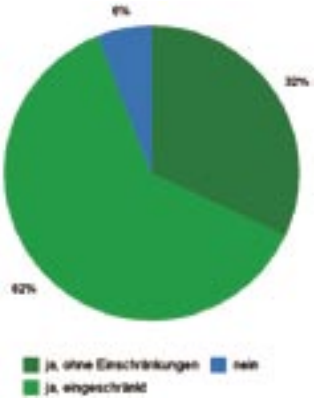
Basis: 87 Antworten

Ein eigenes Computer Emergency (CERT) oder Security Incident Response Team (CSIRT) unterhalten 21 % aller Teilnehmer – 31 % nutzen Dienste eines externen Teams, nur ein knappes Drittel davon allerdings auch kostenpflichtige Leistungen. Auch hier liegen größere Organisationen vorn: 29 % von ihnen haben ein eigenes Team, 42 % nutzen externe CERT/CSIRT-Dienste, wobei immerhin zwei Fünftel hierfür auch Geld ausgeben.

Der Anteil der Studien-Teilnehmer, die regelmäßig (8 %) oder gelegentlich (47 %) externe ISi-Beratung nutzen, ist gegenüber der Erhebung von 2004 um vier Prozentpunkte zurückgegangen. Die gefragtesten Aufgaben waren dabei erneut Risiko- und Schwachstellenanalysen sowie Konzeptentwicklung (s. Tab. 4). Die Zufriedenheit mit den Leistungen der Berater ist indes gesunken: Nur noch 32 % (2004: 51 %) äußerten sich uneingeschränkt, 62 % mit Einschränkungen (2004: 46 %) zufrieden – der Anteil der unzufriedenen Berater-Kunden verdoppelte sich auf 6 % (vgl. Abb. 4).

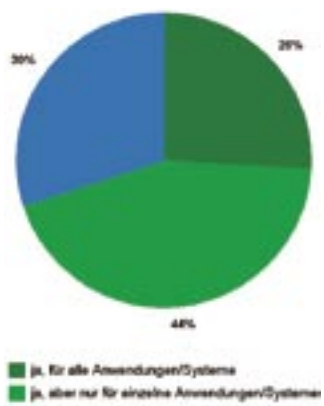
Die Leistungen von Outsourcern wurden sogar noch etwas zurückhaltender beurteilt: 28 % gaben an uneingeschränkt, 67 % mit Einschränkungen zufrieden zu sein. Insgesamt nutzen 56 % der Teilnehmer Outsourcing – die hierfür vorgesehenen Funktionen nennt Tabelle 5. Es zeigt sich ein ähnlich hoher Nutzer-Anteil wie bei Beratungsleistungen, die Schnittmenge liegt jedoch nur bei etwa zwei Dritteln. Auffällig ist, dass nicht etwa die kleineren und mittleren Unternehmen vorrangig Beratung und Outsourcing nutzen, um etwaige Kapazitäts- oder Know-how-Engpässe zu kompensieren: Im Gegenteil ist der Anteil der Nutzer externer Dienste bei den Unternehmen ab 500 Mitarbeitern deutlich größer (80 % Beratung, 73 % Outsourcing) als bei den KMU (43 % bzw. 46 %).

Ansprechpartner für (computer-)forensische Analysen suchen die meisten Teilnehmer naheliegenderweise bevorzugt im eigenen Haus (Tab. 6). Als wichtigster Externer fungieren dann schon die Strafverfolgungsbehörden, die immerhin fast ein Viertel der Befragten auf jeden Fall einbinden würden. Alle anderen externen Institutionen würden zudem jeweils über fünfzig Prozent nur



Basis: 81 Antworten

Abbildung 4: Zufriedenheit mit Beratungsdienstleistungen



Basis: 159 Antworten

Abbildung 5: Reichweite der Risikobewertung

„nachrangig“ oder keinesfalls einbeziehen. Bei immerhin 15 % der Stichprobe wurde übrigens 2005 ein Sicherheitsvorfall tatsächlich rechtlich verfolgt. Dies deckt allerdings nur knapp die Hälfte aller Vorfälle ab: Zwei Fünftel der Organisationen, die einen Vorfall angaben, sahen mangels Verfolgungsinteresse von rechtlichen Schritten ab – ein Siebtel nannte mangelndes Wissen um Ermittlungsmöglichkeiten als Grund für die Nichtverfolgung.

Bei Versicherungen als Form der externen Risikoabwälzung belegte erneut klar die Feuerversicherung den Spitzenplatz: 86 % waren gegen Brände versichert, 7 % der so Versicherten gaben an, diese Policen auch schon einmal in Anspruch genommen zu haben. Auf Rang Zwei bei den Abschlüssen folgen mit 68 % die Elektronik- und IT-Sachversicherungen, die sogar bei einem Drittel der Versicherten schon einmal einspringen mussten. Auf „den Plätzen“ folgen Elektronik-/IT-Betriebsunterbrechungsversicherung mit 27 %, Daten-/Softwareversicherung mit 20 %, Datenhaftpflicht mit 16 % und Datenrechtsschutz-Versicherung mit 10 % Abschlüssen im Teilnehmerfeld. Immerhin 29 % äußerten, überhaupt keine Versicherung mit ISi-Bezug abgeschlossen zu haben. Weiterhin eher selten war die Forderung oder Förderung eines ISi-Audits oder anerkannten ISi-Zertifikats im Zusammenhang mit Versicherungen: Nur 4 % mussten für eine Police einen solchen Nachweis vorlegen, für 12 % hätte oder hat dies zumindest günstigere Konditionen bedeutet.

Genutzte Outsourcing-Funktionen	ja, bei
Vernichtung von Datenträgern (Papier, EDV)	61%
Netzwerk-Management	35%
Managed Firewall/IDS/IPS	34%
Anwendungssysteme	27%
Content Security/Virenabwehr	26%
gesamte(s) Rechenzentrum/IT	19%
Haustechnik	19%
Betriebssystempflege/Administration	18%
Datenbank-Systeme/-Werkzeuge	18%
Datensicherung, Backup-Lösungen	17%
Personaleinsatz/-entwicklung, Mitarbeiterweiterbildung	11%
Sonstiges	10%
Notfallvorsorge/Business Continuity	9%
Dokumentation, Archivierung	8%
Datenschutz	8%
externer ISi-Beauftragter	5%
Überwachung, Kontrolle, Qualitätssicherung	2%

Basis: 88 Antworten

Tabelle 5: Genutzte Outsourcing-Funktionen

Risikobewertung

Dem Punkt „Verzögerungen von Arbeitsabläufen“ wurde bei den Kriterien zur Risikobewertung in diesem Jahr ein höherer Stellenwert zugemessen – solche Störungen liegen jetzt an dritter Stelle der Werteskala (Tab. 7). Im Übrigen blieb alles in etwa beim Alten: Verstöße gegen Gesetze, Vorschriften und Verträge stehen unangefochten auf Rang 1, gefolgt von der Angst vor Imageverlusten. Zur Risikoanalyse haben – wie schon 2004 – 70 % der Teilnehmer Anwendungen und Systeme hinsichtlich der Bedeutung für die Aufgabenerfüllung und bestehender Risiken bewertet. Der Anteil, der hierbei alle Systeme einbezieht, ist um fünf Prozentpunkte auf 26 % gestiegen (s. Abb. 5).

Die meistgenutzte Methodik zur Risikobewertung waren standardisierte Verfahren (BS 7799, IT-Grundschutz usw.): 47 % der Teilnehmer greifen darauf zurück. 41 % nutzen eine eigene Methodik oder Software, 16 % Verfahren von Herstellern oder Beratern (Mehrfachnennungen möglich). Spezielle Risikomanagement-Software ist nur bei 2 % der Befragten im Einsatz – 16 % gaben an, kein strikt methodisches Vorgehen anzuwenden. Im Übrigen bejahten 54 %, dass das IT-Risikomanagement in ihrem Hause in ein allgemeines Risikomanagement des (Gesamt-)Unternehmens eingebunden ist.

Gesetze und Regularien

Die erneut gestiegene Zahl von Teilnehmern, welche die Einhaltung von Gesetzen und Regularien als „sehr wichtig“ ansehen, korrespondiert heuer mit gesteigerten Kenntnissen (potenziell) einschlägiger Regelwerke

Ansprechpartner für forensische Analysen	auf jeden Fall	bevorzugt	normalerweise	nachrangig	keinesfalls	Vergleichszahl **
eigene IT-Abteilung	57%	20%	14%	6%	3%	2,09
eigene Rechtsabteilung	41%	9%	18%	19%	13%	1,03
eigene Revision	34%	19%	11%	19%	18%	0,79
Strafverfolgung (Polizei, Staatsanwaltschaften)	23%	17%	23%	29%	8%	0,74
Fachdienstleister für Computer-Forensik	13%	20%	13%	34%	20%	-0,01
externer, bereits bekannter IT-Dienstleister	9%	22%	17%	32%	21%	-0,07
externer Rechtsbeistand	14%	16%	12%	35%	24%	-0,23
BSI	12%	13%	13%	38%	23%	-0,31
externes CERT/CSiRT	7%	8%	5%	37%	43%	-1,26
externe Wirtschaftsberatung/-prüfer	5%	8%	4%	39%	43%	-1,34
** Gewichtung für Vergleichzahl	3	2	1	-1	-3	

Basis: 144 Antworten (mind. einer Teilfrage)

Tabelle 6: Ansprechpartner für forensische Analysen

Folgende Kriterien sind ...	sehr wichtig	wichtig	un-wichtig	Vergleichs-zahl	Vergleichs-zahl 2004
Verstöße gegen Gesetze/ Vorschriften/Verträge	56%	34%	10%	1,46	1,40
Imageverlust	52%	33%	15%	1,36	1,35
Verzögerung von Arbeitsabläufen	39%	53%	8%	1,31	1,21
direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	39%	49%	11%	1,28	1,26
Schaden bei Dritten/ Haftungsansprüche	40%	48%	12%	1,28	1,27
indirekte finanzielle Verluste (z.B. Auftragsverlust)	35%	42%	23%	1,12	1,14
direkter finanzieller Schaden an Hardware u. ä.	17%	61%	22%	0,95	0,75
Verstöße gegen interne Regelungen	13%	63%	24%	0,89	0,72

Tabelle 7: Kriterien zur Risikobewertung

Basis: Ø 145 Antworten

(Abb. 6): Die Bekanntheit stieg jeweils um 5–18 Prozentpunkte im Vergleich zur vorigen Studie; gleichzeitig sahen auch jeweils 10–18 Prozentpunkte mehr Befragte diese Regelungen als relevant an. Eine Ausnahme bildet lediglich die Signaturgesetzgebung: Die Zahl der Teilnehmer, die Signatur-Gesetz (SigG) und -Verordnung (SigV) inhaltlich kennen, sank um sieben Prozentpunkte, deren Relevanz um einen.

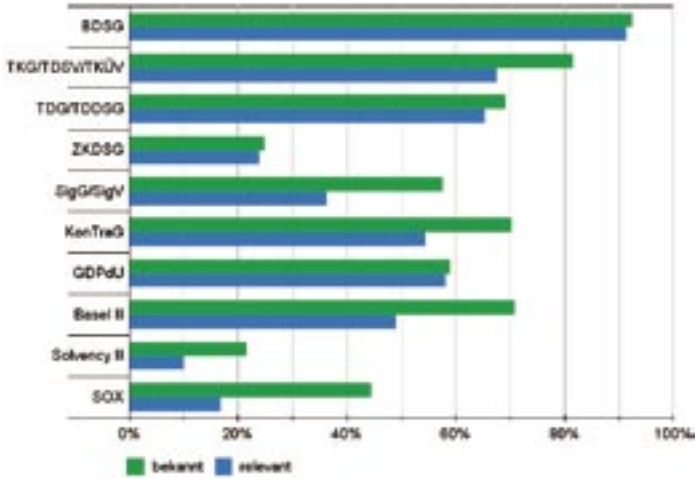


Abbildung 6: Bekanntheit und Relevanz von Gesetzen und Regularien

Basis: Ø 147 Antworten (Bekanntheit), Ø 128 (Relevanz)

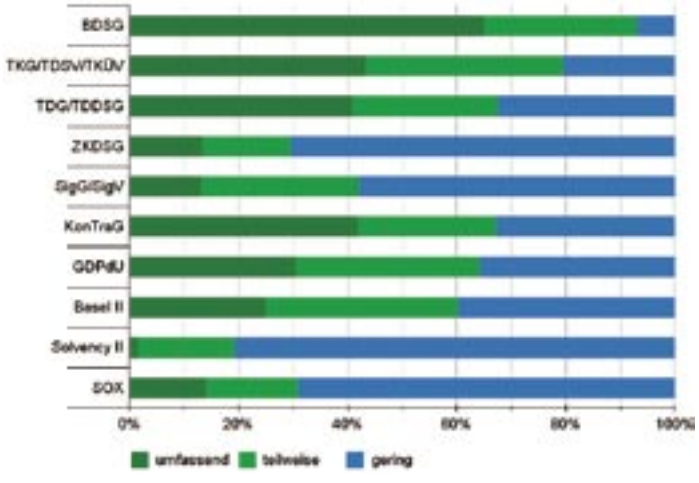


Abbildung 7: Umsetzungsgrad von Gesetzen und Regularien

Basis: Ø 94 Antworten

Die durchweg höchste Steigerung erzielte hingegen – endlich – das Gesetz zur Kontrolle und Transparenz bei Aktiengesellschaften und publizitätspflichtigen Gesellschaften (KonTraG): Kenntnis und Relevanz legten um 18 Prozentpunkte zu und auch bei der Umsetzung machte das Gesetz den deutlichsten Sprung (s. Abb. 7) nach vorne. Ebenfalls nachgelegt wurde bei der Umsetzung der Telekommunikations-Regularien und bei Basel II (Eigenkapitalvorschriften für das Kreditgewerbe).

Keine große Rolle spielen in der Praxis des deutschsprachigen Raums bislang offenbar die „Newcomer" Solvency II (EU-Projekt zum Rahmenwerk für die Versicherungsaufsicht) und der US-amerikanische Sarbanes-Oxley Act (SOX), der zwar schon 44 % der Befragten inhaltlich bekannt ist, aber nur von 17 % als relevant angesehen wird.

Erstmals haben wir zudem nach einer Beurteilung der Angemessenheit deutscher Gesetze und Regulierung gefragt (Tab. 8). Zwischen 49 % und 70 % attestierten dem hiesigen Gesetzgeber dabei jeweils gute Arbeit; die übrigen Befragten waren in den meisten Bereichen klar polarisiert. Die deutlichsten Kritikpunkte: 49 % sehen die Strafgesetze bezüglich der Computer-Kriminalität als unzureichend an – gleichzeitig nannten aber auch 38 % die TK- und Internet-Überwachung überzogen (obwohl diese ja überwiegend vom Interesse der Strafverfolgung getrieben wird). Gespalten zeigte man sich in Sachen Signaturgesetz: Dort bezeichneten fast so viele Studienteilnehmer diesen Bereich als überzogen wie als unzureichend reguliert.

Kenntnisstand und Weiterbildung

Die Einschätzung des Kenntnisstands zur Informations-Sicherheit bei Management und Mitarbeitern zeigt im Großen und Ganzen

Anzeige

Bewertung ...	überzogen	angemessen	unzureichend
Datenschutz	23%	70%	7%
TK-/Internet-Überwachung	38%	49%	13%
Strafgesetze (bzgl. Computer-Kriminalität)	2%	49%	49%
Signaturgesetz	17%	61%	22%
E-Business (Verträge, Haftung, ...)	8%	63%	29%
Risikomanagement	9%	58%	33%

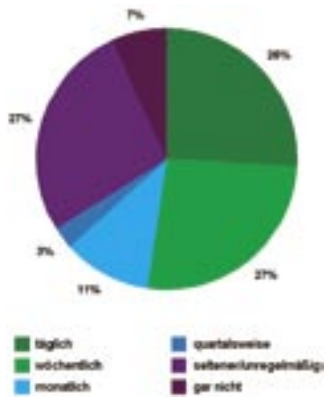
Basis: Ø 144 Antworten

Tabelle 8: Bewertung deutscher Gesetze und Regularien

ein gewohntes Bild (Abb. 8). Lediglich die gewohnt guten Noten für die Sicherheits-Fachleute scheinen mit einem Gesamt-Schnitt von 1,9 etwas nachgegeben zu haben, was aber bei genauerer Betrachtung auf den höheren Anteil aus den kleinen und mittleren Unternehmen (KMU) zurückzuführen ist: In den großen Unternehmen schätzen 93 % die ISi-Kenntnisse ihrer Fachkräfte als „sehr gut" oder „gut" ein, die restlichen 7 % „befriedigend" (Durchschnitt: 1,6). Demgegenüber zeigt sich bei den KMU mit 77 % „sehr gut" und „gut" sowie 13 % „befriedigend" auch noch eine 10 % große Gruppe, die nur „ausreichend" oder „nicht ausreichend" bewertet wird, sodass sich hier nur ein Durchschnitt von 2,1 ergibt. Auch die Noten der Anwender hochsensitiver Bereiche liegen bei den KMU um eine Drittelnote schlechter als in großen Unternehmen.

Vielen Dank für freundliche Unterstützung unserer Studie

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.



Basis: 147 Antworten

Abbildung 10: Prüfungsintervalle passiver Kanäle zu Sicherheits-Updates

Genutzte Ausbildungsmethoden	häufig	gelegentlich	nie	Vergleichszahl*
interne Schulungen durch Frontalunterricht für Spezialgruppen	15%	60%	24%	1,06
externe Schulungen	13%	64%	22%	1,04
Materialien (Schulungsunterlagen) zum Selbstlernen	17%	45%	38%	0,95
interne Schulungen durch Frontal-unterricht, möglichst flächendeckend	14%	45%	41%	0,87
Online-Trainings-Anwendungen/-Tools (Intranet)	10%	36%	54%	0,66
(Multimediale) Lern-CDs zum Selbstlernen	9%	30%	61%	0,58

Basis: Ø 134 Antworten

*Vergleichszahl errechnet aus: häufig = 3, gelegentlich = 1, nie = 0

Tabelle 9: Genutzte Ausbildungsmethoden

Betrachtet man Schulungsmethoden und -frequenz, so findet man wenig Veränderungen zur vorigen Studie. Nach wie vor stehen gelegentliche interne Weiterbildungen durch Frontalunterricht für Spezialgruppen sowie externe Schulungen am höchsten im Kurs (Tab. 9). Häufige externe Trainings sind zwar etwas seltener geworden (von 19 % in 2004 auf jetzt 13 %), gleichzeitig schrumpfte aber auch die Gruppe derer, die überhaupt nicht auf Derartiges zurückgreift um vier Prozentpunkte. Bei den Mitarbeitergruppen fällt auf, dass ISi-Beauftragte und vor allem Revisoren und Prüfer seltener geschult werden. Während die ISi-Spezialisten allerdings immer noch den Spitzenplatz bei der Weiterbildung innehaben, fallen die Prüfer hinter den Weiterbildungswert der Benutzer zurück, da über ein Drittel überhaupt keine Schulung mehr erfährt (vgl. Abb. 9).

Die mehr oder minder große Wertschätzung externer Schulungen mit Prüfung zeigt sich in der Frage nach der Bedeutung von Berufszertifikaten: Jeweils 56 % der Befragten finden solche Zertifikate „weniger wichtig“. Bei herstellerspezifischen Zertifikaten zur Aus- und Weiterbildung (MCSE, CCNE usw.) hielten sich die extremeren Aussagen „sehr wichtig“ und „unwichtig“ mit jeweils 22 % die Waage. Herstellerunabhängige Zertifikate (CISSP, CISM usw.) befanden immerhin 30 % als „sehr wichtig“. In Sachen Bekanntheit führt der CISA mit 62 % Nennungen vor CISM (54 %), CISSP (52 %) und ferner TISP (21 %) und SSCP (19 % – zu den Zertifikaten vgl. <kes> 2006#3, S. 27).

Informationsquellen

Zur allgemeinen Information über IT-Sicherheit auf Messen und Kongressen nutzen 65 % der Befragten die CeBIT, 45 % den BSI-Kongress, 38 % die IT-SecurityArea auf der SYSTEMS, 15 % die Essener SECURITY, 7 % die Infosecurity Europe (London) und 4 % die ISSE (wechselnde Orte). Bei den Zeitschriften stehen neben der <kes> vor allem die c’t, DuD sowie Computerwoche und iX hoch im Kurs. Bei Mailing-Listen und Web-Angeboten dominieren klar das BSI sowie der Heise-Verlag die virtuelle Sicherheitslandschaft; auf dem dritten Platz liegt Security Focus (Bugtraq u. a.). Bei den bevorzugten Webseiten wurden zudem die Angebote von Microsoft und SANS.org gehäuft genannt.

Wenig überraschend ist Microsoft bei den Herstellerangeboten meistgenannt, gefolgt von (gleichauf) Check Point, Cisco, SAP und Sophos, wobei insgesamt nur wenige Teilnehmer Angaben zu Herstellerseiten für allgemeine Sicherheitsinfos gemacht haben. Zur Information über Security-Updates werden diese Angebote jedoch eher genutzt: 62 % gaben an, die ISi-Bulletins von Microsoft abonniert zu haben – es folgen heisec.de (46 %), CERT-Bund (36 %), Symantec (30 %) und ferner US-CERT.gov und SANS.org mit je 10 %.

Generell ist die bevorzugte Informations-Art zu Sicherheits-Updates die aktive Aussendung durch

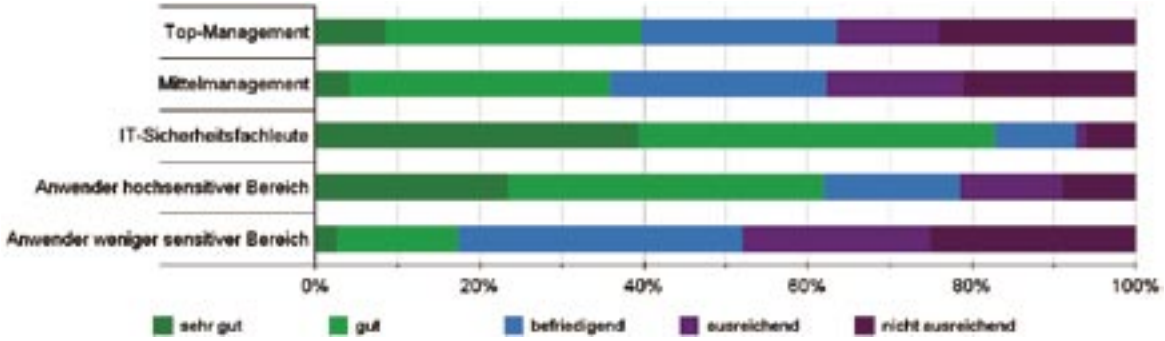
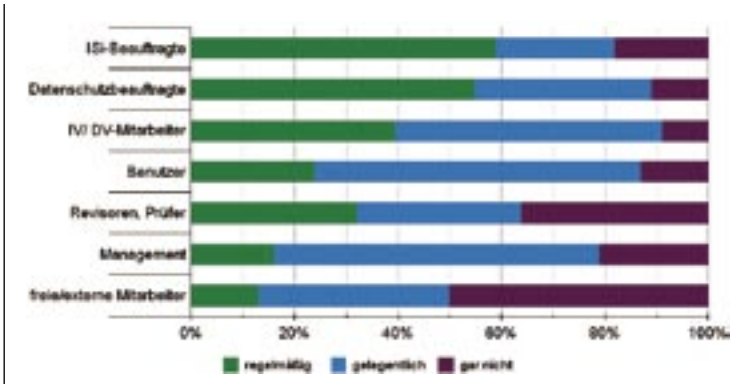


Abbildung 8: Kenntnisstand der Manager und Mitarbeiter



Abbbildung 9: Schulungsfrequenz verschiedener Mitarbeitergruppen

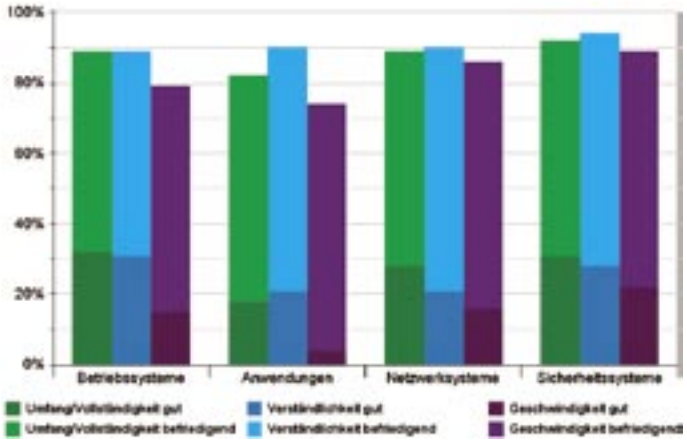


Abbildung 11: Qualität von Herstellerinfos

Basis: Ø 141 Antworten (Umfang), Ø 137 (Verständlichkeit), Ø 138 (Geschwindigkeit)

den Hersteller: 75 % der Befragten nutzen diesen Weg, gefolgt von Mailing-Listen Dritter (45 %), Abfragen der Informationsseiten von Herstellern und Dritten (je 44 %) sowie aktiver Aussendung durch Händler oder Systemhäuser (33 %). Gut die Hälfte der Studienteilnehmer fragt dabei „passive" Kanäle täglich oder zumindest wöchentlich ab (Details s. Abb. 10 auf S. 47).

Die Qualität der Herstellerinformationen kann dabei als befriedigend gelten (Abb. 11): Die größte Zufriedenheit findet man insgesamt bei den Sicherheitssystem-Anbietern sowie bezüglich Vollständigkeit und Verständlichkeit der Betriebssystem-Infos (Benotung jeweils 2,9), die größte Unzufriedenheit bei den Informationen zu Anwendungssystemen (Gesamtnote 3,2). Auffällig ist die kritische Beurteilung der Geschwindigkeit von Informationen der Betriebssystemanbieter, welche die in den anderen Kategorien besseren Noten auf das Niveau der Netzwerkanbieter „drückt" (beide insgesamt 3,0). ■

*Der dritte Teil der Auswertung folgt in <kes>2006*6*

Die Auswertung der <kes>/Microsoft-Sicherheitsstudie erfolgte inklusive Erstellung der Ergebnistabellen und aller Grafiken größtenteils mit dem interaktiven Analysewerkzeug InfoZoom. Wir bedanken uns bei humanIT (www.humanit.de) für die freundliche Unterstützung in technisch-organisatorischer Hinsicht.