SONDERDRUCK KES/KPMG-Sicherheitsstudie 2002

KES

Zeitschrift für Kommunikations- und EDV-Sicherheit

KPMG

Information Risk Management

- Bedeutendste Risiken: Irrtum und Nachlässigkeit eigener Mitarbeiter, gefolgt von Viren, Würmern und Trojanischen Pferden (Malware) – auf Platz drei liegen Softwaremängel
- Risikobewertung: drohender Imageverlust steht an erster Stelle, gefolgt von Verstößen gegen Gesetze und Verträge – Angst vor finanziellen Schäden nachrangig
- Digitale Signaturen: geringe Nutzung in der B2B-Kommunikation – kaum Infrastruktur im Feld – signaturgesetzkonforme Lösungen wenig gefragt
- Verschlüsselung: gewachsene Bereitschaft bei mobilen Systemen und E-Mails – OpenPGP dominiert
- Konzept-Kontrolle dringend geboten: 89 % aller Prüfungen decken Schwachstellen auf

KES/KPMG-Sicherheitsstudie 2002

Lagebericht zur IT-Sicherheit

Von Reinhard Voßbein und Jörn Voßbein, Wuppertal

Verlässliche Zahlen zu Risiken und Angriffen sowie Konzepten und Maßnahmen der IT-Sicherheit in der aktuellen Praxis sind selten, ganz zu schweigen von Erkenntnissen über konkrete Vorhaben für die sicherheitsrelevante Zukunft der IT-Landschaft. Als umso nützlicher dürften sich die Ergebnisse der 9. Sicherheitsstudie aufgrund der umfassenden Antworten hochkarätiger Teilnehmer erweisen.

Mit 260 Teilnehmern hat eine erfreulich große Anzahl von Unternehmen und Behörden an der KES/KPMG-Sicherheitsstudie teilgenommen, sodass hierdurch noch aussagekräftigere Werte ermittelt werden konnten als 2000. Die Autoren sehen darin aber auch eine Bestätigung für das wachsende Interesse an der Studie und ihrer Thematik.

Die Fragen der Studie hatten sich gegenüber den vergangenen Jahren erneut in Einzelgebieten gewandelt, neue Themen sind dem Stand der Technik folgend hinzugekommen, andere weggefallen. Die Komplexität der heutigen IT-Sicherheitslandschaft hat in der Summe zu einer leichten Erweiterung geführt, was jedoch ebenfalls die Aussagefähigkeit der Studie verbessert hat.

Risikosituation

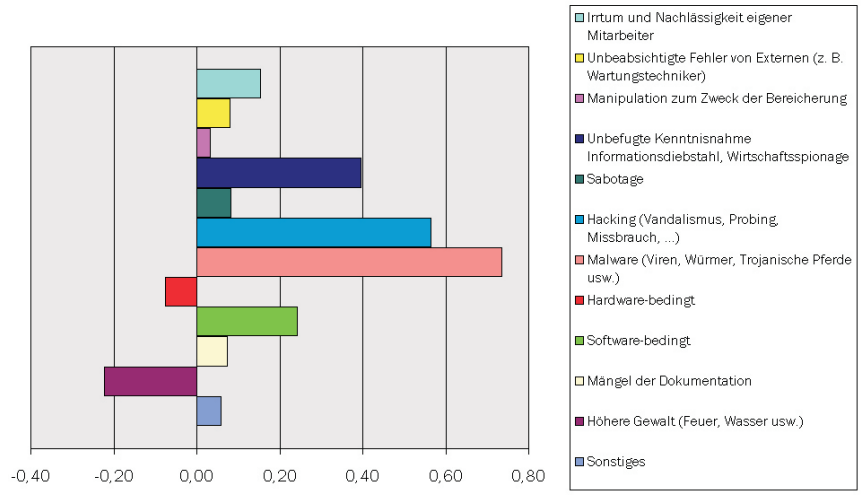
Nach wie vor dominieren die von Menschen direkt verursachten Gefahren die aktuelle Risikolage, wobei die unbeabsichtigten Wirkungen deutlich überwiegen. Als bedeutendstes Einzelrisiko haben die Teilnehmer der KES/KPMG-Studie erneut Irrtum und Nachlässigkeit eigener Mitarbeiter genannt, gefolgt von Malware und Softwaremängeln, und zwar sowohl in der Risikoeinschätzung als auch bei den tatsächlichen Schäden. Die einzelnen Angaben weichen zwar durch eine veränderte Prozentuierung zahlenmäßig von denen der Vorjahre deutlich ab, die eigentlichen Aussagen stimmen aber mit den früheren Ergebnissen überein.

Auch bei den erwarteten Veränderungen gab es keine Überraschungen: Malware und zielgerichteten aktiven Angriffen (Hacking, Spionage, usw.) wird wiederum eine deutliche Zunahme prognostiziert. Etwas milder als in der letzten Studie schätzt man das Ansteigen von Irrtum und Nachlässigkeit sowie Softwareproblemen. Hardwaremängel und höhere Gewalt sollen weiter zurückgehen. Die Gegenüberstellung in der Rangordnung der Gefahrenbereiche zwischen dem „Jetzt“ und der „Zukunft“ avisiert einen Aufstieg von Malware zum Top-Risiko. Die unbeabsichtigten Fehler von Externen steigen von Platz zehn auf Platz vier, hardwarebedingte Gefahren fallen von Platz sechs auf Platz zehn; Sabotage steigt dadurch in ihrer erwarteten zukünftigen Bedeutung deutlich an.

Die Auswertung der *aktuellen* Risiken belegt nach wie vor eine Wahrnehmungsverzerrung in der öffentlichen Diskussion, wo verschiedene Gefahren in ihren Auswirkungen deutlich überschätzt werden, was besonders auf das Hacking zutrifft. Ob die allgemeine Angst vor Viren, Hackern und Spionen, die sich mit der erwarteten Risikoveränderung deckt, auch in den Köpfen der Sicherheitsexperten „zugeschlagen“ hat oder die kommenden Jahre tatsächlich eine Umschichtung der Risiken bringen wird, bleibt abzuwarten. Die Malware hat sich zwar mittlerweile tatsächlich von den Softwarerisiken abgesetzt, mit denen sie vor zwei Jahren noch gleichauf lag. Entsprechende Prognosen der vergangenen Studie scheinen sich jedoch im Hinblick auf gezielte Angriffe (Hacker, Spione) nicht bewahrheitet zu haben – oder zumindest erfolg-

Welche dieser Gefahrenbereiche haben in Ihrem Haus in den vergangenen beiden Jahren tatsächlich zu mittleren bis größeren Beeinträchtigungen geführt?
(Mehrfachnennungen möglich)

Basis der Prozentuierung:		260
	Summe	Prozent
von Menschen direkt verursachte Gefahren	135	52 %
Irrtum und Nachlässigkeit eigener Mitarbeiter	79	30 %
unbeabsichtigte Fehler von Externen (z. B. Wartungstechniker)	23	9 %
Manipulation zum Zweck der Bereicherung	6	2 %
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	16	6 %
Sabotage	4	2 %
Hacking (Vandalismus, Probing, Missbrauch, ...)	21	8 %
Malware (Viren, Würmer, Trojanische Pferde usw.)	64	25 %
technische Defekte/Qualitätsmängel	85	33 %
Hardware-bedingt	38	15 %
Software-bedingt	50	19 %
Mängel der Dokumentation	8	3 %
höhere Gewalt (Feuer, Wasser usw.)	8	3 %
Sonstige	17	7 %



Veränderungsfaktor der Risiken

Nennen Sie bitte die drei Gefahrenbereiche, die aus Ihrer Sicht für Ihr Haus die höchste Bedeutung haben (Mehrfachnennungen möglich)

	Rangfolge	
	Jetzt	Zukunft
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	2
Malware (Viren, Würmer, Trojanische Pferde usw.)	2	1
Software-bedingte technische Defekte/Qualitätsmängel	3	3
Unbefugte Kenntnisnahme Informationsdiebstahl, Wirtschaftsspionage	4	5
Hacking (Vandalismus, Probing, Missbrauch, ...)	5	6
Hardware-bedingte technische Defekte/Qualitätsmängel	6	10
Höhere Gewalt (Feuer, Wasser usw.)	7	11
Manipulation zum Zweck der Bereicherung	8	9
Mängel der Dokumentation	9	8
Unbeabsichtigte Fehler von Externen (z. B. Wartungstechniker)	10	4
Sabotage	11	7
Sonstiges	12	12

reich abgewehrt beziehungsweise erst garnicht registriert worden zu sein.

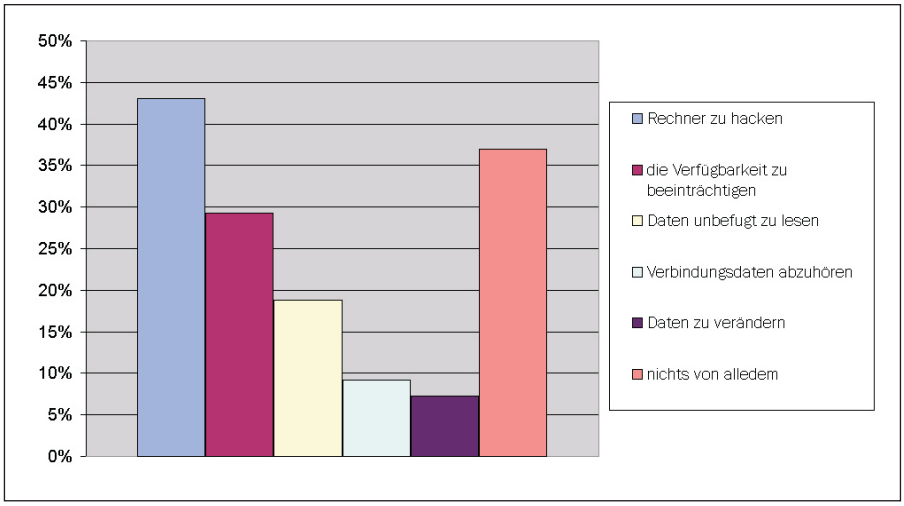
Internet

Ähnliches zeigt sich auch bei den Antworten zu Angriffen über den Internetzugang und auf WWW-Server: 37 Prozent der Befragten haben keinen Angriffsversuch gegen Verfügbarkeit, Vertraulichkeit oder Integrität ihres Internetzugangs vermerkt, bei der spezielleren Webserver-Frage verbuchten 57 Prozent keine solchen Attacken. Spitzenreiter bei den Nennungen zum Internetanschluss waren Hack-Versuche (43 %) und Denial of Service (DoS, 29 %). Bei den Webservern rangierten DoS-Angriffe (28 %) vor Spionage und „Defacement“, dem vandalistischen Verändern von Inhalten (16 %). Nur selten war der Versuch wahrgenommen worden, Daten auf WWW-Servern in betrügerischer Absicht zu manipulieren, wobei sich hier die Frage stellt, ob die meisten Inhalte eine entsprechende Absicht überhaupt lohnend erscheinen lassen.

Zudem bleibt ungewiss, wie viele Angriffsversuche unbeobachtet stattfanden: Nur rund ein Drittel der Studienteilnehmer setzt Intrusion Detection Systeme ein (Näheres siehe Seite 12).

Ein großer Teil der befragten Unternehmen nutzt WWW und vor allem E-Mail für alle Mitarbeiter. Trotz der Gefahren, die aus dem Internet auf interne Netze zukommen können, gestatten übrigens nur 10 Prozent

Ist bereits der Versuch unternommen worden, um auf Ihrem WWW-Server ...? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:		238
	Nennungen	%
Angebote lahmzulegen (Denial of Service)	66	28 %
Daten auszuspionieren	40	17 %
Seiten zu verändern (Vandalismus)	37	16 %
Daten in betrügerischer Absicht zu manipulieren	13	5 %
Daten zu löschen	12	5 %
nichts von alledem	135	57 %



Internetorientierte Gefährdungen

Hatten Sie 2001 Vorfälle mit Malware?											
Ja	Nein										
185	66										
74 %	26 %										
ja, und zwar (Mehrfachnennungen möglich)	File-Viren		Boot-Viren		Makro-Viren		Würmer		Trojanische Pferde/ Backdoors	
über Diskette	57	31 %	62	34 %	47	25 %	23	12 %	17	9 %
über internes Netz	28	15 %	11	6 %	35	19 %	35	19 %	21	11 %
über E-Mail	101	55 %	44	24 %	132	71 %	144	78 %	92	50 %
über Internet-Download	38	21 %	10	5 %	45	24 %	30	16 %	34	18 %
über Internet (autom. Verbreitung)	12	6 %	3	2 %	19	10 %	48	26 %	29	16 %
über WWW-Seite (aktive Inhalte)	6	3 %	0	0 %	7	4 %	16	9 %	15	8 %
unbekannte Herkunft	28	15 %	11	6 %	14	8 %	20	11 %	21	11 %
weniger Fälle als 2000	41	36 %	31	42 %	35	27 %	27	21 %	16	18 %
mehr Vorfälle als 2000	74	64 %	42	58 %	93	73 %	102	79 %	75	82 %
Summe	115		73		128		129		91	
nein	38	15 %	49	20 %	35	14 %	35	14 %	45	18 %

der Unternehmen den Mitarbeitern keinerlei private Nutzung. Somit nimmt die überwältigende Mehrheit der Unternehmen gleichzeitig datenschutzrechtliche Probleme bei der Kontrolle solcher privaten Aktivitäten in Kauf.

Viren, Würmer & Co.

Malware ist jedoch weiterhin eine ernste Bedrohung: 74 Prozent der befragten Unternehmen haben im vergangenen Jahr Malwarevorfälle vermeldet, über 70 Prozent einen Zuwachs von Schadsoftware unterschiedlicher Art wahrgenommen. Zum Glück scheinen die meisten Vorfälle aber glimpflich zu verlaufen: Nur 25 Prozent hatten mittlere bis größere Beeinträchtigungen angegeben.

Bei nahezu 50 Prozent der Teilnehmer gab es bereits einmal einen Virenfehlalarm: Eine teure Angelegenheit, die im Einzelfall bis zu 50 000 Euro geschätzte Kosten verursachen kann (Durchschnitt 8 173 €). Die Schätzungen für Ausfallzeit und Kosten bei nicht-technischen Fehlalarmen durch unbegründete Warnungen vor vermeintlichen Viren (Hoaxes) liegen sogar noch etwas darüber.

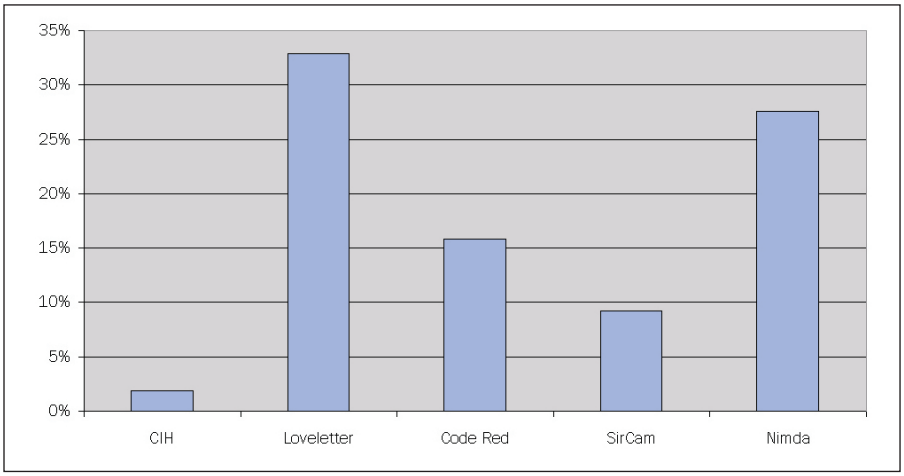
Der höchste genannte Schadenswert für einen einzelnen Virenvorfall betrug 200 000 Euro. Die durchschnittlichen geschätzten Kosten durch einen Virus lagen mit rund 26 000 Euro in etwa bei dem dreifachen Wert der Fehlalarme. Diese Schätzungen wirken erfreulich realistisch im Vergleich zu aus dem amerikanischen Raum gemeldeten Virenschäden, die durchweg erst bei Millionen-Dollar-Werten anfangen.

Bezüglich des Einfallweges für Malware dominiert die E-Mail, lediglich bei Bootviren naturgemäß die Diskette. Die Summe der Schädlinge, die ihren Weg über Netzwerke (Internet und LAN) nehmen, ist ebenfalls hoch. Keine Entwarnung gibt es allerdings auch für Datenträger als Infektionsrisiko: Bei Fileviren, Makroviren und Würmern stehen Disketten (vermutlich auch CD-ROMs) an zweiter Stelle, lediglich bei trojanischen Pferden nimmt der Download aus dem Internet Rang zwei ein. Ein überwiegender Rückgang der Vorfälle war übrigens auch bei den Klassen der File- und Boot-Viren *nicht* zu verzeichnen.

In der Folge sollten Sicherheitsmaßnahmen in Bezug auf Malware unbedingt auf der E-Mail-Ebene beginnen, sie dürfen aber angesichts der Datenträgerrisiken die Arbeitsplatzcomputer nicht außer Acht lassen. Die Situation bei den Teilnehmern der KES/KPMG-

Studie zeigt nahezu vollständige Erfassung von Servern und Client-Rechnern durch Virenschutzmaßnahmen, allerdings Mankos bei mobilen Endgeräten (nur 88 % mit Virenabwehr) und seltenen Einsatz von Virenwächtern im Hintergrund, die nur weniger als ein Fünftel der befragten Unternehmen nutzen (Details zu den Maßnahmen, siehe Seite 10).

Die Sicherheit gegen neue Malware-Bedrohungen ist erwartungsgemäß beschränkt: Jeweils um die 30 Prozent der befragten Studienteilnehmer mussten trotz Viren-„Schutz" in den letzten zwei Jahren nennenswerte Beeinträchtigungen durch Loveletter und Nimda erfahren. Der ältere, aber immer noch verbreitete CIH-Virus verursachte hingegen kaum Probleme.



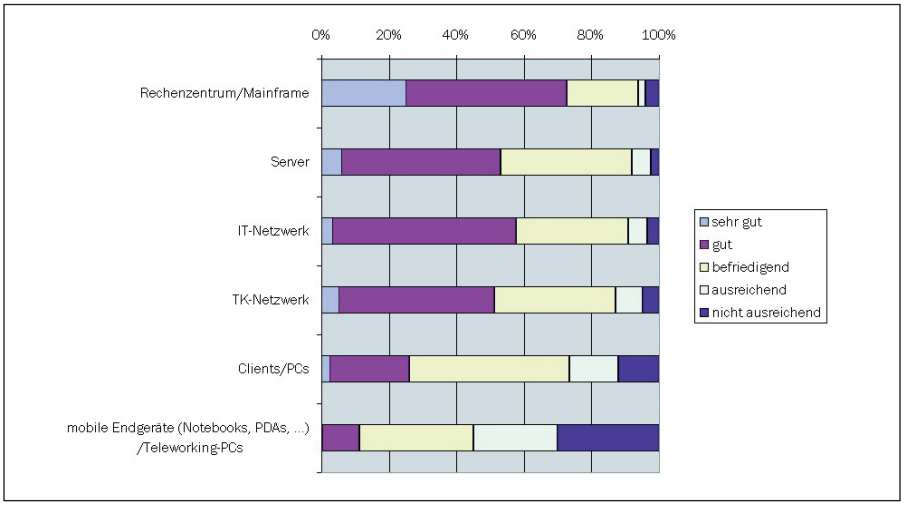
Beeinträchtigung durch verbreitete Malware

Wie hoch schätzen Sie die Ausfallzeit und die Kosten ein?						
	die Ausfallzeit (in Std.)			die Kosten (in €)		
verursacht durch einen einzelnen ...	Höchste Nennung	Durchschnitt	Anzahl Nennungen	Höchste Nennung	Durchschnitt	Anzahl Nennungen
Virus	1680	94	102	200 000 €	26 228 €	70
Fehlalarm (unbegründete Fehlermeldung)	100	10	58	50 000 €	8 173 €	34
unbegründete Warnung (Hoax)	100	13	67	60 000 €	9 621 €	41

Sicherheitslage

Immer wieder bestätigt die KES-Sicherheitsstudie eine positive Einschätzung der Informationssicherheit (ISi) im Rechenzentrumsbereich: Nahezu drei Viertel der Befragten sehen sie als gut bis sehr gut an. Je „weiter" sich die Systeme von der zentralisierten zur verteilten Informationstechnik bewegen, desto schlechter wird die Einschätzung der Sicherheitslage: Bei Servern und Netzwerken antworten die meisten mit „gut", bei Clients/PCs mit „befriedigend". Deutliche Schwächen sehen die Teilnehmer im Bereich der mobilen Endgeräte und Teleworking-PCs: Mehr als die Hälfte der Befragten bewerteten den Stand nur mit „ausreichend" oder „nicht ausreichend" – 30 Prozent gaben selbstkritisch die schlechteste Bewertung.

Wie schätzen Sie die Informationssicherheit (ISi) in Ihrem Haus ein, bezogen auf...?	Durchschnittsnote
Rechenzentrum/Mainframe	2,1
Server	2,5
IT-Netzwerk	2,5
TK-Netzwerk	2,6
Clients/PCs	3,1
mobile Endgeräte (Notebooks, PDAs, ...) / Teleworking-PCs	3,7
Noten von „sehr gut" (1) bis „nicht ausreichend" (5)	



Bewertung der Informationssicherheit

Stellenwert der Informationssicherheit

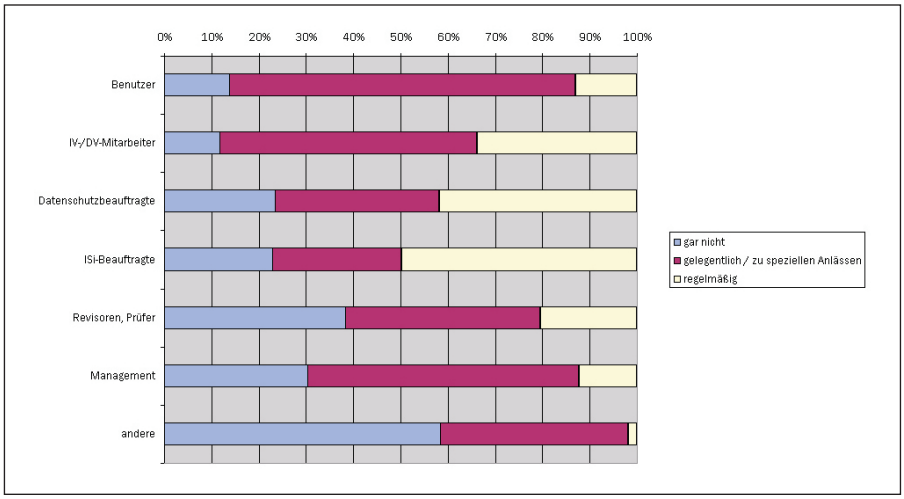
Ein seit Jahren eher trauriges Kapitel ist die Beurteilung des Stellenwertes der IT-Sicherheit für das Top- und Mittlere Management. So wird mit beachtlicher Kontinuität angegeben, dass nur ein geringer Teil des Managements IT-Sicherheit als vorrangiges Ziel der Informationsverarbeitung ansieht und lediglich 50 Prozent der Top-Manager betrachten die IT-Sicherheit als gleichrangiges Ziel im Rahmen der Informationsverarbeitung. Ein Vergleich mit den Werten früherer Studien zeigt, dass sich selbst über einen langen Zeitraum nur wenig im Bewusstsein des Top-Managements verändert hat.

Kenntnisstand und Schulung zur ISi

Ähnlich schlecht ist die Beurteilung des Kenntnisstandes zur IT-Sicherheit. In über

Welchen Stellenwert hat die ISi für Ihr Top-Management?			
	1994	2000	2002
ISi ist ein vorrangiges Ziel der Informationsverarbeitung	16 %	23 %	20 %
ISi ist ein gleichrangiges Ziel der Informationsverarbeitung	49 %	46 %	50 %
ISi ist eher ein „lästiges Übel“	35 %	30 %	29 %

Wie beurteilen Sie den Kenntnisstand zur ISi in Ihrem Unternehmen?					
	sehr gut (1)	gut (2)	mittel (3)	eher schlecht (4)	nicht beantwortbar
IT-Sicherheitsfachleute	32 %	49 %	13 %	1 %	5 %
Anwender in hochsensitiven Bereichen	16 %	37 %	25 %	16 %	6 %
Top Management	10 %	23 %	32 %	30 %	4 %
Mittelmanagement	3 %	15 %	46 %	33 %	4 %
Anwender in weniger sensitiven Bereichen	2 %	9 %	35 %	48 %	6 %



Schulungsaktivitäten

Welche Funktionen haben Sie ausgelagert?	
Basis der Prozentuierung:	144 Outsourcinggeber
Entsorgung von Datenträgern (Papier, EDV)	72 %
Managed Firewall/IDS	48 %
Online-Anwendungssysteme	40 %
Netzwerk-Management	37 %
Datenbank-Systeme, Werkzeuge	33 %
Betriebssystempflege	32 %
Sicherung, Back-up-Lösungen	29 %
Auftragsentwurf, Arbeitsvorbereitung, Operating	26 %
Haustechnik	24 %
Überwachung, Kontrolle, Qualitätssicherung	16 %
Verwaltung, Dokumentation, Archivierung	15 %
Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung	15 %
Datenschutz gemäß BDSG	3 %
Sonstiges	22 %

60 Prozent der Unternehmen wird der Kenntnisstand des Top-Managements als mittel bis eher schlecht beurteilt, bei Anwendern in weniger sensitiven Bereichen liegt diese schlechte Beurteilung sogar bei über 80 Prozent.

Im Zusammenhang mit der Beurteilung der Schulung und Ausbildung ist dieses Ergebnis jedoch stärker erklärlich: So wird das Management nur in zwölf Prozent aller Fälle über Fragen der IT-Sicherheit regelmäßig informiert oder geschult, wohingegen anlassbezogene Schulungen einen Wert von 57 Prozent aufweisen. Das Schwergewicht der Schulungen liegt eindeutig bei Mitarbeitern mit besonderen Aufgabengebieten. Moderne Fortbildungs- und Schulungs-Methoden (online oder Multimedia) werden dabei nur zu einem sehr geringen Teil benutzt. Hier existiert ein deutliches Rationalisierungspotenzial mit Verbesserungsmöglichkeiten zur Erzielung eines besseren Wissensstandes in den Unternehmen.

Informationsquellen

Als weiterer Input dienen Messen: 78 Prozent der Befragten nutzen die CeBIT zur Information über IT-Sicherheit, 50 Prozent besuchen dazu die IT-SecurityArea auf der SYSTEMS, 31 Prozent den BSI-Kongress, 12 Prozent die InfoSecurity und 10 Prozent die Security in Essen.

In der offenen Frage zu Zeitschriften wurde naheliegenderweise die KES mit Abstand am häufigsten als Informationsquelle zur IT-Sicherheit genannt. Überdies gaben 22 Prozent der Antwortenden die c't an, 16 Prozent die DuD (Datenschutz und Datensicherheit), 7 Prozent die „IT-Sicherheit“. 6 Prozent die „IT-Security“, 3 Prozent die Informationweek und 1 Prozent die PC-Professional.

Bei der Suche nach aktuellen Patches gegen Sicherheitslücken stehen Informationsseiten sowie aktive Informationen der Hersteller mit weitem Abstand an der Spitze, gefolgt von Mailinglisten und Informationsseiten anderer Quellen.

Organisation

Die organisatorischen Lösungen zur Gestaltung der IT-Sicherheit werden dominiert durch die Funktion des zentralen Sicherheitsbeauftragten. Er ist immerhin in 36 Prozent aller Unternehmen für die Durchführung von Risikoanalysen, in 38 Prozent für die Erstel-

lung von Konzeptionen und in 35 Prozent für Notfall- und Eskalationsmaßnahmen verantwortlich. Im Hinblick auf diese Aufgaben hat nur der Leiter DV eine ähnlich starke Funktion, wobei diese bei Notfall-und Eskalationsmaßnahmen mit 56 Prozent noch deutlich häufiger genannt ist.

Dienstleister

73 Prozent der Befragten betreiben Outsourcing in irgendeiner Form, wobei die Entsorgung von Datenträgern mit Abstand an der Spitze steht. Auf Platz zwei landen Managed Firewalls/IDS. Erstaunlich ist, dass im Hinblick auf die Bedeutung von Business Recovery und Business Continuity diese Bereiche zusammen mit der Auslagerung von Sicherungsfunktionen unter 30 Prozent liegen.

Allerdings enthalten lediglich 60 Prozent der vertraglichen Vereinbarungen mit den Outsourcingnehmern explizite Anforderungen an die IT-Sicherheit. Und hiervon sehen zirka ein Fünftel der Verträge kein explizites Kontrollrecht vor. In Bezug auf die ausdrücklichen Anforderungen an den Datenschutz ist es in den betreffenden Verträgen nicht erheblich besser bestellt: Hier gelten ähnliche schlechte Zahlen wie bei der Sicherheit.

Das Thema Sicherheitsberatung zeigt hingegen ein deutlich positives Bild. So lassen sich insgesamt zirka 60 Prozent aller befragten Unternehmen regelmäßig oder gelegentlich durch Sicherheitsberater unterstützen. An der Spitze liegt hier deutlich die Durchführung von Risikoanalysen und Konzeptionsentwicklung, gefolgt von Schwachstellenanalysen, Penetrationstests sowie der Strategie- und Managementberatung. Besonders erfreulich ist, dass sich zirka 50 Prozent der Unternehmen uneingeschränkt mit der Beratung zufrieden erklären, und nur drei Prozent nicht zufrieden waren.

Versicherungen

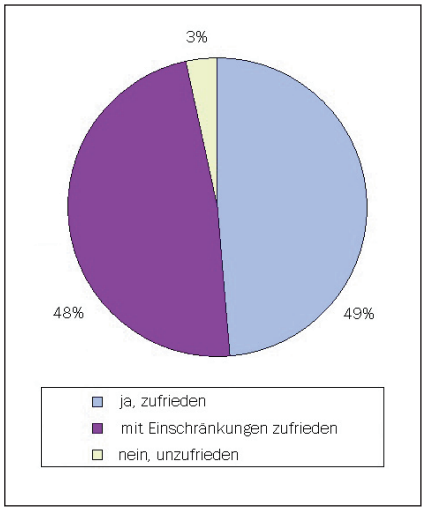
Auch das Bild der Absicherung durch Abschluss von Versicherungen ist im Bereich IT-Sicherheit positiv zu bewerten: So geben 86 Prozent der Befragten an, eine Elektronikversicherung abgeschlossen zu haben, die von einem Drittel auch bereits in Anspruch genommen wurde. Allerdings handelt es sich vorrangig um Sachversicherungen. Nicht überraschend ist der hohe Anteil von Feuerversicherungen, da diese zu den Standards zählen. Im Gegensatz zu der vergleichsweise hohen Inanspruchnahme der Elektronikversicherungen müssen letztere (glücklicherweise) vergleichsweise selten einspringen.

Welche Form von ISi-Beratung nutzen Sie? (Mehrfachnennungen möglich)	
Basis der Prozentuierung:	154 Beratungskunden
Strategie- und Managementberatung	42 %
Durchführung von Risikoanalysen und Konzeptentwicklung	75 %
Durchführung von Schwachstellenanalysen	66 %
Durchführung von Penetrationstests	55 %
Umsetzung von Konzepten und Maßnahmen	32 %
Kontrolle vorhandener Konzepte auf Eignung und Einhaltung	31 %
Sonstiges	8 %

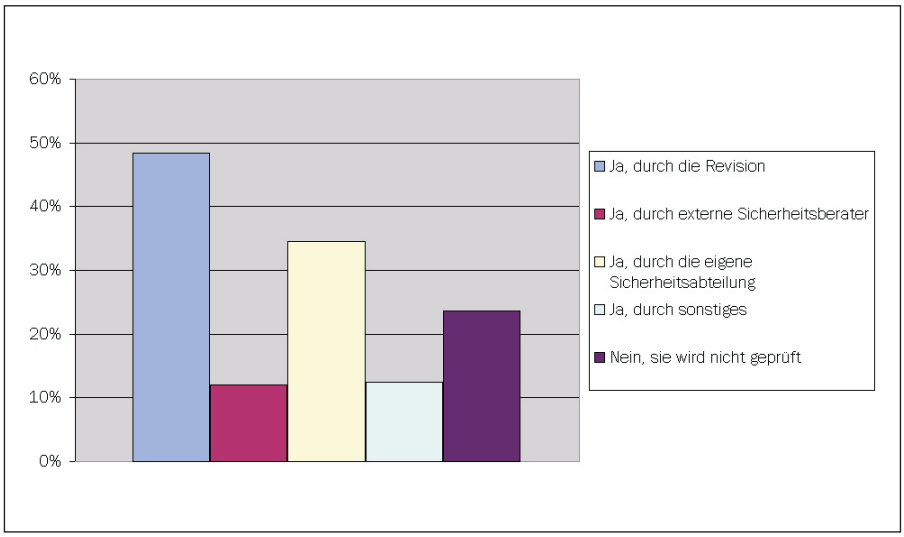
Welche Versicherung aus dem Bereich ISi haben Sie abgeschlossen? (Mehrfachnennungen möglich)				
Basis der Prozentuierung:	235		jeweilige Anzahl Abschlüsse	
	abgeschlossen		davon in Anspruch genommen	
Elektronikversicherung	202	86 %	69	34 %
– Sachversicherung	194	83 %	60	31 %
– Datenversicherung/Softwareversicherung	69	29 %	4	6 %
– Erweiterte Datenversicherung (inkl. Schäden durch Viren, fehlerhaftes Programmieren, versehentliches Löschen)	23	10 %	11	48 %
– Mehrkostenversicherung	26	11 %	6	23 %
– Elektronik-Betriebsunterbrechungsversicherung	65	28 %	3	5 %
Feuerversicherung	188	80 %	10	5 %
„Technologie-Police“ o. ä. (Kombination von Elektronik- u. Maschinenversicherung)	23	10 %	3	13 %
Vertrauensschaden-Versicherung	36	15 %	4	11 %
– Computermissbrauch-Versicherung	36	15 %	4	11 %
– Datenmissbrauch-Versicherung	18	8 %	4	22 %
Datenschutzversicherung	29	12 %	6	21 %
– Datenhaftpflicht-Versicherung	29	12 %	3	10 %
– Datenrechtsschutz-Versicherung	12	5 %	4	33 %
Keine der genannten	22	9 %	11	5 %

Konzepte

Das Thema IT-Sicherheitsstrategie und -Konzepte erwies sich in nahezu allen KES-Studien in der Vergangenheit als eher notleidend. Hier scheint sich eine gewisse Verbesserung abzuzeichnen: 56 Prozent der Befragten gaben an, eine schriftlich fixierte Strategie für die IT-Sicherheit zu haben. Auch die Sicherheitsmaßnahmen basieren zu über 70 Prozent auf schriftlichen Formulierungen. Die Nutzung von Internet und E-Mail beruht sogar zu 86 Prozent auf einer schriftlich fixierten Konzeption. Die genannten Punkte sind somit in den betreffenden Unternehmen kontrollierbar, revisionsfähig und nach den Grundsätzen ordnungsmäßiger Projektabwicklung nachvollziehbar.



Zufriedenheit mit ISi-Beratung



Überprüfung der Einhaltung der Maßnahmen

Die (fortdauernde) Eignung der Konzepte / Richtlinien wird überprüft mithilfe von (Mehrfachnennungen möglich)	
Basis der Prozentuierung:	258
(erneuten) Schwachstellenanalysen	44 %
(erneuten) Risikoanalysen	40 %
Übungen (Notfall, Wiederanlauf)	31 %
Penetrationsversuchen	27 %
Simulationen oder Szenarien	12 %
Sonstiges	6 %
Es erfolgt keine Überprüfung	16 %

Welche Probleme behindern Sie am meisten bei der Verbesserung der ISi? (Mehrfachnennungen möglich)	
Basis der Prozentuierung:	260
Es fehlt an Bewusstsein bei den Mitarbeitern	65 %
Es fehlt an Bewusstsein beim mittleren Management	61 %
Es fehlt an Bewusstsein und Unterstützung im Top-Management	50 %
Es fehlt an Geld	46 %
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	38 %
Es fehlen verfügbare und kompetente Mitarbeiter	37 %
Die Kontrolle auf Einhaltung ist unzureichend	34 %
Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	34 %
Anwendungen sind nicht für ISI-Maßnahmen vorbereitet	22 %
Es fehlen realisierbare (Teil-)Konzepte	21 %
Die vorhandenen Konzepte werden nicht umgesetzt	20 %
Es fehlen geeignete Methoden und Werkzeuge	18 %
Es fehlen geeignete Produkte	12 %
Es fehlt an praxisorientierten Sicherheitsberatern	10 %
Sonstiges	6 %
Keine	4 %

Dies bestätigt sich auch darin, dass lediglich ein Viertel der Teilnehmer die *Einhaltung* der vorgesehenen Maßnahmen nicht prüft, wohingegen bei denjenigen, die Kontrollen durchführen, die Revision eine dominierende Position einnimmt.

Sogar 84 Prozent der Teilnehmer prüfen die *Eignung* der Konzepte, vor allem durch erneute Schwachstellen- und Risikoanalysen sowie Notfall- und Wiederanlaufübungen. Das ist auch dringend geboten: Denn nahezu 90 Prozent aller Überprüfungen haben Schwachstellen aufgedeckt, deren Beseitigung bei zwei Drittel der befragten Unternehmen noch andauert. Lediglich bei einem Prozent wurden anschließend keine Aktivitäten ergriffen. Die Überprüfungen erstrecken sich bei rund 60 Prozent nur auf einzelne Systeme, bei immerhin 33 Prozent auf alle geschäftskritischen Systeme.

Ein EDV-Notfall-/Wiederanlaufkonzept mit schriftlicher Fixierung und Validierung besitzen allerdings nur 26 Prozent der Unternehmen. Zwar geben weitere zirka 60 Prozent an, ein solches Konzept zu haben, dieses sei aber entweder nicht schriftlich fixiert oder nicht validiert und freigegeben worden. An der Sinnhaftigkeit solcher Verfahrensweisen dürften Zweifel angebracht sein. Die Hochverfügbarkeitsanforderungen von E-Business-Systemen sind nur bei einem Bruchteil der untersuchten Unternehmen in den Konzepten berücksichtigt.

Bewertung der Verbesserungssituation

Der Sinn von Schwachstellenkonzeptionen und Sicherheitsmaßnahmen kann nur in einer Verbesserung der Sicherheitssituation liegen. Bei der Frage nach Hindernissen für eine Verbesserung der IT-Sicherheit steht fehlendes Problembewusstsein mit weitem Abstand an der Spitze: So fehlte es nach Aussage der Befragten in zwei Drittel aller Fälle am richtigen Bewusstsein der Mitarbeiter, dicht gefolgt von dem des mittleren Managements und immerhin noch bei 50 Prozent des Top-Managements. 46 Prozent der Befragten nannten fehlendes Geld als wesentliches Hindernis für die Beseitigung von Sicherheitsmängeln. Die Auswertung der Mehrfachnennungen zeigt, dass im Durchschnitt 4,7 Hindernisse bestehen, in den Unternehmen und Behörden also meist ein ganzer Kanon von Problemen existiert, die eine Verbesserung der Informationssicherheit (ISi) erschweren.

Diese Problematik zeigt sich auch darin, dass fast 70 Prozent der Befragten angeben,

Sicherheitsaspekte seien bei der Beschaffung von EDV-Systemen eher zweitrangig oder unbedeutend. Zwei Drittel der befragten Unternehmen verzichten auf eine Verifikation der Erfüllung von Sicherheitsanforderungen vor der Inbetriebnahme von Systemen.

Risikobewertung

Das Thema Risikobewertung ist seit den grundlegenden Arbeiten des Bundesamts für Sicherheit in der Informationstechnik (BSI) aus der Sicherheitsdiskussion nicht mehr wegzudenken. Erfreulicherweise führen 21 Prozent der befragten Unternehmen eine Risiko- und Schutzbedarfsbewertung für *alle* Anwendungen und Systeme durch, immerhin 49 Prozent zumindest für einzelne Systeme. 30 Prozent der Teilnehmer gaben an, dass bei ihnen keine Risikobewertung vorgenommen wird. Hierbei wird die Klassifizierung durch die Beurteilung des Imageverlusts dominiert, gefolgt von Verstößen gegen Gesetze, Vorschriften und Verträge. Die Gruppe der direkten und indirekten finanziellen Schäden landet hingegen nur im Mittelfeld.

Gesetzliches Umfeld

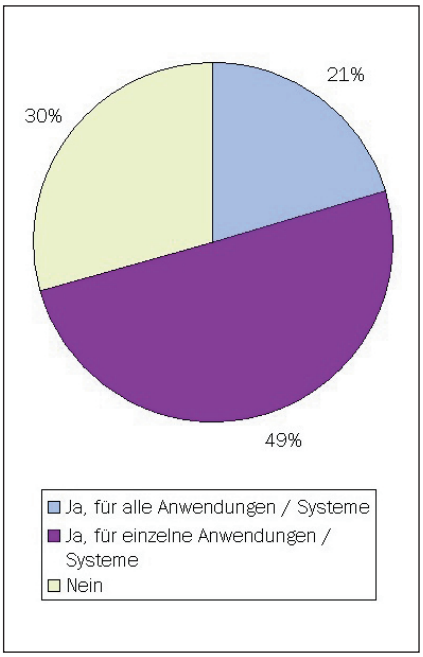
Angesichts der hohen Bedeutung, die Gesetzen bei der Risikobewertung eingeräumt wird, nehmen die Teilnehmer der Studie Probleme, die aus Gesetzen und Regelungen für die Unternehmen hervorgehen, häufig in einem zu geringen Maße wahr. Die Antworten zur Umsetzung der Gesetze mussten allerdings mit einer gewissen Vorsicht interpretiert werden, da sie teilweise inkonsistent zu den Relevanz- und Bekanntheits-Angaben wirken. Das bekannteste Gesetz ist eindeutig das Bundesdatenschutzgesetz (BDSG): 74 Prozent der Befragten gaben zudem an, dass das BDSG für sie auch relevant sei – aufgrund der Befragtenstruktur müsste man jedoch eine noch höhere Durchdringung erwarten. In immerhin knapp zwei Dritteln der befragten Unternehmen wird das BDSG umfassend umgesetzt.

Schlechtere Ergebnisse zeigten sich für die Telekommunikations- und Teledienste-Gesetze, sowohl beim Bekanntheitsgrad als auch in der Umsetzung: Jeweils rund 25 Prozent sind die Regelungen von TKG, TDG sowie der zugehörigen Datenschutzbestimmungen gänzlich *unbekannt.* Von den Teilnehmern, die Angaben zur Umsetzung dieser Bestimmungen gemacht haben, bezeichneten nur ein Viertel diese als umfassend. Angesichts der Bedeutung gerade der Teledienstegesetze für das E-Business sowie die Protokollierung auf Firewalls und Webservern ist das eine ernüchternde Quote.

Als ähnlich unbekannt erweist sich bei den Befragten das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), das Unternehmen unter anderem zur Einrichtung von Risikomanagementsystemen verpflichtet. Die Formulierung des KonTraG wendet sich zwar unmittelbar nur an den Vorstand börsennotierter Gesellschaften, die Gesetzesbegründung legt aber nach Meinung vieler Experten den Schluss nahe, dass sich ähnliche Verpflichtungen auch für andere Unternehmensformen aus den Sorgfaltspflichten der Geschäftsführer ergeben.

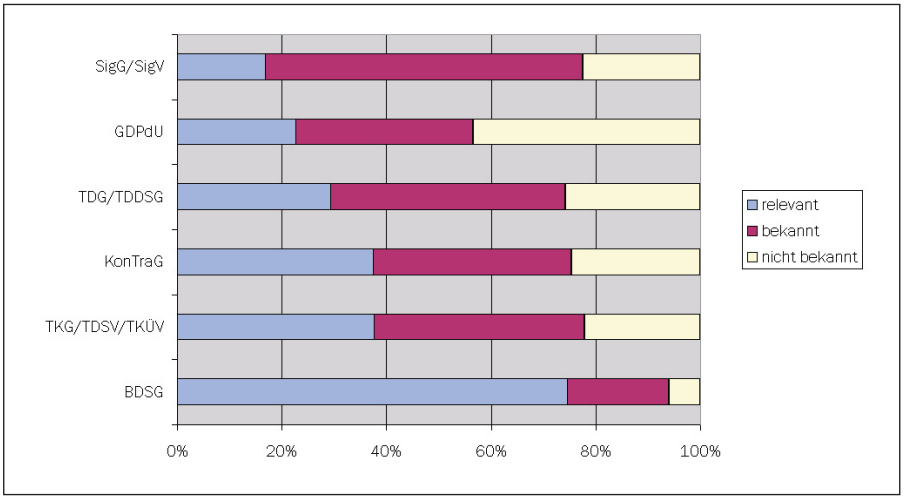
Tools und Vorgehensweisen

Die für die Beurteilung der IT-Sicherheit eingesetzten methodischen Vorgehensweisen und Software-Tools werden dominiert von checklistengestützten Schwachstellenanalysen, gefolgt von Verfahren nach dem IT-



Risikoklassifizierung

Wie wichtig sind die folgenden Kriterien für die Klassifizierung von Anwendungen / Systemen in Ihrem Haus?	sehr wichtig (2)	wichtig (1)	unwichtig (0)	Bedeutungsfaktor
Imageverlust	60 %	31 %	9 %	1,51
Verstöße gegen Gesetze / Vorschriften / Verträge	54 %	39 %	7 %	1,47
direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	52 %	32 %	16 %	1,36
Verzögerung von Arbeitsabläufen	44 %	46 %	9 %	1,35
Schaden bei Dritten / Haftungsansprüche	30 %	51 %	19 %	1,11
indirekte finanzielle Verluste	28 %	41 %	31 %	0,98
direkter finanzieller Schaden an Hardware u. ä.	27 %	44 %	29 %	0,97
Verstöße gegen interne Regelungen	13 %	59 %	28 %	0,85



Relevanz und Bekanntheit der Gesetze

Vielen Dank für freundliche Unterstützung

Die folgenden Unternehmen fördern die Durchführung unserer aktuellen Sicherheitsstudie:

Design Institut GmbH

DR. VOSSBEIN GmbH & Co KG

Für zusätzliche Anregungen und Hinweise bedanken wir uns beim Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie bei Prof. Dr. Alfred Büllesbach – DaimlerChrysler AG, Dr. Gerhard Weck – INFODAS Gesellschaft für Systementwicklung und Informationsverarbeitung mbH, Hans-Joachim Gaebert Unternehmensberatung, Dr. Louis Marinos – MNEMON sowie bei der UIMC Dr. Voßbein GmbH & Co KG, der auch die wissenschaftliche Beratung und Auswertung dieser Studie obliegt.

Nicht zuletzt gilt unser Dank den Verbänden und Anwendervereinigungen, die den Fragebogen der Studie ihren Mitgliedern zugänglich machen.

Im Rahmen von Prüfungen werden unter ISi-Aspekten geprüft:	z. B. durch interne Revision, Wirtschaftsprüfer
Basis der Prozentuierung:	254
Konzeption und Zielsetzung	41 %
Aufbauorganisation	39 %
Ablauforganisation (z. B. für einzelne Vorgänge, Verfahren)	56 %
Software (Korrektheit, Fehlerfreiheit usw.)	41 %
Software-Entwicklung (inkl. Test- und Freigabeverfahren)	42 %
Software-Einsatz	53 %
Übereinstimmung der System-Konfiguration mit Vorgaben	35 %
Datenklassifizierung und Zugriffsrechte	57 %
Change Management (z. B. Änderungshistorie)	40 %
Virenschutz	38 %
Sonstiges	7 %
nichts Derartiges	22 %

Grundschutzhandbuch des BSI. Die „Verfolgergruppe" bilden selbst und von Beratern entwickelte Verfahren, Softwareanalyse-Tools sowie das IT-Sicherheitshandbuch des BSI.

An der Spitze der *Prüfungsobjekte* stehen Datenklassifizierung und Zugriffsrechte gefolgt von der Ablauforganisation. Eine zweite eng beieinander liegende Gruppe bilden softwareorientierte Prüfungen: Softwareeinsatz, -entwicklung und der -funktionalität. Auch Konzeptionen und Zielsetzungen werden noch von über 40 Prozent einer ISi-orientierten Prüfung unterzogen.

Maßnahmen

Die Erfassung der realisierten, geplanten und nicht vorgesehenen Maßnahmen zur Erhöhung der IT-Sicherheit erfolgte in einer komplexen Tabelle, wobei einige Maßnahmen nochmals in Untergruppen genauer behandelt wurden. Bei der Auswertung wurde diese Tabelle zur besseren Übersicht zusätzlich in sinnvolle Einzeltabellen zerlegt, zumal die

Gesamtansicht der Maßnahmen, die realisiert wurden			
	Server	Clients	mobile Endgeräte (Notebooks, PDAs)
	realisiert	realisiert	realisiert
Physische Sicherheit	99 %	85 %	66 %
Authentisierung	98 %	97 %	95 %
Virenschutzmechanismen	98 %	97 %	88 %
Firewalls	98 %	58 %	48 %
Unterbrechungsfreie Stromversorgung	97 %	59 %	29 %
Klimatisierung	94 %	40 %	27 %
Proxy-Server	91 %	67 %	57 %
Protokollierung unberechtigter Zugriffe	87 %	72 %	71 %
Reserve-Netzzugang zur Ausfallüberbrückung	79 %	68 %	56 %
Rückrufautomatik bei Modemzugriff	77 %	48 %	51 %
physikalisches Löschen von Datenträgern	76 %	64 %	56 %
Verschlüsselung	70 %	67 %	67 %
Benutzerverzeichnis mit Security-Policy	69 %	61 %	59 %
Content Inspection/Filtering (Adress-/Inhaltsfilter)	66 %	32 %	31 %
Intrusion Detection System	43 %	12 %	5 %
Public Key Infrastructure (PKI)	20 %	23 %	18 %

Bezugsgrundlagen der Prozentuierung durch unterschiedliche Stellungnahmen oder fehlende Antworten ständig wechseln. Dabei lag unser besonderes Augenmerk auf den bereits realisierten Maßnahmen. In der Gesamtansicht ist die Differenz zwischen dem Prozentanteil derjenigen Unternehmen, die eine Maßnahme realisiert haben, und der Gesamtheit von 100 Prozent jeweils in denjenigen Unternehmen zu sehen, die die betreffende Maßnahme erst planen oder aber nicht vorgesehen haben. Grundsätzlich haben die Serversysteme den höchsten Realisationsstand im Hinblick auf Sicherheit.

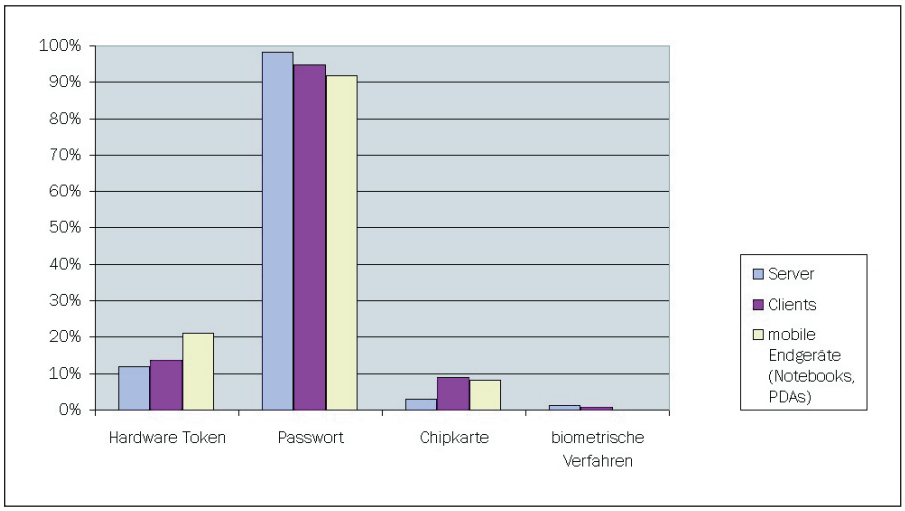
Die Teilübersicht zu den Authentisierungsmaßnahmen zeigt leider immer noch eine starke Dominanz des Passworts. Die biometrischen Verfahren erweisen sich in der derzeitigen Praxis generell als bedeutungslos und liegen auch in der *Planung* regelmäßig nur auf Platz zwei hinter den Chipkarten.

Verschlüsselung

Die Maßnahmen zur Verschlüsselung zeigen eine klare Dominanz bei ausgewählten sensitiven Daten – besonders positiv fällt auf, dass vor allem die Festplatten und Dateien mobiler Endgeräte in hohem Maße chiffriert werden. Bei der konkreten Frage, ob man E-Mail verschlüssele, sofern der Kommunikationspartner über einen Kryptoschlüssel verfügt, antworteten 44 Prozent der Befragten, dies für sensitive Nachrichten zu tun, 13 Prozent bei allen externen E-Mails. Vier Prozent gaben an, jede Nachricht, die verschlüsselt werden kann, zu chiffrieren. An der Spitze der verwendeten Standards steht eindeutig PGP, mit nahezu dem doppelten Wert wie S/MIME. Im Vergleich zu den eingesetzten Verschlüsselungsverfahren ist die Verwendung digitaler Signaturen noch außerordentlich gering verbreitet.

Digitale Signatur

Nur rund ein Viertel der befragten Unternehmen nutzt digitale Signaturen beispielsweise im Rahmen der B2B-Kommunikation. Auf die Frage nach der verwendeten Infrastruktur haben dementsprechend deutlich weniger Teilnehmer geantwortet, sodass sich die Prozentangaben der Tabelle von Seite 12 nur auf eine recht kleine Stichprobe beziehen. Selbst dort zeigt sich – abgesehen von reinen Softwarelösungen – eine geringe Marktdurchdringung mit einem durchgängig hohen Antwortwert der Möglichkeit „nicht vorgesehen". Auf einem abgeschlagenen zweiten Platz in Sachen Realisierung liegen Chipkarten. In Sachen gesetzeskonformer Signaturen haben die fortgeschrittenen elektronischen Signaturen noch die besten Aussichten.



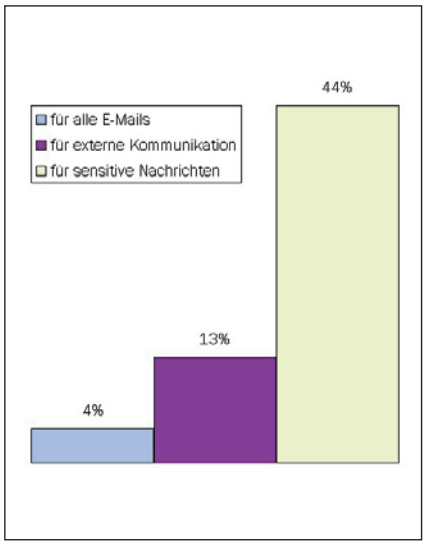
Maßnahmen zur Authentisierung

Detaillierte Übersicht der Maßnahmen zur Verschlüsselung

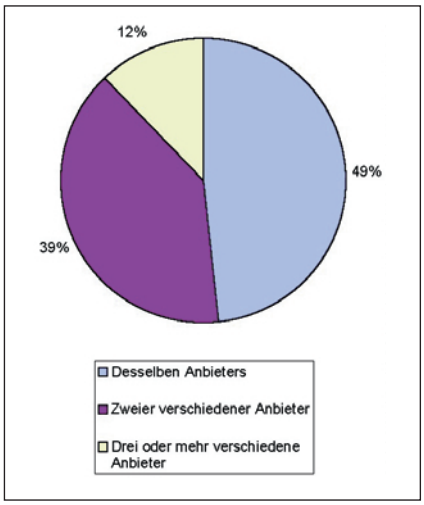
	Server	Clients	mobile Endgeräte (Notebooks, PDAs)
	realisiert	realisiert	realisiert
Verschlüsselung	100 %=147	100 %=132	100 %=134
- sensitive Dateien	54 %	51 %	69 %
- Festplatten (kpl.)	16 %	17 %	46 %
- Archivdatenträger/Backups	24 %	12 %	11 %
- LAN / Intranet-Verbindungen	39 %	40 %	32 %
- WAN / Internet-Verbindungen	59 %	55 %	44 %
- Telefon	10 %	8 %	4 %
- Fax	7 %	8 %	6 %
- E-Mail	46 %	60 %	46 %

Das Thema PKI hat deutlich an Interesse gewonnen: rund 20 Prozent der befragten Unternehmen haben bereits eine PKI realisiert (2000 waren es 7 %), bei 53 Prozent der Unternehmen bestehen Planungen zur Implementierung von PKIs (2000: 31 %).

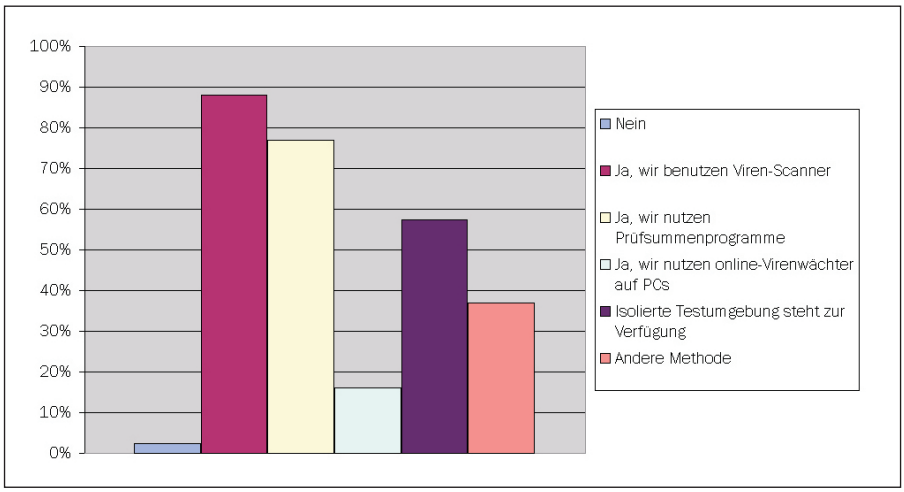
An der Spitze der Einsatzzwecke steht E-Mail-Verschlüsselung, gefolgt vom Einsatz an Tele-Arbeitsplätzen, Dateiverschlüsselung und VPN. Hierbei sind die Einsatzzwecke sowohl bei „realisiert" wie bei „geplant" nahezu identisch. Für 81 Prozent ist das Herkunftsland der PKI-Lösung von Bedeutung. Bei den weiteren Auswahlkriterien steht die Automatisierung der Prozesse zur Erstellung und Verwaltung von Zertifikaten mit 72 Prozent aller Nennungen an der Spitze.



Nutzung der E-Mailverschlüsselung, sofern der Kommunikationspartner über einen Kryptoschlüssel verfügt



Einsatz von Anti-Viren-Software verschiedener Hersteller auf Servern/Gateways beziehungsweise PC-Systemen



Vorsorge gegen Malware

Malware-Schutz

Virenschutzmechanismen wurden wenig überraschend für nahezu alle Clients und Server als realisiert gemeldet – lediglich bei mobilen Endgeräten ist mit 88 Prozent eine vergleichsweise geringe Durchdringung vorhanden. Bei der Detailfrage nach den konkreten Vorsorgemechanismen führen die Virenscanner klar mit 88 Prozent, wobei immerhin 51 Prozent auf Servern/Gateways und PCs aus Sicherheitsgründen Software von zwei oder mehr verschiedenen Anbietern einsetzen. 77 Prozent der befragten Unternehmen nutzen zudem Prüfsummenprogramme. Über 75 Prozent der Befragten sind der Auffassung, dass die getroffenen Maßnahmen auch eine hinreichende Wirksamkeit gegen Makroviren bei Office-Dokumenten und gegen online-übertragene Schadsoftware haben (zum Beispiel in E-Mail-Anhängen oder Downloads) – je 5 Prozent halten den Schutz für nicht ausreichend, der Rest ist sich nicht sicher.

Angriffserkennung

Intrusion Detection Systems (IDS) sind nach wie vor relativ selten. Um die 40 Prozent der befragten Unternehmen hat IDS im Einsatz, in etwa die gleiche Zahl *plant* den Einsatz auf Serversystemen. Bei der Auswertung von Log-Dateien zeigte sich, dass Firewall- und Betriebssystem-Protokolle am sorgfältigsten durchgesehen werden, zu einem beträchtlichen Teil mehr als einmal pro Woche. Die Log-Files von Netzwerkkomponenten (Router, Switches usw.) sowie Web- und E-Commerce-Applikationen prüfen die Befragten hingegen zu einem größeren Anteil anlassbezogen oder gar nicht.

Nahezu zwei Drittel der Unternehmen haben in den letzten zwölf Monaten einen Penetrationstest in Auftrag gegeben, wobei 78 Prozent dies in Bezug auf die Internet-Infrastruktur und 50 Prozent in Bezug auf kritische Systeme von innen durchführten.

Security-Management

Auch bei der Frage nach der Bedeutung für das unternehmensweite Security-Management zeigten sich IDS als weniger wichtig und landeten nur auf Rang sechs. An der Spitze steht eindeutig die zentrale Überwachung der eingesetzten Security-Systeme; nur vier Teilnehmer sahen dies als unwichtig an. 92 Prozent erachten eine plattformübergreifende Benutzerverwaltung für sehr wichtig oder wichtig. Für tendenziell unwichtig wurde Kontrolle und Überwachung von Internet-Missbrauch gehalten: Hier handelt es sich

Welche Infrastruktur nutzen Sie für digitale/elektronische Signaturen?

	B2B-Server			B2C-Server			Client/PC			mobile Endgeräte		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
nur Software	58 %	7 %	34 %	53 %	12 %	35 %	64 %	15 %	21 %	64 %	3 %	33 %
Hardwaremodule	8 %	15 %	77 %	9 %	16 %	76 %	0 %	10 %	90 %	9 %	15 %	76 %
Hardware-Token	15 %	15 %	71 %	9 %	15 %	77 %	24 %	8 %	67 %	9 %	17 %	74 %
Chipkarten	25 %	11 %	64 %	22 %	12 %	66 %	37 %	19 %	44 %	9 %	32 %	60 %
„Klasse-2"-Chipkartenterminal (sichere PIN-Eingabe)	12 %	8 %	80 %	9 %	4 %	87 %	13 %	4 %	83 %	0 %	4 %	96 %
„Klasse-3"-Chipkartenterminal (mit eigenem Display)	11 %	0 %	89 %	7 %	2 %	91 %	7 %	0 %	93 %	0 %	0 %	100 %
lt. SigG	0 %	14 %	86 %	8 %	11 %	82 %	8 %	10 %	83 %	0 %	5 %	95 %
- fortgeschrittene Signatur	15 %	24 %	61 %	10 %	26 %	64 %	6 %	23 %	70 %	0 %	15 %	85 %
- qualifizierte Signatur	7 %	14 %	80 %	0 %	23 %	78 %	13 %	20 %	67 %	4 %	21 %	74 %
- qualifizierte Signatur mit Anbieterakkreditierung	15 %	4 %	80 %	14 %	12 %	74 %	10 %	10 %	80 %	4 %	4 %	91 %

immerhin um 24 Prozent, die diesem Merkmal eine niedrige Priorität beimessen.

Physische Sicherheit

Maßnahmen zur physischen Sicherheit sind vorrangig für Server implementiert, hierbei dominiert die Zutrittskontrolle. Nicht unerwartet sind auch Einbruchs- und Brandmeldesysteme sowie Löschanlagen recht verbreitet. Positiv ist auch ein relativ hoher Wert von Maßnahmen gegen Hardwarediebstahl bei den mobilen Endgeräten (57 %) zu werten, wobei hier eine genauere Analyse der eingesetzten Maßnahmen von Interesse sein könnte. Generell geringe Beachtung finden Schutzmaßnahmen gegen kompromittierende Abstrahlung, eine in der Vergangenheit häufig überschätzte Gefahr.

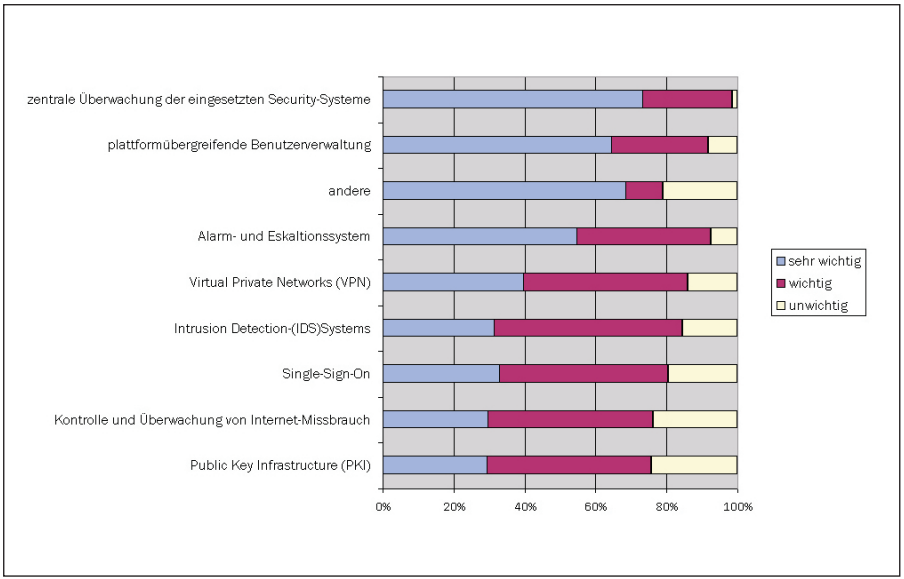
Mit 89 Prozent der Teilnehmer haben erwartungsgemäß viele die Stromversorgung ihrer EDV mit Überspannungsschutz ausgerüstet; Daten-, Telefon- und Modemleitungen sind bei 43 Prozent der Befragten geschützt. Wer keinen Überspanunngsschutz realisiert hat, hält vor allem das entsprechende Risiko für wenig gravierend. Eine generelle Bewertung physischer Risiken im Sicherheitskonzept findet übrigens nur bei 30 Prozent der Befragten statt.

Katastrophenvorsorge

Ein wesentliches Merkmal zur Sicherstellung der Business Continuity ist das Vorhalten wesentlicher Systemkomponenten an verschiedenen Orten. Hier zeigt sich, dass die Kooperation mit einem externen Anbieter bei denjenigen, die überhaupt eine Auslagerung praktizieren, an letzter Stelle steht. Auf Rang eins befindet sich die Auslagerung in einem anderen Gebäude, gefolgt von der in einem anderen Brandabschnitt.

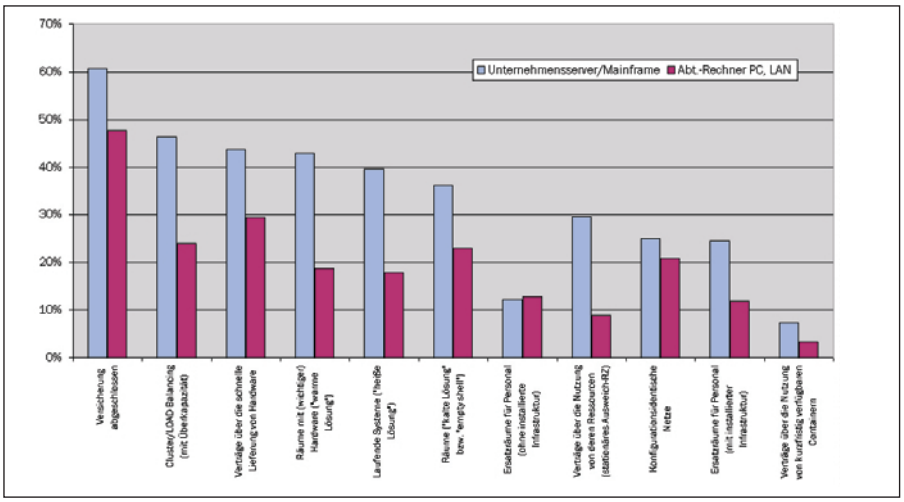
Bei der Bereitstellung für längere Ausfälle dominieren Cluster und Load Balancing mit Überkapazitäten sowie die „warme Lösung", bei der komplette Räume mit wichtiger Hardware vorgehalten werden. In den letzten Jahren haben zudem auch Konfigurationen mit identischen Netzen größere Bedeutung erlangt. Von denjenigen Unternehmen, die Verträge mit externen Dienstleistern/Partnern abgeschlossen haben, stehen Verträge über die schnelle Lieferung von Hardware an der Spitze, dicht gefolgt über Verträge zur Nutzung eines stationären Ausweichrechenzentrums. Die Containerlösungen sind der Anzahl der Nennungen nach weit entfernt von den anderen Lösungen. Die hohe Zahl der Befragten, die angeben, auf diesem Gebiet

Setzen Sie Intrusion Detection Systeme ein?				
Basis der Prozentuierung:	82 Institutionen, die Intrusion Detection Systeme einsetzen			
	netzbasiert	hostbasiert	zentrale Auswertung der Logfiles	unveränderliche Speicherung der Logfiles
Firewall zum Internet	55 %	33 %	54 %	23 %
DMZ	43 %	23 %	34 %	11 %
Interne Firewalls	11 %	5 %	15 %	2 %
Intranet/LAN	23 %	12 %	11 %	7 %



Bewertung der Komponenten des Security-Managements

Detaillierte Übersicht der Maßnahmen zur physischen Sicherheit			
	Server	Clients	mobile Endgeräte (Notebooks, PDAs)
	realisiert	realisiert	realisiert
Physische Sicherheit	100 %=253	100 %=144	100 %=90
- Zutrittskontrolle	86 %	66 %	46 %
- Bewachung	46 %	35 %	21 %
- Video-Überwachung	28 %	10 %	1 %
- Einbruchsmeldesysteme	70 %	48 %	27 %
- Schutz von Glasflächen gegen Durchbruch / Durchwurf	56 %	26 %	8 %
- Sicherheitstüren	76 %	32 %	20 %
- Brandmeldesysteme	83 %	60 %	31 %
- Löschanlagen	50 %	22 %	8 %
- andere Meldesysteme (z. B. Gas, Staub, Wasser)	38 %	8 %	4 %
- Datensicherungsschränke/-räume	80 %	32 %	26 %
- Schutz gegen kompromittierende Abstrahlung	13 %	3 %	0 %
- Maßnahmen gegen Hardwarediebstahl	42 %	35 %	57 %



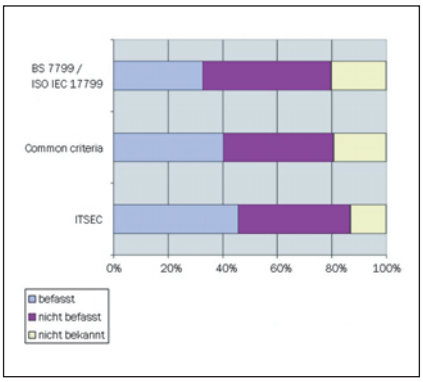
Bereitstellung für längere Ausfälle

eine Versicherung abgeschlossen zu haben, ist innerhalb der Stichprobe der KES/KPMG-Sicherheitsstudie 2002 deutlich höher als im gesamten Markt.

Eine erstaunlich hohe Zahl von Unternehmen (92 Prozent) ist der Auffassung, dass Recovery-Maßnahmen nur über ein strategisches Konzept entschieden werden sollen. Dieses wird dann mit eigenen Kräften unter Nutzung externer Beratung erstellt.

Notfall-Dokumentation

Eine Notfall-Dokumentation existiert in über 50 Prozent aller Unternehmen. Hierbei dominiert das manuelle Handbuch, wobei weiterhin eine beachtliche Zahl der Befragten ein solches in Arbeit oder Planung haben (35 %). Auf diesem Sektor ist seit dem 11. September 2001 generell eine verstärkte Aufmerksamkeit zu vermerken. Die Notfall-Dokumentation ist grundsätzlich allgemein ausgelegt (96 Prozent) und enthält in den meisten Fällen vor allem Aktionspläne für den K-Fall sowie für Störungen im Tagesbetrieb. Typisch für die befragte Gruppe ist, dass die Dokumentation



Bekanntheit internationaler Kriterien zur Informationssicherheit

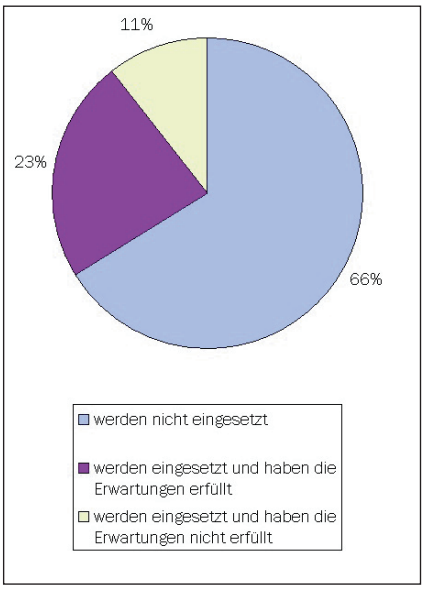
nach Auffassung von 87 Prozent der Teilnehmer die Anforderungen nach dem KonTraG erfüllt. Weniger als 20 Prozent gaben an, eine Notfall-Dokumentation weder zu besitzen noch zu planen.

Die Aktualisierung der Dokumentation erfolgt bei den meisten nur sporadisch (47 %). Fast achtzig Prozent der Antwortenden sind der Meinung, dass die Aktualität der gesamten Dokumentation durch den Einsatz im Tagesbetrieb erreichbar ist. Die gesamte Bedeutung des Notfallproblems kommt auch darin zum Ausdruck, dass 62 Prozent für Erstellung und Koordination der Notfallplanung eine verantwortliche Person ernannt haben, und dass die Ergebnisse von Notfallübungen vom überwiegenden Teil in die Dokumentation einfließen.

Zertifizierung

Das Wirken des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf dem Sektor der IT-Sicherheit ist den meisten Befragten bekannt. Das IT-Sicherheitshandbuch sowie das Grundschutzhandbuch haben einen sehr hohen Bekanntheitsgrad erlangt, während verschiedene Dienstleistungen des BSI wie Akkreditierung und Evaluierung nur noch rund einem Drittel der Unternehmen bekannt sind.

Dass über 60 Prozent der Befragten Zertifizierungsdienste des BSI kennen, dürfte in erster Linie auf die Tätigkeiten im Bereich der Produkt-Zertifizierung zurückzuführen sein. Die IT-Sicherheit wird seit Jahren stark durch internationale Kriterien bestimmt. Der Bekanntheitsgrad der ITSEC, der Common Criteria (CC) und der BS 7799/ISO-IEC 17799 ist durchaus nicht schlecht zu nennen,



Zertifizierte Sicherheitsprodukte

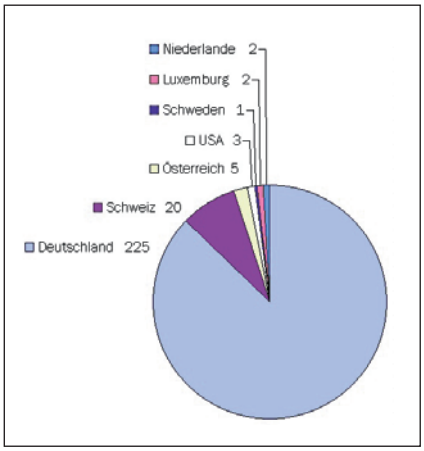
obwohl sich eine hohe Zahl der Befragten damit bisher noch nicht ernsthaft befasst hat.

34 Prozent der Befragten setzen zertifizierte Sicherheitsprodukte ein; 23 Prozent geben an, in Zukunft zertifizierte Produkte bevorzugt einsetzen zu wollen. Die Erwartungen an den Nutzen und die Zuverlässigkeit haben sich bei den jetzigen Anwendern zertifizierter Produkte in hohem Maße erfüllt (69 %). Darüber hinaus rechtfertigt ein zertifiziertes Produkt nach ihrer Meinung auch einen höheren Preis.

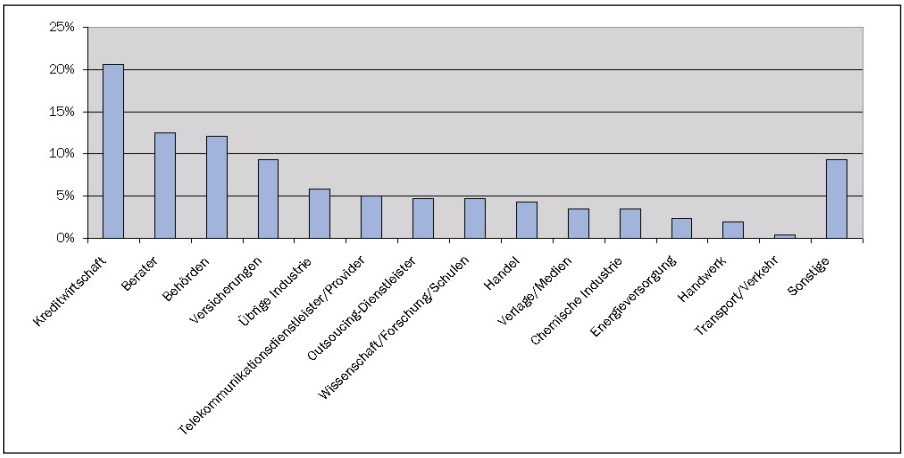
Teilnehmer

Basierend auf den statistischen Angaben, die abschließend erfragt wurden, ist festzustellen, dass in erster Linie große mittelständische Unternehmen sowie Großunternehmen und -institutionen an der Untersuchung teilgenommen haben. Der Maximalwert bei den Beschäftigten liegt bei mehreren Hunderttausend, wobei die durchschnittliche Anzahl der Mitarbeiter über 8000 beträgt. Die durchschnittliche Anzahl von Beschäftigten in der Informationsverarbeitung ist mit über 400 ebenfalls als sehr hoch anzusehen und wird teilweise durch eine Anzahl sehr großer Institutionen beeinflusst. Bei Unternehmen, die Mitarbeiter ausschließlich für Aufgaben der IT-Sicherheit beschäftigen, liegt auch dieser Wert mit einem Durchschnitt von 16 über einem gesamtwirtschaftlich anzunehmenden Mittel.

Die IT-Ausstattung belegt die These der „Großen". Durchschnittlich sind bei den Teilnehmern der Studie über 4000 Clients/



(Haupt-)Sitz der teilnehmenden Institutionen



Branchenzuordnung der Teilnehmer an der KES/KPMG-Sicherheitsstudie

PCs vorhanden, bei einem Maximalwert von 120 000. Die größte Institution verfügt über 200 Mainframes, was stolzen 23 Prozent aller 883 Großrechner entspricht, die im Rahmen dieser Analyse genannt werden.

Bemerkenswert ist weiterhin, dass bereits über zehn Prozent der genannten Endgeräte auf mobile Systeme wie Notebooks oder PDAs entfallen. Ein Wert von fast 150 000 solcher Geräte belegt zum einen das Vordringen der mobilen Technik, zeigt aber auch ein erhöhtes Risikopotenzial auf, das deren Nutzung begründet – besonders angesichts der aufgezeigten schlechten Einschätzung der Informationssicherheit für mobile Endgeräte.

Branchen

Über ein Fünftel der Befragten sind der Kreditwirtschaft zuzurechnen, gut ein Zehntel bezeichnen sich als Berater; den gleichen Anteil haben Behörden, denen man noch die fast fünf Prozent der Institutionen aus dem Bereich Wissenschaft/Forschung/Schulen zuordnen kann, um den öffentlichen Sektor zusammenzufassen. Generell sind gerade diejenigen Institutionen und Unternehmen vertreten, bei denen aufgrund ihrer Tätigkeit von einem erhöhten Sicherheitsbewusstsein auszugehen ist. Die teilweise immer noch erschreckenden Ergebnisse entstammen somit einer eher positiv verzerrten Stichprobe, bei der man eine erhöhte Sensibilisierung in Sachen Sicherheit vermuten kann. Die IT-Security dürfte sich im Allgemeinen noch deutlich schlechter darstellen.

Budgets

149 Teilnehmer haben Angaben zum Budget für die Informationsverarbeitung – inklusive der Personalkosten – gemacht, ihre Unternehmen veranschlagen hierfür insgesamt 132 781 000 Euro. 125 Institutionen gaben darüber hinaus Informationen über das Budget für Informationssicherheitsmaßnahmen an, die bei 7 682 927 Euro liegen (inkl. Personal). Dabei ist festzustellen, dass die Antworten insbesondere bei den Angaben zum IT-Sicherheitsbudget zu 95 Prozent nur geschätzt werden konnten und nur bei fünf Prozent der Angaben hierfür eine Grundlage im Rahmen der Budgetierung oder des Rechnungswesens benutzt wurde.

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

Basis der Prozentuierung:	147
Konkurs / Pleite	7 %
Unternehmensende	2 %
Bankrott	7 %
nicht bezifferbar	6 %
unter 100 000 €	5 %
100 000–250 000 €	6 %
250 000–1 000 000 €	21 %
über 1 000 000 €	46 %

Datenwert

Den immensen Wert der vorgehaltenen Daten verdeutlicht die Schlussfrage nach den Auswirkungen der Vernichtung aller elektronisch gespeicherten Daten: Rund 16 Prozent der Befragten waren der Auffassung, dass ein solcher Verlust gleichbedeutend mit dem finanziellen Ende des Unternehmens sei (Konkurs, Unternehmensende, Bankrott). 46 Prozent schätzten einen Schaden von über einer Million Euro, weitere 21 Prozent sahen mehr als 250 000 Euro Schaden bei totalem Datenverlust. Die konkret geschätzten Zahlen weisen auf beachtliche Schadenshöhen hin, die sich aber in einem wirtschaftlich plausiblen Rahmen halten. Es liegt nahe zu vermuten, dass die Prognosen zum Unternehmensende entweder Extrembeispiele sind oder aber die Antwortenden eine etwas pauschale Wertung vorgenommen haben. ◆

Prof. Dr. Reinhard Voßbein ist Geschäftsführer der UIMCert GmbH. Dr. Jörn Voßbein ist Geschäftsführer der UIMC Dr. Vossbein GmbH & Co. KG (www.uimc.de).

Impressum

Sonderdruck aus KES 2002/3+4 für KPMG Frankfurt Information Risk Management, Emil-von-Behring-Str. 2, 60439 Frankfurt/M, Tel.: 069 9587-2566, Fax: 069 9587-2559, E-Mail: bradchapman@kpmg.com

Verantwortlich für den Inhalt: Norbert Luckhardt

Satz: Black Art Werbestudio, 55218 Ingelheim

Titelbild: Siemens (Montage KES)

Druck: G. Schmidt GmbH, Offsetdruckerei, Haagweg 44, 65462 Ginsheim-Gustavsburg

Printed in Germany.

Die Zeitschrift KES ist ein führendes Fachmagazin im Bereich der IT-Sicherheit. Sie ist offizielles Organ des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Erscheinungsweise: 6 Ausgaben pro Jahr. Jahresabo Deutschland: € 122,00. Andere Länder: € 137,00

Probeheftanforderung: Fax 06725/5994, E-Mail: vertrieb@secumedia.de