Die Zeitschrift für Informations-Sicherheit

special

Auszüge aus <kes> 2004#4/5

Sonderdruck für Microsoft®

Von Geldmangel bis Mehrwert

Lagebericht zur Informations-Sicherheit

SecuMedia

Sicherheit in einer vernetzten Welt: Die Strategie von Microsoft

Ohne Basisdaten zur IT-Sicherheit aus unterschiedlichen Untenehmen und Behörden gibt es keine sinnvolle Strategie. Microsoft freut sich, erstmals Hauptsponsor der kes-Sicherheitsstudie zu sein und wünscht Ihnen eine aufschlussreiche Lektüre.

Sicherheit ist in der heutigen vernetzen Welt ständiges Thema und für alle Kunden ein elementares Bedürfnis. Daher hat IT-Sicherheit bei Microsoft allerhöchste Priorität.

Die Vorteile einer vernetzen Welt sind heutzutage nahezu selbstverständlich: Wir kaufen online ein, erledigen unsere Bankgeschäfte online und Firmen verknüpfen ihre Geschäftsprozesse online. Diese Vernetzung, zusammen mit der alles umfassenden Digitalisierung – nicht nur von Text, sondern auch von Sprache, Bildern und Musik – führt dazu, dass wir heute die Arbeit mit Computern aus einem ganz anderen Blickwinkel als noch vor ein paar Jahren betrachten.

Firmen und Konsumenten weltweit zusammenzuführen hat unbeabsichtigt ein Wirtschaftssystem geschaffen, das durch Angriffe von Menschen mit bösartigen oder kriminellen Absichten verwundbar ist. Die Ära des rasanten Booms ist heute vorbei. Wir befinden uns jetzt in einer neuen Ära, in der Sicherheit zur entscheidenden Herausforderung geworden ist, in der Identitäten gestohlen werden können, und in der arglistige Hacker weit mehr Schäden anrichten können als jemals zuvor.

Microsoft wird eine entscheidende Rolle dabei spielen, die negativen Eindrücke der Kunden und die Sicherheit des Internet zu verändern. Unsere Produkte werden weltweit am meisten genutzt und sind auf hohem technischem Niveau, was für böswillige Hacker eine Herausforderung ist, weil sie großen Schaden anrichten können.

Microsofts Bemühungen zielen darauf ab, mehr Vertrauen in die Arbeit mit Computern zu bilden. Dazu haben wir unsere Kernkompetenzen bei technischen Innovationen für IT-Sicherheit basierend auf dem Feedback unserer Kunden auf folgende Probleme konzentriert:

- Verbesserung der Isolierung und des Schutzes von Computern und Netzwerken, um schädlichen Code zu unterbinden (Isolierung) und damit die Systeme insgesamt resistenter gegen Angriffe zu machen (Schutz)

- Bessere Updatemöglichkeiten mit einer Verbesserung der Verfahren, Tools und Verwaltung von Sicherheitsupdates

- Entwicklung von effektiven Authentifizierungs-, Autorisierungs- und Zugriffsverfahren (AAA – Authentication, Authorization, Access Control)

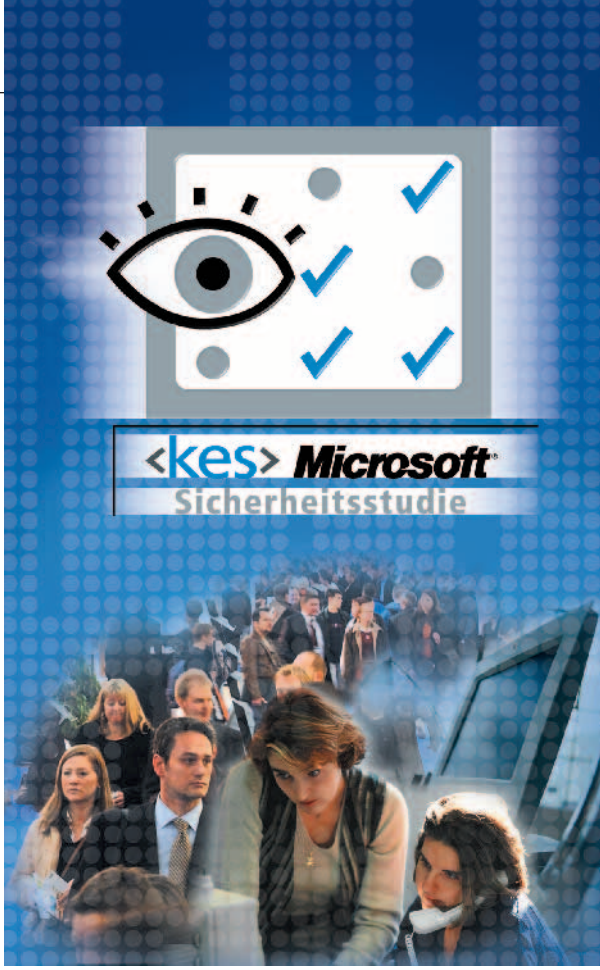
- Weiterhin Verbesserung der Qualität unserer Software durch intensive Code-Analysen und die fortschrittlichsten Software-Testverfahren

Der Mensch ist der wichtigste Faktor zum Erreichen eines hohen Levels für IT-Sicherheit. Deshalb gibt es von Microsoft über die technischen Innovationen hinaus Beratung, Trainings, Tools und Kommunikations-Maßnahmen für unsere Kunden, die zum einem großen Teil kostenlos zur Verfügung stehen.

Um jedes einzelne Glied der „Sicherheitskette" zu festigen und zu ergänzen, arbeiten wir in allen Bereichen mit Sicherheits-Partnern zusammen.

Informieren Sie sich direkt bei der Geschäftskundenbetreuung von Microsoft über spezielle Sicherheits-Dienstleistungen für den Mittelstand und Großunternehmen: Telefon 0180 5229552 (0,12 Euro pro Minute, deutschlandweit)

Lagebericht zur Informations-Sicherheit



Verlässliche Zahlen zur Informations-Sicherheit sind selten. Noch seltener sind konkrete Angaben zu Schäden und Budgets sowie selbstkritische Bestandsaufnahmen zur Sicherheitslage. Auch in diesem Jahr haben hochkarätige Teilnehmer den <kes>-Fragebogen als Checkliste für ihre eigene Sicherheit genutzt und damit gleichzeitig wertvolle Daten geliefert.

Die <kes>/Microsoft-Sicherheitsstudie ist die zehnte <kes>-Studie, die durch die vertrauensvollen und umfassenden Antworten ihrer Teilnehmer sowie die Unterstützung von Sponsoren und Partnern tiefe Einblicke in die Informations-Sicherheit (ISi) des deutschsprachigen Raums ermöglicht – dafür vielmals Dankeschön. In diesem Jahr sind 163 Fragebögen eingegangen. Die wichtigsten Kernpunkte der Auswertung lauten:

_____ Bedeutendster Gefahrenbereich bleibt „Irrtum und Nachlässigkeit eigener Mitarbeiter“ – „unbeabsichtigte Fehler von Externen“ steigen in der Beachtung der Teilnehmer

_____ Größerer Einfluss von technischem Versagen bei Datenunfällen – Unfälle führten bei mehr Teilnehmern zu nennenswerten Beeinträchtigungen als Angriffe

_____ Malware ist die Gefahr mit dem größten Zuwachs – erstmals verzeichnen mehr Teilnehmer mittlere bis größere Beeinträchtigungen durch Malware als durch Irrtum und Nachlässigkeit

_____ Unbefriedigende Sicherheitslage bei Notebooks, PDAs, Heim- und Telearbeitsplätzen sowie Wireless LAN (WLAN)

_____ Bessere Unterstützung durch das Top-Management – Hauptproblem jetzt: fehlende Finanzmittel

Risikosituation

Vermutlich *die* zentrale Frage der Studie steht regelmäßig an erster Position von Fragebogen und Auswertung: die Bedeutung der verschiedenen Gefahrenbereiche zur Risikoklassifizierung. Seit Beginn der <kes>-Studien nennen die Teilnehmer hier allem voran „Irrtum und Nachlässigkeit eigener Mitarbeiter“ – so auch in diesem Jahr. Weiterhin folgen knapp dahinter als Gefahrenbereich mit der zweitgrößten Bedeutung Viren, Würmer und Trojanische Pferde (Malware), mit etwa demselben „Abstand“ wie in der vorausgegangenen Studie von 2002. Beides sind gleichzeitig die Risiken, denen mit jeweils über 80 % die weitaus meisten Befragten mindestens einen von sechs möglichen Prioritätspunkten zugestanden haben – bei den Plätzen drei bis fünf waren das jeweils 40–50 %. Durch die Kumulation von bis zu drei Punkten pro Gefahrenbereich konnten die Teilnehmer zudem Schwerpunkte bekunden (Priorität s. Tab. 1).

Auch sonst blieb die Rangfolge mit einer Ausnahme stabil (Platz 3 und 4 sind zwar vertauscht, liegen

	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,50	2	1,70	2	51%
Malware (Viren, Würmer, Troj. Pferde,...)	2	1,34	1	2,80	1	54%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,60	4	1,14	8	9%
Software-Mängel/-Defekte	4	0,57	5	0,96	3	43%
Hacking (Vandalismus, Probing, Missbrauch,...)	5	0,48	3	1,26	5	9%
Hardware-Mängel/-Defekte	6	0,40	8	0,32	4	38%
unbeabsichtigte Fehler von Externen	7	0,30	9	0,26	7	15%
höhere Gewalt (Feuer, Wasser,...)	8	0,24	11	0,04	9	8%
Manipulation zum Zweck der Bereicherung	9	0,17	7	0,43	10	8%
Mängel der Dokumentation	10	0,15	10	0,20	6	17%
Sabotage (inkl. DoS)	11	0,12	6	0,55	11	8%
Sonstiges	12	0,03	12	0,00	12	3%

Basis: 161 Antworten (Bedeutung), Ø 124 (Prognose), Ø 128 (Schäden)

Tabelle 1: Bedeutung der verschiedenen Gefahrenbereiche

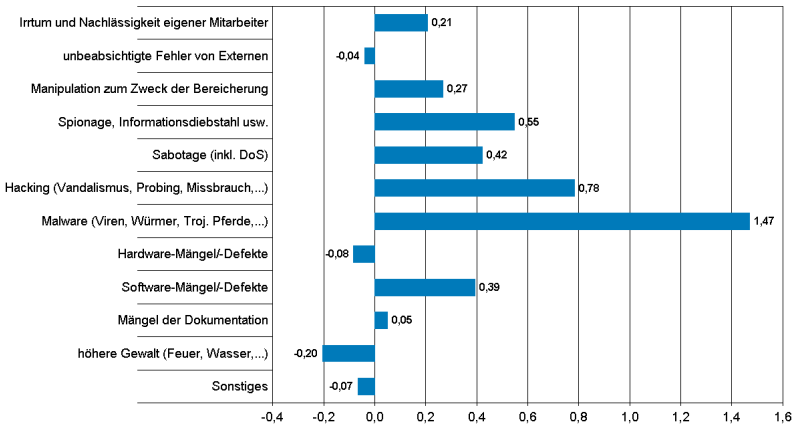


Abbildung 1: Prognostizierte Veränderungen der Gefahrenbereiche

Basis: Ø 124 Antworten

jedoch nahezu gleichauf, sodass hier noch keine Trendwende zu folgern ist). Auffällig ist jedoch der Sprung der „unbeabsichtigten Fehler von Externen" von Rang 10 auf Rang 7. Hier scheint sich die Prognose der vorigen Studie ansatzweise bestätigt zu haben, die eine drastische Bedeutungs-Steigerung dieses Gefahrenbereichs vorhergesagt hatte (prognostiziert war sogar Rang 4). In der aktuellen Einschätzung nicht wiederzufinden sind hingegen die Prognosen sinkender Probleme mit der Hardware (Prognose 2002: fallend von Rang 6 auf Rang 10) sowie steigender Bedeutung von Sabotage (steigend von Rang 11 auf Rang 7) – beide Risiken erzielten jeweils dieselbe Einschätzung wie vor zwei Jahren.

Die diesjährigen Prognosen stimmen großenteils mit den erwarteten Trends von 2002 überein: deutlich mehr Malware-Probleme und eine Zunahme von Hacking und Spionage, weniger Probleme mit Hardware und höherer Gewalt. Neu ist, dass die Teilnehmer eine deutlich höhere Steigerung bei Sabotage und Manipulationen zum Zwecke der Bereicherung erwarten. Treffen diese Erwartungen ein, so würden beide um mehrere Rangstufen klettern – die Sabotage „profitiert" zudem erneut von dem erwarteten Nachgeben anderer Bereiche, sodass sie sogar um fünf Plätze aufsteigen würde (2002 korrespondierte der erwartete Aufstieg um vier Ränge hingegen kaum mit dem damaligen Veränderungswert von +0,08). Ebenfalls neu ist ein leichter erwarteter Rückgang der (gerade erst deutlich gestiegenen) Bewertung unbeabsichtigter Fehler von Externen.

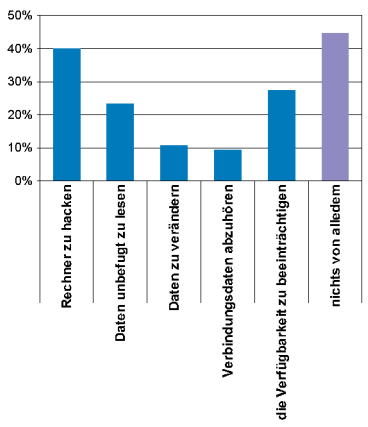


Abbildung 2: Über das Internet wurde bereits versucht ...

Basis: 150 Antworten

Schadensstatistik

Richtet man den Blick auf die Gefahrenbereiche, die in den vergangenen zwei Jahren tatsächlich zu mittleren bis größeren Beeinträchtigungen geführt haben, so zeigen sich drei Auffälligkeiten. Allem voran hat diese „Schadensstatistik" den immer wieder vorhergesagten Anstieg der Malware-Bedeutung auf Rang 1 bereits vorweggenommen: Erstmals haben hier mit 54 % mehr Befragte einen tatsächlichen Schaden angegeben als bezüglich Irrtum und Nachlässigkeit eigener Mitarbeiter (51 %) – 2002 lag diese höchstrangige Bedrohung auch bei den Schadensmeldungen noch fünf Prozentpunkte vor der Malware.

Deutlich abweichend von ihrem Rang in der Bedrohungseinschätzung liegen Spionage (unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage usw.) und Mängel an der (technischen) Dokumentation: Spionage (Rang 3 in der Bedrohung) hat nur bei 9 % der Antwortenden tatsächlich nennenswerte Beeinträchtigungen bewirkt (Rang 8 der Schadensstatistik). Ob hieraus eine Überschätzung des Risikos gefolgert werden darf, ist allerdings fraglich: Einerseits steht gerade bei dieser Gefahr eine enorme Dunkelziffer zu befürchten, zum anderen könnte die erhöhte Aufmerksamkeit auch gerade zu einem Ausbleiben von Schäden geführt haben.

Vermutlich unterschätzt zeigt sich hingegen das Risiko von Dokumentationsmängeln: Während ihm im Bedrohungsindex ein stabiler 10. Rang eingeräumt wird, landet es in der Schadensstatistik auf Rang 6 (mittlere bis größere Beeinträchtigungen bei immerhin 17 % der Antwortenden). Auch hier ist zudem – wie bei Sabotage und betrügerischen Manipulationen – eine hohe Dunkelziffer im Spiel: In all diesen Bereichen konnte jeweils mehr als ein Viertel der Teilnehmer keine klare Aussage zu tatsächlichen Beeinträchtigungen treffen.

Fasst man die verschiedenen Risikogruppen alternativ in die Kategorien (Daten-)Unfälle (ohne höhere Gewalt) und Angriffe zusammen, so zeigt sich, dass die Unfälle weiterhin die größere Bedeutung haben. Allerdings ist der Abstand geschrumpft: 2002 lag das Verhältnis – bezogen auf die Nennungen von mindestens einer wesentlichen Beeinträchtigung („Schaden") in den jeweiligen Kategorien – noch bei 1,78:1 (Unfallopfer:Angriffsopfer), heuer sind es nur noch 1,66:1. Zudem hat bei den kumulierten Unfall-Ursachen technisches Versagen den Menschen als Hauptgrund abgelöst: einerseits durch eine erhöhte Nennung von Beeinträchtigungen

durch Dokumentations-Mängel und zum anderen durch (im Verhältnis zur Stichprobe) weniger Schadensfälle aufgrund von Fehlern und Irrtümern (vgl. Tab. 2).

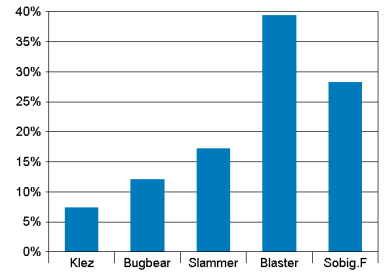
Die These der vergleichsweise geringen Zahl gezielter Attacken belegen auch die Angaben zu Angriffen aus dem Internet und auf Webserver. Etliche Unternehmen blieben weiterhin unbehelligt: 45 % haben noch gar keinen der genannten Angriffe aus dem Internet registriert (vgl. Abb. 2), bei 56 % der Teilnehmer gab es noch keine Angriffe auf den Web-Server (s. Tab. 3). Die Top-Attacken waren Hacking-Versuche (von denen aber auch immer noch 60 % der Teilnehmer bislang komplett verschont blieben) und Denial-of-Service-Angriffe, denen sich etwa jeder Vierte irgendwann einmal ausgesetzt sah. Erstaunlicherweise steigen diese Zahlen nicht, obwohl doch mit den Jahren die „Online-Zeitspanne" und damit die Dauer der Exponiertheit gewachsen sein müssten.

Bei der Frage nach dem größten Schadensereignis der letzten zwei Jahre dominiert wieder die Malware: Von den einhundert Antworten auf diese Freitextfrage entfielen 34 % auf Viren und Würmer, an zweiter Stelle folgten 13 % Ausfälle bei Speichersystemen (Festplattencrashs, RAID-Versagen, SAN-Probleme usw.). Bei 7 % der antwortenden Unternehmen verursachte die Stromversorgung (Ausfall oder Überspannung) den größten Ärger der letzten zwei Jahre, bei 5 % handelte es sich um Server-Ausfälle, bei 4 % um Angriffe. Zu den Schadenssummen haben nur 60 Teilnehmer Angaben gemacht: der „durchschnittliche größte Vorfall" verursachte demzufolge gut 50 000 € direkte Kosten (max. 1 Mio. €) und knapp 7 500 € Rekonstruktionsaufwand (max. 100 000 €).

Malware

Generell ist die Zahl der Unternehmen, die Virenvorfälle zu verzeichnen hatten, im Vergleich zur vorigen Studie um 14 Prozentpunkte gestiegen: 88 % der Teilnehmer waren in mindestens einer Malware-Kategorie betroffen. Spitzenreiter waren dabei klar die Würmer (84 %), gefolgt von File-Viren (64 %). Mit Boot-Viren hatte hingegen nur noch jedes vierte der befragten Unternehmen zu kämpfen; dies ist gleichzeitig die einzige Kategorie, bei der sich steigende und sinkende Vorfallszahlen in etwa die Waage hielten (vgl. Tab. 4).

Abbildung 3: Nennenswerte Beeinträchtigung durch „Top-5"-Malware



Basis: Ø 127 Antworten

	Priorität	Schäden min. 1 bei	Schäden Nennungen
Unfälle	**2,91**	**73%**	**229**
... menschliches Versagen	1,80	54%	98
... technisches Versagen	1,12	57%	131
Angriffe	**2,70**	**60%**	**138**
... ungezielt (Malware)	1,34	54%	82
... gezielt (Hacker, Sabotage, Spionage usw.)	1,37	25%	56

Basis: s. Tab. 1

Tabelle 2: Alternative Zusammenfassung der Gefahrenbereiche

Wurde bereits versucht auf dem Web-Server...	ja
Seiten zu verändern (Vandalismus)	22%
Daten auszuspionieren	17%
Daten zu löschen	9%
Daten in betrügerischer Absicht zu manipulieren	7%
Angebote lahmzulegen (Denial of Service)	27%
nichts von alledem	56%

Basis: 124 Antworten

Tabelle 3: Angriffe auf WWW-Server

Haupteinfallstor für Malware aller Art ist mittlerweile ganz klar die E-Mail (insgesamt 311 Nennungen); Downloads aus dem Internet landen auf einem etwas abgeschlagenen zweiten Platz (109 Nennungen). Doch auch der klassische Weg über Datenträger stellt immer noch eine Bedrohung dar: Mit 76 Nennungen sind Disketten, CD-ROMs und Ähnliches noch immer erfolgreicher als die automatische Verbreitung von Würmern über Internet (66 Nennungen) oder LAN (52 Nennungen). Durchschnittlich zehn Prozent der Teilnehmer haben zudem Infektionen aus unbekannter Quelle angegeben.

Bei der Frage nach nennenswerten Beeinträchtigungen durch die „Top 5" der Malware hat vor allem Blaster/

	Vorfälle ja, bei	Tendenz gestiegen	Tendenz gesunken
File-Viren	64%	77%	23%
Boot-Viren	24%	51%	49%
Makro-Viren	51%	71%	29%
Würmer	84%	91%	9%
Troj. Pferde / Backdoors	57%	83%	17%

Basis: Ø 143 Antworten (Vorfälle), Ø 74 (Tendenz)

Tabelle 4: Malware-Vorfälle

	Ausfallzeit Mittel	Ausfallzeit max.	Kosten Mittel	Kosten max.
Virus-/Wurm-Infektion	54,54	1200	25.954	500.000
Fehlalarm (unbegründete Fehlermeldung)	5,66	60	1.817	30.000
Hoax (unbegründete Warnung)	10,1	100	1.270	10.000

Basis: Ø 76 Antworten (Infektion), Ø 41 (Fehlalarm/Hoax)

Tabelle 5: Aufwand durch Malware-Infektion/-Fehlalarm

Lovsan zugeschlagen; 39 % der antwortenden Teilnehmer hatten damit Probleme. Und dort wo Blaster landen konnte, tat er dies oft besonders heftig: Zwölf Unternehmen nannten den Wurm explizit als größten Schadensstifter der vergangenen zwei Jahre (Top-5-Frage: 51 Nennungen). Im Schnitt musste jeder Teilnehmer an der Studie 37 Malware-Infektionen pro Jahr bekämpfen – selbst unter Ausschluss der Maximalangabe von sage und schreibe 2 500 Infektionen bleiben noch 10 Vorfälle pro Unternehmen und Jahr. Hinzu kommen durchschnittlich 9 technische Fehlalarme und 8 unbegründete Warnungen, so genannte Hoaxes – berücksichtigt man hier auch die beiden Ausreißerwerte von je eintausend Hoaxes, so sind im Schnitt sogar 41 solche Störungen pro Jahr zu bearbeiten.

Als Trost bleibt, dass die geschätzten Kosten für Fehlalarme und Hoaxes mit 1 817 € beziehungsweise 1 270 € deutlich unter den vor zwei Jahren genannten Werten liegen (2002: 8 173 € bzw. 9 621 €). Die Beseitigung wirklicher Viren und Würmer bleibt aber eine teure Angelegenheit: Im Mittel veranschlagen die Befragten hierfür 25 954 € pro Vorfall (2002: 26 228 €). Die mittlere Ausfallzeit bleibt jedoch mit nunmehr 54 Stunden deutlich unter dem Schätzwert der vorigen Studie (2002: 94 Std, vgl. Tab. 5 auf S. 5).

Sicherheitslage

Die allgemeine Selbsteinschätzung zum Stand der Informations-Sicherheit in den befragten Unternehmen entspricht den langjährigen Erfahrungen: Je „näher" ein Infrastrukturelement an der zentralen Administration sitzt, umso besser ist die generelle Sicherheitslage. Im Rechenzentrum sehen erneut 75 % der Teilnehmer die Sicherheit als sehr gut oder gut an, bei den Servern verlagert sich diese fest umrissene Gruppe zu gut/befriedigend, bei den Endgeräten gibt die Durchschnittsbewertung bei den PCs und mobilen Geräten jeweils um eine halbe Note nach. Ähnlich schlecht wie Heimarbeitsplätze und Notebooks bewerten die Teilnehmer WLANs: Auch hier ist fast die Hälfte der Meinung, die Sicherheit sei gerade noch oder noch nicht einmal ausreichend (vgl. Abb. 4).

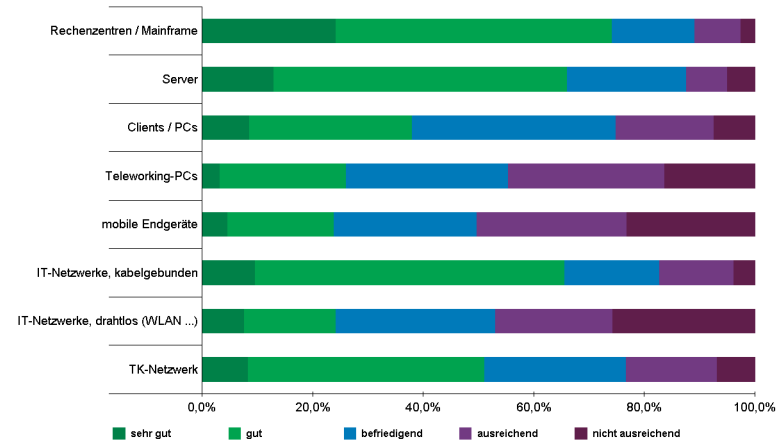


Abbildung 4: Einschätzung der Sicherheit

Basis: Ø 131 Antworten

In Bezug auf den Stellenwert, den die Informations-Sicherheit beim Top-Management einnimmt (Abb.5), ist in diesem Jahr ein erfreulicher Anstieg der „Befürworter" zu erkennen: Die Gruppe derer, die in der ISi ein vorrangiges Ziel oder sogar einen Mehrwert erkennen, ist sprunghaft auf 38 % gestiegen (2002: 20 %). Allerdings ist auch bei denjenigen, die ISi eher als ein „lästiges Übel" ansehen, erstmals wieder ein – wenn auch leichter – Anstieg um einen Prozentpunkt festzustellen. Ob es sich hierbei um eine statistische Schwankung handelt oder sich eine Polarisierung der Lager abzeichnet, wird man weiter beobachten müssen. Bei den kleineren und mittleren Unternehmen (KMU) könnte sich das stärker andeuten: Dort sind durch 46 % „vorrangig oder Mehrwert"-Nennungen und andererseits 32 % „lästigen Übeln" die Extrempositionen stärker vertreten. Weniger „Bewegung aus der Mitte heraus" ist bei den Unternehmen mit mehr als 500 Mitarbeitern zu erkennen: 28 % Befürworter stehen hier 42 % „Gleichrangigkeits-Unterstützern", aber auch nur 29 % eher ablehnender Haltung gegenüber.

Bei der Verbesserung der ISi behindern am meisten:	
Es fehlt an Geld	62%
Es fehlt an Bewusstsein bei den Mitarbeitern	51%
Es fehlt an Bewusstsein und Unterstützung im Top-Management	45%
Es fehlt an Bewusstsein beim mittleren Management	42%
Es fehlen verfügbare und kompetente Mitarbeiter	33%
Es fehlen die strategischen Grundlagen/ Gesamt-Konzepte	31%
Die Kontrolle auf Einhaltung ist unzureichend	29%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	28%
Es fehlen geeignete Methoden und Werkzeuge	18%
Die vorhandenen Konzepte werden nicht umgesetzt	18%
Es fehlen geeignete Produkte	17%
Anwendungen sind nicht für ISi-Maßnahmen vorbereitet	17%
Es fehlen realisierbare (Teil-)Konzepte	16%
Es fehlt an praxisorientierten Sicherheitsberatern	8%
Sonstiges	6%
keine Hindernisse	3%

Tabelle 6: Hindernisse für bessere Informations-Sicherheit

Basis: 160 Antworten

Die Probleme, welche die Teilnehmer am meisten bei der Verbesserung der Informations-Sicher-

heit behindern, wurden in den vorigen Studien regelmäßig von mangelndem Bewusstsein der Mitarbeiter und Manager angeführt. Dieses Jahr ist hingegen zu wenig Geld erstmals als Haupthindernis angegeben worden: Fast zwei Drittel (62 %) der Teilnehmer klagten über Behinderung durch finanzielle Beschränkung (vgl. Tab. 6). Damit ist dieses Problemfeld erneut um 16 Prozentpunkte in der Bedeutung gestiegen, nachdem es bereits von 2000 auf 2002 um 15 Prozentpunkte zugelegt hatte. Positiv zeigte sich hingegen die Entwicklung der „Awareness“: Das mangelnde Bewusstsein bei den Mitarbeitern und Managern wurde von deutlich weniger Teilnehmern beklagt, belegt aber immer noch die Problem-Ränge zwei bis vier. Da eine beliebige Zahl von Mehrfachnennungen zulässig war, ist nicht zu erwarten, dass sich lediglich ein Verdrängungseffekt durch die Geldnot zeigte. Nach wie vor haben die Befragten im Mittel 4–5 Probleme als „meist behindernd“ angegeben.

Dennoch zeigt der Kenntnisstand zur Informations-Sicherheit (Abb. 6) ein gewohntes Bild und kei-

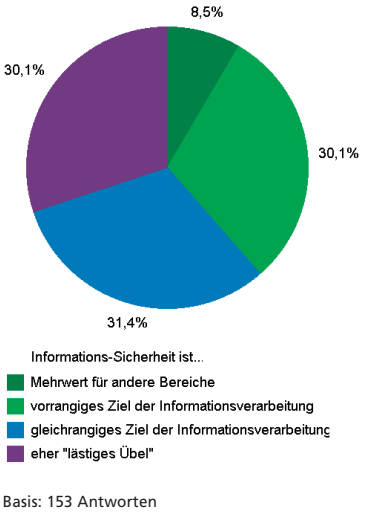


Abbildung 5: Stellenwert der Informations-Sicherheit beim Top-Management

Vielen Dank für freundliche Unterstützung

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 allen Teilnehmern an der Befragung, die durch Ihre wertvolle Mitarbeit ein sinnvolles Gesamtbild entstehen lassen.

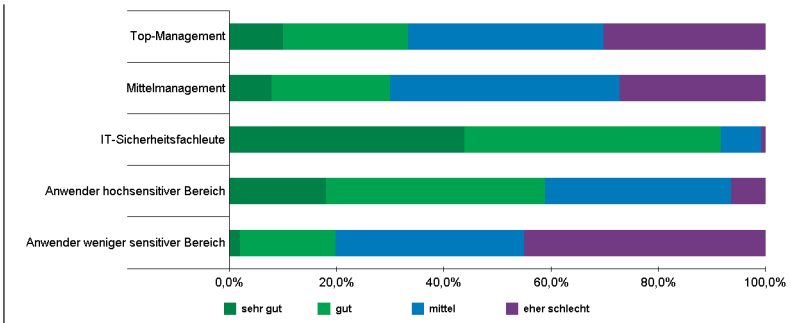


Abbildung 6: Kenntnisse der Manager und Mitarbeiter

Basis: Ø 148 Antworten

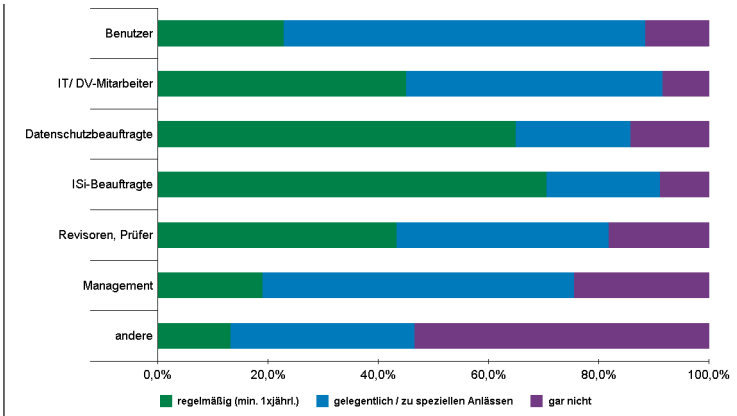


Abbildung 7: Schulungsfrequenz verschiedener Mitarbeitergruppen

Basis: Ø 128 Antworten, 83 (Prüfer), 45 (andere)

Ausbildungsmethode wird eingesetzt	häufig	gelegentlich	nie	Antworten
interne Schulungen durch Frontalunterricht, möglichst flächendeckend	10%	44%	46%	132
interne Schulungen durch Frontalunterricht für Spezialgruppen	17%	56%	28%	133
externe Schulungen	19%	55%	26%	138
Materialien (Schulungsunterlagen) zum Selbstlernen	14%	58%	28%	139
(Multimediale) Lern-CDs zum Selbstlernen	8%	28%	64%	119
Online-Trainings-Anwendungen/ -Tools (Intranet)	11%	31%	58%	120

Tabelle 7: Schulungsmethoden

Basis: s. „Antworten"

nen deutlichen Wissenszuwachs bei Anwendern und Management: die Bewertungen fielen höchstens ein bis zwei Zehntelnoten besser aus als 2002, das Top-Management stagnierte bei „etwas besser als mittelmäßig". Und noch immer wird fast ein Viertel der Manager „gar nicht" zu Fragen der Informations-Sicherheit geschult oder informiert (vgl. Abb. 7); allerdings ist auf der anderen Seite eine erfreuliche Steigerung derjenigen Managergruppe zu beobachten, die regelmäßig solche Weiterbildung erfahren (jetzt 19 %, 2002 12 %). Der Schwerpunkt der Schulungen liegt aber weiterhin bei den Spezialisten und zwar in Form gelegentlicher externer Schulungen. Online-Trainings und interaktives Material (Lern-CDs o. Ä.) sind weiterhin eher die Ausnahme und bei weit über 50 % überhaupt nicht im Einsatz (vgl. Tab. 7).

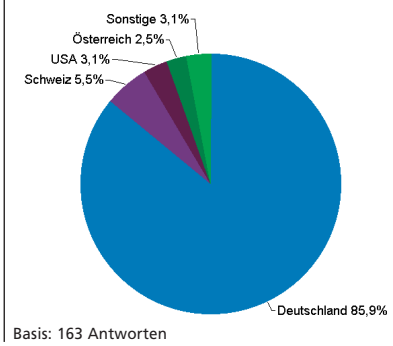


Abbildung 8: (Haupt-)Sitz der teilnehmenden Unternehmen und Behörden

Basis: 163 Antworten

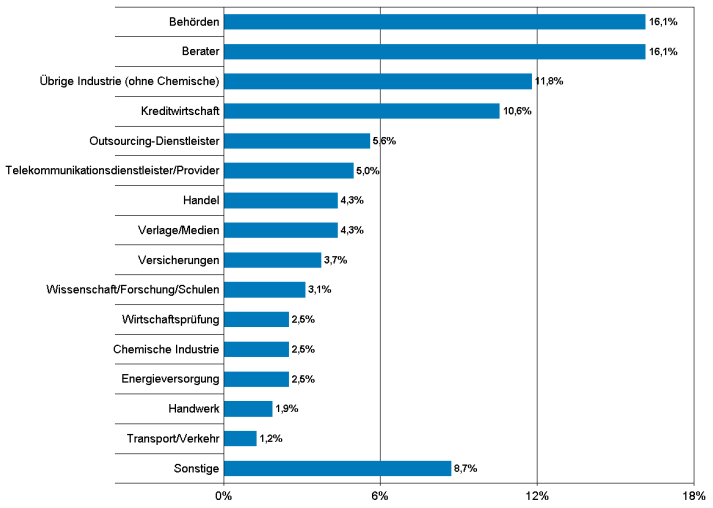
Teilnehmer

Die Teilnehmer der <kes>-Sicherheitsstudien entstammen klassischerweise eher großen mittelständischen sowie Großunternehmen und -institutionen: Die durchschnittliche Mitarbeiterzahl beträgt über 4 600, in der Summe repräsentieren die Befragten rund eine Dreiviertelmillion Beschäftigte. In diesem Jahr hat sich auch ein beträchlicher Anteil kleinerer und mittlerer Unternehmen an der Studie beteiligt, die offenbar überwiegend besonderen Wert auf die Sicherheit legen (s. a. Budgets): Obwohl die Unternehmen mit weniger als 500 Mitarbeitern (KMU) nur 1,5 % der Gesamtzahl beschäftigen, zeichnen sie für rund 30 % der insgesamt erfassten 1 139 ISi-Spezialisten verantwortlich. Das spiegelt sich auch in den „überdurchschnittlichen" IT-Abteilungen der „Kleinen" wider, die (bei durchschnittlich 128 Mitarbeitern insgesamt) im Schnitt 15 Köpfe zählen; vier davon sind Sicherheitsspezialisten, 40 % haben eine zentralen ISi-Beauftragten. Ein überdurchschnittlich großer Teil in dieser Teilnehmer-Gruppe sind Berater und sonstige Dienstleister; „kleinere" Banken und Behörden sind dort ebenfalls stark vertreten.

Die „Großen" haben hingegen im Schnitt gut 10 000 Mitarbeiter; die durchschnittliche IT-Abteilung zählt dort rund 300 Beschäftigte, von denen sich 12 speziell der Informationssicherheit widmen; ein zentraler ISi-Beauftragter ist in vier Fünfteln dieser Unternehmen vorhanden. Die IT-Ausstattung der Befragten zeigt sich – unter Auslassung eines „Ausreißerwerts" – im Mittel wie folgt (Werte in Klammern geben die Durchschnittszahlen für KMU bzw. Großbetriebe an): 3 Mainframes (2/4), 145 Server (15/321), 2 434 Clients/PCs (168/5 631), 55 Heimarbeitsplätze (5/132) sowie 381 mobile Endgeräte (22/864). Der Anteil mobiler Endgeräte ist dabei weiter gewachsen: 2002 lag dieser bei gut

10 %, heuer bereits bei 13 %. Nimmt man die Heim- und Telearbeitsplätze hinzu, so befinden sich heute rund 14,5 % aller Endgeräte außerhalb der unmittelbaren oder zumindest stetigen Verfügungsgewalt der Unternehmen.

Auch hinsichtlich der Netzwerke zeigt sich der Trend zum verteilten Arbeiten: Die Studie erfasst dieses Jahr insgesamt 1 877 Weitverkehrsnetze (WAN, inkl. VPN und gemieteten Netzen), somit durchschnittlich 16 (7/27) pro befragtem Unternehmen. Im Mittel betreibt jedes teilnehmende Unternehmen zudem 65 LAN/PC-Netze (8/155) und 3 Wireless LANs (1/6).



Basis: 161 Antworten

Abbildung 9: Branchenzugehörigkeit der Teilnehmer an der <kes>/Microsoft-Sicherheitsstudie

Budgets

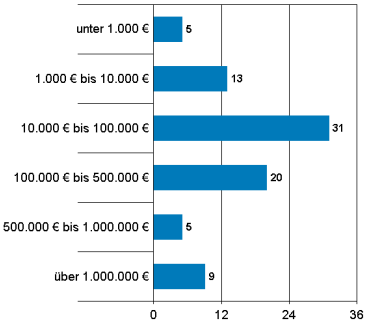
84 Teilnehmer haben Angaben zu Umsatz oder Bilanzsumme ihres Unternehmens gemacht (weitere 38 gaben an, dass eine solche Zahl aufgrund eines Status als Behörde o. Ä. irrelevant wäre). Der durchschnittliche angegebene Umsatz belief sich dabei auf knapp 2 Mrd. € – auch von den KMU, die hier Angaben gemacht haben, konnte mehr als ein Drittel mindestens 10 Mio. € Umsatz verbuchen. Die mittlere angegebene Bilanzsumme (entscheidende Kennzahl für Versicherungs- und Kreditwirtschaft) kam auf beinahe 20 Mrd. €.

Zu den bereitstehenden Budgets (jeweils inkl. Personalkosten) haben 93 Befragte geantwortet: Bei einem durchschnittlichen Wert von gut 10 Mio. € für die IT-Budgets 2004 kommen für die Stichprobe der <kes>/Microsoft-Sicherheitsstudie hochgerechnet deutlich über 1,6 Mrd. € zusammen, von denen aber vermutlich der Löwenanteil auf Personalkosten entfallen dürfte. Der Anteil für die Informationssicherheit liegt im Mittel bei 13 % (18 % bei KMU, 6 % bei den „Großen"). Aus 83 Fragebögen, in denen wir sowohl zum IT-Budget als auch zum ISi-Anteil Angaben erhalten haben, ließ sich als mittlerer absoluter Betrag für die geplanten ISi-Ausgaben 381 787 € errechnen (wiederum kategorisiert nach Mitarbeiterzahl: 132 Tsd. € / 779 Tsd. €, s. a. Abb. 10).

Allerdings mussten die meisten Teilnehmer die entsprechenden Werte schätzen – der Anteil der „ermittelten" Daten liegt jedoch im Vergleich zur vorigen Studie höher: 17 % der Antwortenden konnten sich beim IT-Budget auf „sichere" Zahlen stützen, immerhin 9 % auch beim ISi-Anteil (2002 waren das nur 5 %). Bei Organisationen mit mehr als 500 Mitarbeitern lagen die Anteile der „ermittelten" Werte mit 31 % beziehungsweise 20 % dabei deutlich über den KMU, bei denen nur 9 % der IT-Budgets beziehungsweise 2 % der ISi-Anteile nicht der erhöhten Varianz von Schätzungen unterworfen waren.

Datenwert

Auch dieses Jahr zeigte sich der immense Wert der vorgehaltenen Informationen in den Aussagen von 90 Teilnehmern, die sich zu Verlusten nach der Vernichtung aller elektronisch gespeicherter Daten äußerten: Neun Antworten davon lauteten schlichtweg „unvorstellbar", „unbezahlbar" oder legten nahe, dass dies den Geschäftsverlust zur Folge hätte. Die 81 quantifizierten Antworten ergaben einen mittleren Datenwert von rund 281 Mio. € (12,5 Mio. € / 694 Mio. €), wobei die höchste Nennung 6,3 Mrd. € lautete. Die meisten Schätzungen lagen zwischen einer und einhundert Millionen Euro (vgl. Tab. 8), wobei die geringeren Werte – nicht überraschend – eher bei den kleineren, die höheren Verluste eher bei den größeren Unternehmen erwartet wurden.



Basis: 83 Antworten

Abbildung 10: Budget für Informations-Sicherheit (Anzahl Nennungen)

Datenwert/Verlust	Nennungen
unter 10.000 €	3
10.000 bis 100.000 €	11
100.000 bis 1 Mio. €	19
1 Mio. bis 100 Mio. €	27
100 Mio. bis 500 Mio. €	13
500 Mio. bis 1 Mrd. €	2
über 1 Mrd. €	6
Unternehmenswert, Bankrott o.Ä.	9

Basis: s. „Nennungen"

Tabelle 8: Geschätzter Verlust bei Vernichtung aller elektronisch gespeicherter Daten (Anzahl der Nennungen pro Staffel)

Organisation

Bei der Frage nach den Verantwortlichkeiten in Sachen Informations-Sicherheit (ISi) sind die bedeutendsten Positionen der zentrale ISi-Beauftragte und der Leiter der Informations-/Datenverarbeitung (IV/DV bzw. RZ-Leiter): 58 % der Befragten haben einen zentralen ISi-Beauftragten (Tab. 9), der dort naturgemäß die Formulierung der ISi-Ziele, Risikoanalysen und Konzepte sowie die Business Continuity dominiert. Wo es keinen zentralen ISi-Beauftragten gibt, übernimmt vor allem der Leiter IV/DV/RZ wesentliche Teile der Sicherheitsverantwortung, aber auch Top-Management und Administratoren nehmen in diesen Unternehmen verstärkt Sicherheitsaufgaben wahr. Einen durchweg besonders hohen Anteil haben die Leiter IV/DV/RZ an Notfall- und Eskalationsmaßnahmen sowie Business Continuity: Hierbei stehen sie bei knapp 43 % der Befragten in der Pflicht, während zentrale ISi-Beauftragte „nur“ von rund 35 % für diesen Bereich als (mit-)verantwortlich benannt wurden.

Insgesamt liegt die Verantwortung für Sicherheitsaufgaben allerdings häufig nicht nur bei einer Person – bei vorhandenem zentralen ISi-Beauftragten sogar noch seltener als in den Organisationen, wo dieser Posten nicht existiert. Bei der Prüfung und Einhaltung gesetzlicher Vorgaben tragen zentrale Datenschutzbeauftragte (vorhanden bei 43 % der Teilnehmer) sogar häufiger (Mit-)Verantwortung als zentrale ISi-Beauftragte. Die Revision wirkt dabei naturgemäß auch verstärkt mit; darüber hinaus wird dieser Funktionsbereich vor allem bei Risiko- und Sicherheitsanalysen mit einbezogen.

Bei der (Mit-)Verantwortlichkeit für die Sensibilisierung und Schulung der Anwender folgen dem zentralen ISi-Beauftragten (29 %) die Administratoren (22 %) und der Benutzerservice (21 %).

Dass Sicherheitsaspekte bei der Beschaffung und Inbetriebnahme von IT-Systemen von immerhin 35 % der Befragten als Hauptkriterium genannt wurden (vgl. Abb. 11), schlägt sich nicht in der Verantwortlichkeit für Beschaffung und Betrieb nieder: Dies ist klar die Domäne der Leiter IV/DV/RZ – ISi-Beauftragte haben dort nur bei rund 3–6 % der Unternehmen eine Mitverantwortung. Immerhin gaben 38 % der Teilnehmer an, dass die Erfüllung von ISi-Anforderungen als Voraussetzung für die Inbetriebnahme auch verifiziert wird – diese Gruppe ist allerdings überraschenderweise nur zu rund zwei Dritteln deckungsgleich mit der Nennung von Sicherheitsaspekten als Hauptkriterium.

Outsourcing / Beratung

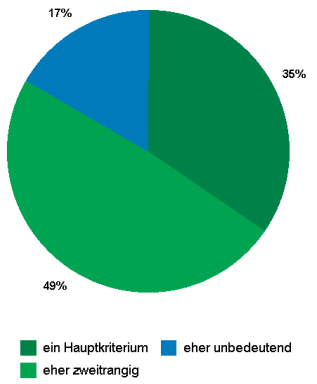
Mit nur 52 % lag heuer der Anteil der Befragten, die Outsourcing in der einen oder anderen Form betreiben, deutlich niedriger als vor zwei Jahren (2002 waren es 73 %). Neben der Entsorgung von Datenträgern sind dabei weiterhin Managed

Tabelle 9: Vorhandene Posten

Gibt es im Unternehmen... ?	ja, bei
zentraler ISi-Beauftragter	58%
dezentraler ISi-Beauftragter	12%
zentraler Datenschutzbeauftragter	60%
dezentraler Datenschutzbeauftragter	10%
ISi-Ausschuss (o. Ä.)	13%
Leiter IV/DV/RZ	70%
IV/DV-Revision	35%
Leiter Sicherheit/Werkschutz	31%
DV-orientierter Jurist	10%

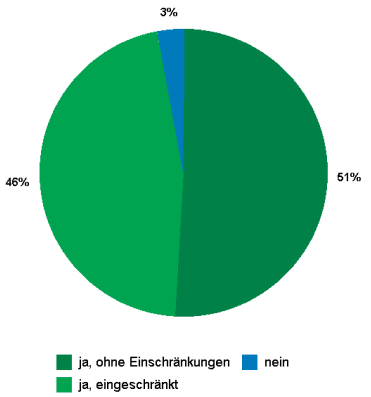
Basis: 145 Antworten

Abbildung 11: Bedeutung von Sicherheitsaspekten bei der Beschaffung von IT-Systemen



Basis: 156 Antworten

Abbildung 12: Zufriedenheit mit Beratungsdienstleistungen



Basis: 95 Beratungs-Kunden

Genutzte Outsourcing-Dienstleistungen	
Entsorgung von Datenträgern (Papier, EDV)	63%
Managed Firewall/IDS	32%
Betriebssystempflege	29%
Netzwerk-Management	28%
Datensicherung, Backup-Lösungen	26%
gesamtes Rechenzentrum	23%
Datenbank-Systeme, Werkzeuge	23%
Online-Anwendungssysteme	21%
Sonstiges	18%
Auftragsentwurf, Arbeitsvorbereitung, Operating	15%
Notfallvorsorge/Business Continuity	15%
Verwaltung, Dokumentation, Archivierung	13%
Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung	13%
Haustechnik	13%
Überwachung, Kontrolle, Qualitätssicherung	12%
Datenschutz gemäß BDSG	11%

Tabelle 10: Outsourcing-Dienstleistungen Basis: 82 Outsourcing-Geber

Firewalls/IDS beliebt, gefolgt von extern gepflegten Netzwerken und Betriebssystemen (vgl. Tab. 10). Service-Level-Agreements (SLAs) haben in der Outsourcing-Stichprobe eine etwas stärkere Bedeutung als bei den 2002 Befragten: Drei Viertel der Outsourcing-Geber haben ein SLA abgeschlossen, 69 % auch mit expliziten Anforderungen an die ISi (2002: 60 %), Datenschutzanforderungen sind sogar bei 74 % der Unternehmen enthalten, für die diese Thematik relevant erschien. Ein knappes Drittel der SLAs enthalten zudem ein regelmäßiges Kontrollrecht.

Bei der Nutzung von Beratungsdienstleistungen zeigt sich ein ähnliches Bild wie vor zwei Jahren: 53 % der Befragten nutzen gelegentlich Consultants, 6 % tun dies regelmäßig. Haupt-Aufgabe der Berater waren dabei Risikoanalysen und Konzeptentwicklung sowie Penetrationstests und sonstige Schwachstellenanalysen (s. a. Tab. 11). Die Zufriedenheit mit den Beratungsleistungen hat sich im Vergleich zur vorigen Studie sogar noch etwas verbessert (vgl. Abb. 12): Bei weiterhin nur 3 % unzufriedenen Kunden zeigten sich heuer sogar 51 % uneingeschränkt zufrieden (2002: 49 %).

Erstmals haben wir in dieser <kes>-Studie nach Computer Emergency (CERTs) und Security Incident Response Teams (CSIRTs) gefragt: 23 % der Teilnehmer nutzen externe CERT/CSIRT-Dienstleistungen; allerdings nur ein gutes Drittel davon kostenpflichtige Leistungen. Ein eigenes CERT oder CSIRT betreiben 19 % der Befragten.

Versicherungen

Bei der Risikoabwälzung auf Versicherungen lagen die „Klassiker“ klar vorne: 79 % der Teilnehmer haben eine Feuerversicherung abgeschlossen (gut jeder Zwanzigste davon musste diese auch bereits in Anspruch nehmen), 69 % haben eine Sachversicherung, die sogar schon bei fast zwei Fünftel ihrer Versicherten einmal einspringen musste (Tab. 12).

Zertifikate und Audits scheinen im Zusammenhang mit Versicherungen derzeit dennoch nur eine Randerscheinung zu sein: Nur 2 % bejahten unsere Frage, ob sie für den Abschluss mindestens einer Versicherung ein ISi-Audit durchlaufen oder ein anerkanntes ISi-Zertifikat vorlegen mussten. Bei möglichen Rabatten sah es nicht viel anders aus: 7 % wussten von günstigeren Konditionen mindestens einer ihrer abgeschlossenen Versicherungen zu berichten, falls freiwillig eine solche Überprüfung durchlaufen würde.

Konzepte

Der Anteil der Befragten mit einer schriftlich fixierten Strategie zur Informations-Sicherheit ist im Vergleich zu 2002 erfreulicherweise um vier Prozentpunkte auf jetzt 60 % gestiegen; auch bezüglich des Vorhandenseins eines integrierten Sicherheitshandbuchs liegen die Angaben mit 31 % deutlich über dem Ergebnis der vorigen Studie. Gleichzeitig sind bezogen auf die gesamte Stichprobe die Zahlen bezüglich spezifischer schriftlicher Konzepte und Richtlinien zu Detailthemen um vier bis neun Prozentpunkte gesunken – Spitzenreiter sind erneut Richtlinien zur Internet- und E-Mail-Nutzung (bei 77 % der Befragten vorhanden), Schlusslicht bleiben mit wiederum nur 33 % Nennungen Richtlinien zur Verschlüsselung (Tab. 13).

Genutzte Beratungs-Dienstleistungen	
Risikoanalysen und Konzeptentwicklung	55%
Penetrationstests	48%
Schwachstellenanalysen	44%
Strategie- und Managementberatung	35%
Kontrolle vorhandener Konzepte auf Eignung und Einhaltung	31%
Umsetzung von Konzepten und Maßnahmen	28%
Sonstiges	6%

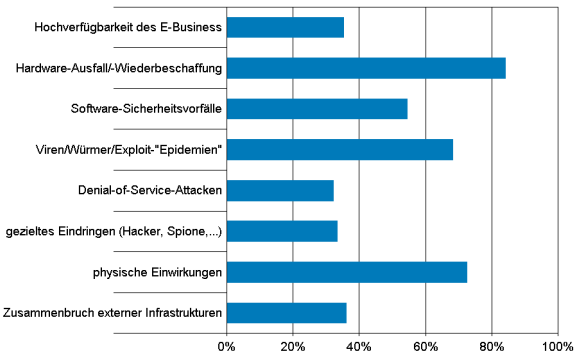
Basis: 95 Beratungs-Kunden

Tabelle 11: Beratungsdienstleistungen

Versicherungen	abgeschlossen von	bereits beansprucht (Nennungen)
Feuerversicherung	79%	6
Sachversicherung	69%	33
„Technologie-Police“ o.ä. (Kombination von Elektronik- u. Maschinenversicherung)	19%	3
Computermissbrauch-Versicherung	11%	0
Datenmissbrauch-Versicherung	7%	0
Datenrechtsschutz-Versicherung	7%	0
Sonstige	5%	2
Datenversicherung/Softwareversicherung	3%	3
Elektronik-Betriebsunterbrechungsversicherung erw. Datenversicherung (inkl. Schäden durch Viren, fehlerhaftes Programmieren, versehentliches Löschen)	1%	1
Mehrkostenversicherung	1%	1
keine	22%	

Basis: Ø 101 Antworten

Tabelle 12: Versicherungen



Basis: Ø 123 Antworten

Abbildung 13: Berücksichtigung spezieller Anforderungen im EDV-Notfall-/Wiederanlaufkonzept

Ein EDV-Notfall- und Wiederanlaufkonzept existiert bei 82 % der Teilnehmer – allerdings nur bei einem Fünftel davon in verifizierter und validierter Form. Mehr als zwei Fünftel haben dieses Konzept hingegen nicht einmal schriftlich niedergelegt, was wohl Zweifel an seiner Tragfähigkeit im Falle eines Falles aufwirft. Der Anteil der „überlieferten" Notfallkonzepte stieg damit gegenüber 2002 um 10 Prozentpunkte, während validierte Konzepte um 10 Prozentpunkte zurückgingen (Inhalte von Notfallkonzepten s. Abb. 13).

Gesunken ist auch die Bereitschaft, Konzepte, Richtlinien und Maßnahmen zu überprüfen: Während vor zwei Jahren nur 24 % die *Einhaltung* vorgesehener Maßnahmen *nicht* geprüft haben, sind dies heuer 31 % (Tab. 14) – bezogen auf die gesamte Stichprobe verzichten sogar 34 % aktuell auf die Prüfung der fortdauernden *Eignung* von Konzepten und Richtlinien (Tab. 15, 2002 waren das nur 16 %).

Betrachtet man die Antworten auf diese Fragen getrennt für die Unternehmen *mit* schriftlicher Sicherheits-Strategie, so zeigt sich – wenig verwunderlich – eine insgesamt höhere Bereitschaft, Konzepte und Maßnahmen schriftlich zu fixieren und anschließend zu prüfen (vgl. Tab. 13). Dennoch bleiben auch bei diesem Teil der Stichprobe noch 14 %, die nach der Festlegung von Konzepten, Richtlinien und Maßnahmen *keine* weiteren Prüfungen durchführen (zur Reichweite s. Abb. 14).

Wie riskant fehlende (fortdauernde) Prüfungen sind, belegen jedoch eindrücklich die Zahlen der bei Überprüfungen zu Tage tretenden Probleme: In 75 % der Fälle wurden dabei Schwachstellen gefunden – und das sah bei Unternehmen mit schriftlicher Strategie nicht anders aus als bei denen ohne.

Tabelle 13: Strategien, Richtlinien und Konzepte

Gibt es im Unternehmen... ?	ja, bei	eingegrenzt auf Unternehmen mit ISi-Strategie	ohne ISi-Strategie
schriftlich fixierte IV-Strategie	56%	83%	16%
schriftlich fixierte ISi-Strategie	60%	100%	0%
umfassendes, integriertes Sicherheitshandbuch	31%	48%	8%
schriftlich fixierte spezifische ISi-Konzepte/-Richtlinien...			
... zum Einsatz von Verschlüsselung	33%	47%	13%
... zur Handhabung sensitiver/ kritischer Daten	61%	78%	37%
... zur Nutzung von Internet, E-Mail, ...	77%	91%	54%
... zum Softwareeinsatz auf PCs	70%	84%	49%
... zur Nutzung mobiler Endgeräte (Notebook, PDA, ...)	54%	72%	30%
... Sonstige	26%	45%	9%
Eignung von Konzepten/Richtlinien wird geprüft	*66%*	*86%*	*39%*
schriftlich formulierte Maßnahmen	65%	92%	34%
Einhaltung vorgesehener Maßnahmen wird geprüft	*69%*	*86%*	*40%*

Basis: Ø 157 Antworten (exist. Maßnahmen: 102), Ø 155 (Prüfung)

Open Source Software

Der Einsatz von Open Source Software (OSS) ist unter den Befragten weit verbreitet: Zwei Drittel nutzen OSS. Obwohl mit 59 % der größte Teil Open Source für sicherer hält als Produkte mit nicht-offengelegtem Quelltext (vgl. Abb. 15), liegt der Hauptgrund für den OSS-Einsatz doch beim Geld: 50 % gaben an, Open Source aus Kostengründen zu verwenden, nur 31 % wegen der Sicherheit. Weitere genannte Beweggründe waren beispielsweise mögliche Anpassungen oder bestehende Funktionen, Leistungsfähigkeit, Interoperabilität, Unabhängigkeit von Herstellern oder ideologische Gründe.

Heterogenität

Zugenommen hat der Einsatz von Produkten mehr als eines Herstellers bei Anti-Virus-Systemen: Vor zwei Jahren lag der Anteil der Befragten, die auf einen *einzelnen* Anbieter gesetzt haben, noch um neun Prozentpunkte höher als dieses Mal. Heuer setzen bereits 47 % die Lösungen *zweier* Anbieter in Kombination ein, um die Sicherheit der Malware-Abwehr zu verbessern, 13 % nutzen sogar drei oder mehr unterschiedliche Produkte auf verschiedenen Systemen oder Netzwerksegmenten. Erstmals haben wir dieses Jahr auch nach der Heterogenität in anderen Bereichen gefragt und hier bei Server-Betriebssystemen und Applikations-Servern ebenfalls einen deutlichen Anteil heterogener Architekturen gefunden (s. Tab. 16).

Evaluierungen

Der Bekanntheitsgrad der drei von uns bereits in der vorigen Studie erfragten internationalen Kriterienwerke ITSEC, Common Criteria (CC) und BS 7799 (bzw. ISO 17799) ist ungefähr so groß wie vor zwei Jahren – CC und BS 7799 sind noch immer rund einem Fünftel der Teilnehmer unbekannt. Gestiegen ist allerdings der Anteil derjenigen Teilnehmer, welche die Kriterien kennen und sich damit auch näher befasst haben, vor allem beim BS 7799, wo heuer 13 Prozentpunkte mehr zu verzeichnen sind als noch vor zwei Jahren. Erstmals gefragt haben wir nach ITIL und COBIT sowie dem US-Standard FIPS 140, der aber offenkundig im deutschsprachigen Raum keine nennenswerte Akzeptanz findet (vgl. Abb. 16).

Gestiegen ist hingegen mit der näheren Betrachtung der allgemeinen Kriterien zur Evaluierung auch der Einsatz evaluierter Produkte: Mit 39 % der Teilnehmer setzen fünf Prozentpunkte mehr als 2002 mindestens ein zertifiziertes Sicherheitsprodukt ein; ihre Erwartungen an Nutzen und Zuverlässigkeit dieser Produkte sahen – wie schon vor zwei Jahren – wiederum rund zwei Drittel als erfüllt an.

Eine klare Absage haben die Befragten heuer jedoch Mehrkosten für Sicherheitszertifikate erteilt: Während vor zwei Jahren noch 78 % der Antwortenden meinten, ein zertifiziertes Produkt rechtfertige einen höheren Preis, so sprach sich in der heute offenkundig angespannten finanziellen Lage sogar eine schwache Mehrheit gegen diese Aussage aus – nur noch 44 % sehen einen höheren Preis nunmehr als gerechtfertigt an.

Diese Ablehnung könnte auch einer der Gründe sein, warum dieses Jahr weniger Teilnehmer sich bezüglich des künftigen Einsatzes zertifizierter Lösungen unentschlossen zeigten: 26 % äußerten eine klares Nein zum bevorzugten Einsatz evaluierter Produkte (2002: 13 %), 24 % bejahten dies allerdings auch ebenso klar (2002: 23 %).

Risikobewertung

70 % der befragten Unternehmen führen eine Risikobewertung von Anwendungen und Systemen hinsichtlich ihrer Bedeutung für die Aufgabenerfüllung durch (vgl. Abb. 17); gut ein Fünftel der Teilnehmer prüft dabei alle Systeme. Diese Werte sind praktisch identisch mit dem Ergebnis von 2002. Deutlich verändert haben sich hingegen die Kriterien, die dabei vorrangig herangezogen werden: So verdrängt die Bedeutung möglicher Verstöße gegen Gesetze, Vorschriften und Verträge die Angst vor Imageverlust von Platz Eins der Skala. Um zwei Plätze höher bewertet haben die Teilnehmer dieses Jahr zudem Haftungsansprüche und Schäden bei Dritten (Tab. 17).

Gesetze und sonstige Rahmenwerke

Die nochmals gestiegene Priorität von Gesetzen und Verträgen

Die Einhaltung vorgesehener Maßnahmen wird geprüft...	ja, bei
durch die eigene Sicherheitsabteilung	33%
durch die Revision	32%
durch Sonstige	11%
durch externe Sicherheitsberater	9%
nein, sie wird nicht geprüft	31%

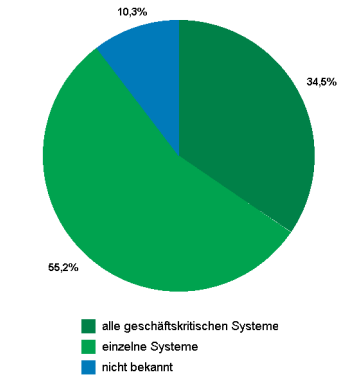
Basis: 159 Antworten

Tabelle 14: Prüfung vorgesehener Maßnahmen

Die (fortdauernde) Eignung von Konzepten/Richtlinien wird geprüft mithilfe von...	ja, bei
(erneuten) Risikoanalysen	44%
(erneuten) Schwachstellenanalysen	40%
Übungen (Notfall, Wiederanlauf)	32%
Penetrationsversuchen	32%
Simulationen oder Szenarien	13%
Sonstiges	8%
nein, es erfolgt keine Überprüfung	34%

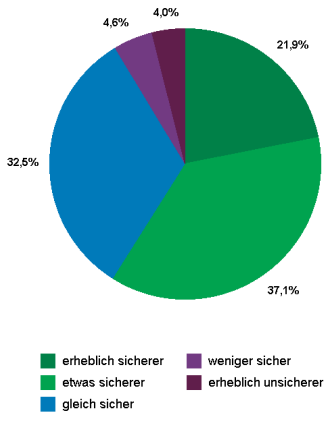
Basis: 157 Antworten

Tabelle 15: Prüfung der Eignung von Konzepten und Richtlinien



Basis: 116 Antworten

Abbildung 14: Reichweite der Eignungs-Überprüfung von Konzepten und Richtlinien



Basis: 151 Antworten

Abbildung 15: Einschätzung der Sicherheit von Open Source Software

Im Einsatz sind Lösungen von	einem Anbieter	zwei Anbietern	drei und mehr Anbietern
Anti-Virus-Software	40%	47%	13%
Firewalls	64%	28%	8%
Router	65%	22%	13%
Server-Betriebssysteme	44%	32%	24%
Web-Server	66%	24%	10%
Applikation-Server	49%	29%	22%

Tabelle 16: Heterogenität aus Sicherheitsgründen

Basis: Ø 142 Antworten

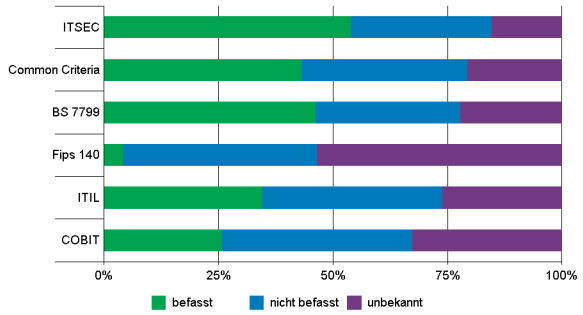


Abbildung 16: Bekanntheitsgrad internationaler ISi-Kriterien

Basis: Ø 149 Antworten

für die Risikobewertung beziehen die Befragten anscheinend vorrangig auf Verträge – zumindest ist ein gesteigerter Bekanntheitsgrad wichtiger Gesetze nicht feststellbar (Abb. 18): Beispielsweise geben auch in diesem Jahr 48 % der Befragten an, das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) *nicht* zu kennen, die Vorschriften des Teledienste- und Telekommunikationsrechts sind 45 % beziehungsweise 33 % der Befragten unbekannt, obwohl sie große Bedeutung für die Protokollierung auf Firewalls, Web- und Mail-Servern sowie für die E-Mail-Bearbeitung im Allgemeinen haben.

Immerhin sind aber die Angaben zum Umsetzungsgrad der meisten Bestimmungen etwas fortgeschrittener als 2002: Abgesehen von Rückschritten beim – in Bekanntheit und Umsetzung klar vorne liegenden – Bundesdatenschutzgesetz (BDSG) und auch beim KontraG zeigten sich ein höherer Anteil umfassender Umsetzung sowie weniger Unternehmen mit nur geringer Umsetzung (naturgemäß beruhen diese Angaben auf einer reduzierten Stichprobe, da die Umsetzung eines unbekannten bzw. als irrelevant angesehenen Gesetzes nur selten erfolgt).

Dennoch kann der Grad der „regulatorischen Compliance" insgesamt wohl nur als ungenügend gelten, wenn beispielsweise noch immer jedes zweite Unternehmen die größtenteils als relevant angesehenen Bestimmungen des BDSG nur „teilweise oder gering" umsetzt. Bei Telekommunikations- und Teledienstegesetzen sieht es noch deutlich schlechter aus, wenn bislang selbst in der verringerten Stichprobe, die hier eine Relevanz erkannt hat, nur etwa jeder Dritte „umfassend" reagiert (vgl. Abb. 19).

Tools und Vorgehensweisen

Beim Einsatz methodischer Vorgehensweisen und Software-Tools führt die checklistengestützte Schwachstellenanalyse, die bereits 49 % der Teilnehmer nutzen (in Planung bei weiteren 29 %). Auf den Plätzen Zwei bis Vier folgen Verfahren nach dem IT-Grundschutzhandbuch des BSI (45 %), selbstentwickelte Verfahren (40 %) und das IT-Sicherheitshandbuch des BSI (32 %). Das größte Ausbaupotenzial hat dabei der BSI-Grundschutz: nochmals 31 % der Teilnehmer planen zukünftig seine Umsetzung. Eine deutliche Absage haben die Befragten Sicherheitshandbüchern von Softwareherstellern und softwaregestützten Standardmethoden erteilt: jeweils fast drei Viertel äußerten, deren Einsatz sei nicht vorgesehen.

Die drei Top-Nennungen der bei Prüfungen unter ISi-Aspekten einbezogenen Sachgebiete waren bei jeweils mehr als der Hälfte aller Antwortenden das Berechtigungskonzept, der Virenschutz (deutlich gestiegen von 38 % in 2002) und das Notfallkonzept. Am unteren Ende der Skala

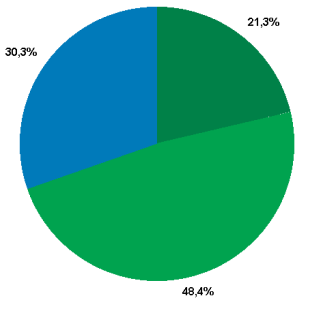


Abbildung 17: Reichweite der Risikobewertung

Basis: 155 Antworten

Kriterien zur Risikobewertung	sehr wichtig	wichtig	unwichtig	Vergl.-wert	Vgl.-W. 2002
Verstöße gegen Gesetze, Vorschriften oder Verträge	48%	44%	8%	1,40	1,47
Imageverlust	50%	36%	15%	1,35	1,51
Schaden bei Dritten/ Haftungsansprüche	43%	42%	16%	1,27	1,11
direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	38%	49%	12%	1,26	1,36
Verzögerung von Arbeitsabläufen	33%	55%	12%	1,21	1,35
indirekte finanzielle Verluste (z. B. Auftragsverlust)	36%	42%	22%	1,14	0,98
direkter finanzieller Schaden an Hardware u. Ä.	12%	50%	37%	0,75	0,97
Verstöße gegen interne Regelungen	9%	54%	37%	0,72	0,85

Tabelle 17: Kriterien zur Risikobewertung

Basis: Ø 135 Antworten

landeten – bei maximal einem Drittel der Befragten geprüft – die Übereinstimmung der System-Konfiguration mit den Vorgaben sowie Änderungshistorie und Korrektheit von Software (vgl. Tab. 18).

Maßnahmen

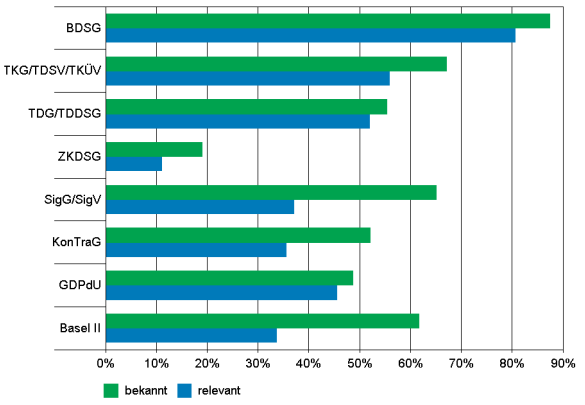
Schwerpunkt der realisierten und geplanten Maßnahmen zur Informations-Sicherheit (Tab. 19 auf S. 16) sind bei den Befragten klar die Bereiche von Servern und zentraler IT/TK. Dort findet man einen äußerst hohen Umsetzungsgrad was Datensicherung (99 %), Virenschutz (97 %) und Firewalls (95 %) angeht. Auch auf die physische Sicherheit wird dort deutlich stärker geachtet als dies bei Client-Systemen der Fall ist.

Als Authentifizierungsmethode Nummer Eins muss weiterhin klar das Passwort gelten – weit abgeschlagen folgen Hardware-Token und Chipkarten, wenn auch mit einem gewissen Planungspotenzial bei Clients und mobilen Endgeräten. Eine deutliche Absage erteilen die Befragten der Biometrie: Sowohl zur Authentifizierung beim Rechnerzugriff als auch in Sachen Zutrittskontrolle bleibt sie die große Ausnahme: Je nach Einsatzort und -zweck sagen 93–99 % der Teilnehmer deutlich „Biometrie ist nicht vorgesehen".

Eine gewisse Risikobereitschaft oder notgedrungenen Pragmatismus verheißen hingegen jeweils rund 45 % der Unternehmen, bei denen für PCs und mobile Endgeräte kein Backup vorgesehen ist – es steht zu bezweifeln, dass in allen diesen Fällen eine zentrale Datenhaltung vorliegt, die dafür sorgt, dass auf den Endgeräten keine wichtigen Dateien entstehen oder modifiziert werden. Bei noch weniger Teilnehmern kommen zudem auch Endgeräte in den Genuss einer unterbrechungsfreien Stromversorgung (USV) – hier dürfte der Hintergrund in den bislang sehr positiven Erfahrungen mit dem Versorgungsnetz liegen (s. aber bspw. <kes> 2003#3, S. 6). Eine bekannte Situation zeigte sich beim Überspannungsschutz: Gut vier Fünftel haben ihre EDV auf der Stromversorgungsseite gesichert – bei Daten- und TK-Leitungen allerdings weiterhin nur rund zwei Fünftel.

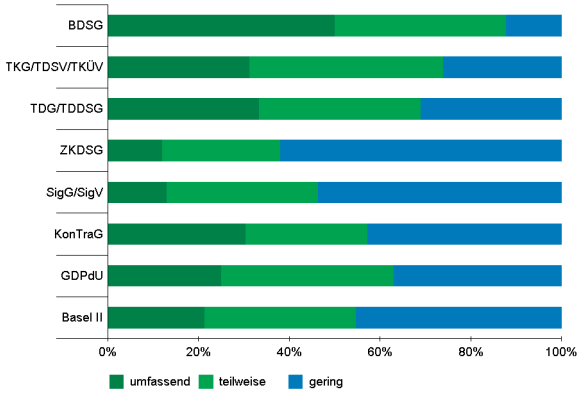
Trotz einer heute üblichen hohen Abhängigkeit von Telekommunikations- und Datennetzen ist überdies – vermutlich auch hier nicht zuletzt aufgrund der guten Verfügbarkeitswerte – bei relativ vielen Befragten *kein* Reserve-Netzzugang zur Überbrückung bei Ausfällen eingerichtet oder vorgesehen. Selbst Server und Zentrale bleiben hier in 36 % der befragten Unternehmen im Falle eines Falles ohne geplante Ersatz-Verbindung zur Außenwelt.

Riskant erscheinen zudem die Aussagen von bis zu 69 % der Befragten bei WLAN-Verbindungen *keine* Kryptographie einsetzen zu wollen. Auch sonst liegen die Angaben realisierter Verschlüsselungsmaßnahmen unter den Werten der vorigen Studie. Allerdings sind hier noch etliche Vorhaben in der Planung, besonders zur E-Mail- und Datei-Verschlüsselung sowie dem Chiffrieren ganzer Festplatten auf mobilen Systemen.



Basis: Ø 144 Antworten (Bekanntheit), Ø 134 Relevanz

Abbildung 18: Bekanntheitsgrad und geäußerte Relevanz gesetzlicher und sonstiger Rahmenwerke



Basis: Ø 87 Antworten

Abbildung 19: Umsetzungsgrad gesetzlicher und sonstiger Rahmenwerke

Darüber hinaus liegt das größte Planungspotenzial bei der (zentralen) Spam-Abwehr und Intrusion Detec-

Prüfung unter ISi-Aspekten von...	ja, bei
Berechtigungskonzept	59%
Virenschutz	56%
Notfallkonzept	52%
Netzwerkstrategie/Firewalls	51%
Datenklassifizierung und Zugriffsrechte	49%
Ablauforganisation	47%
physische Sicherheit	43%
Konzeption und Zielsetzung	41%
Software-Einsatz	41%
Aufbauorganisation	40%
Software-Entwicklung (inkl. Test- und Freigabeverf.)	35%
Übereinstimmung der System-Konfiguration mit Vorgaben	33%
Änderungshistorie (Change Management)	32%
Software (Korrektheit, Fehlerfreiheit usw.)	30%
Sonstiges	1%
nichts Derartiges	24%

Basis: 147 Antworten

Tabelle 18: Prüfung unter Aspekten der Informations-Sicherheit

tion/Prevention sowie der Ausstattung von Endgeräten mit verbessertem Zugangsschutz (Chipkarten und Hardware-Token).

Systemadministration

Manuelle Administration erfolgt nach wie vor bei sehr vielen Befragten in nennenswertem Umfang: 69 % gaben an, bei Netzwerksystemen häufig „Hand anzulegen", 72 % bei Host- und PC-Systemen. Managementlösungen der jeweiligen Hersteller (vor allem Cisco und Microsoft) sind bei 50 % der Teilnehmer für Netzwerk- beziehungsweise bei 39 % für PC-/Host-Systeme im Einsatz. Mit zentralen Managementlösungen arbeiten in nennenswertem Umfang 36 % der Befragten im Netzwerk und 41 % auf Hosts und PCs (meistgenannt: IBM Tivoli).

Informationen über Sicherheits-Updates beziehen die meisten direkt vom Hersteller: 67 % über aktive Kanäle (push) und 66 % über den offiziellen Internetauftritt. 42 % nutzen „unabhängige" Mailing-Listen auch, um sich über Updates zu informieren, 31 % tun dies über Webseiten Dritter. Derartige passive Kanäle prüfen 54 % der Befragten mindestens einmal in der Woche (vgl.

	Server / Zentrale			Clients / Endstellen			mobile Endgeräte		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
Firewalls	95%	2%	3%	43%	11%	46%	41%	20%	39%
Virenschutzmechanismen	97%	1%	2%	93%	2%	5%	86%	6%	8%
Datensicherung (Backup)	99%	1%	1%	51%	4%	45%	44%	11%	46%
Intrusion Detection Systems	44%	26%	31%	13%	7%	79%	7%	7%	86%
Benutzerverzeichnis mit Security-Policy	63%	13%	24%	32%	11%	57%	28%	7%	64%
Authentifizierung									
... Hardware-Token	15%	9%	76%	7%	14%	79%	17%	17%	67%
... Passwort	95%	1%	5%	94%	2%	5%	85%	1%	14%
... Chipkarte	11%	14%	74%	7%	19%	74%	10%	20%	70%
... biometrische Verfahren	1%	4%	95%	1%	4%	95%	0%	3%	97%
Protokollierung unberechtigter Zugriffe	76%	14%	10%	35%	15%	50%	20%	15%	65%
Content Inspection/Filtering	52%	15%	33%	19%	11%	70%	12%	10%	78%
Spam-Abwehr	56%	28%	15%	36%	16%	48%	24%	16%	60%
Verschlüsselung									
... sensitive Dateien	41%	22%	37%	31%	12%	57%	39%	17%	44%
... Festplatten (kpl./partitionsw.)	17%	18%	65%	12%	13%	75%	36%	22%	43%
... Archivdatenträger/Backups	23%	12%	65%	8%	5%	87%	8%	7%	85%
... LAN/Intranet-Verbindungen	28%	11%	61%	16%	7%	77%	20%	4%	76%
... WLAN-Verbindungen	24%	15%	61%	18%	14%	69%	24%	17%	59%
... WAN/Internet-Verbindungen	47%	8%	45%	33%	8%	60%	33%	10%	57%
... Telefon	5%	3%	92%	2%	1%	98%	2%	0%	98%
... Fax	4%	4%	93%	2%	1%	98%	2%	0%	98%
... E-Mail	34%	23%	43%	37%	20%	43%	32%	18%	49%
Physische Sicherheit									
... Zutrittskontrolle, biometrisch	4%	4%	93%	0%	1%	99%			
... Zutrittskontrolle, sonstige	81%	4%	15%	45%	1%	54%			
... Bewachung	49%	3%	49%	26%	1%	73%			
... Video-Überwachung	39%	3%	58%	11%	1%	88%			
... Einbruchmeldesysteme	72%	4%	24%	39%	4%	57%			
... Schutz von Glasflächen gegen Durchbruch/Durchwurf	55%	3%	41%	22%	2%	77%			
... Sicherheitstüren	76%	3%	21%	25%	1%	74%			
... Brandmeldesysteme	83%	2%	15%	47%	1%	52%			
... Löschanlagen	57%	3%	40%	20%	2%	79%			
... andere Meldesysteme (z. B. Gas, Staub, Wasser)	37%	6%	57%	9%	2%	89%			
... Datensicherungsschränke/-räume	85%	3%	12%	24%	2%	75%			
... Schutz gegen kompromittierende Abstrahlung (TEMPEST)	13%	1%	86%	2%	2%	96%	2%	1%	97%
... Maßnahmen gegen Hardwarediebstahl	63%	3%	33%	32%	6%	63%	35%	11%	54%
physikalisches Löschen von Datenträgern	53%	8%	39%	30%	11%	59%	26%	9%	64%
Unterbrechungsfreie Stromversorgung	91%	3%	6%	17%	7%	77%	8%	2%	91%
Klimatisierung	83%	3%	13%	12%	3%	85%			
Rückrufautomatik bei Modemzugriff	47%	4%	49%	20%	2%	78%	21%	3%	77%
Reserve-Netzzugang (IT/TK) zur Ausfallüberbrückung	55%	9%	36%	20%	3%	77%	13%	1%	86%

Tabelle 19: Realisierte und geplante Sicherheitsmaßnahmen

Basis: Ø 144 Antworten (Server), Ø 131 (Clients), Ø 124 (mob. Ger.)

Abb. 20). Zur allgemeinen Information über ISi nutzen die Teilnehmer übrigens vor allem die Mailing-Listen von BSI und Heise vor Bugtraq, CERT CC und Bruce Schneiers Cryptogram.

Als wichtigste Komponenten im Security Management nannten die Teilnehmer eine zentrale Überwachung der Sicherheitssysteme (für 62 % „sehr wichtig", 36 % „wichtig"), eine plattformübergreifende Benutzerverwaltung (56 %/38 %), das Alarm- und Eskalationssystem (42 %/51 %) sowie Virtual Private Networks (VPN, 45 %/39 %). Danach folgen Intrusion Detection, Single Sign-on, Internet-Missbrauchs-Überwachung und Public Key Infrastructure (PKI).

Content Security

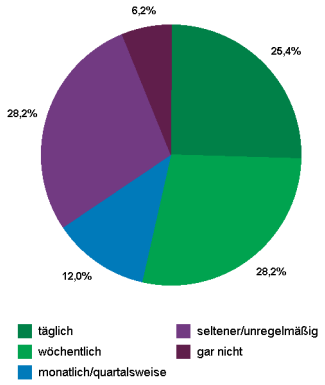
Die Abwehr von Malware zeigt bei den Befragten – wenig überraschend – einen enormen Realisierungsgrad auf allen Ebenen, wenngleich bei mobilen Systemen noch ein deutlicher Rückstand besteht. Auch Online-Virenwächter auf PCs liegen neuerdings hoch im Kurs: 52 % der Teilnehmer betreiben solche Dienste (2002 waren es nur 16 %). 37 % halten für nähere Analysen eine isolierte Testumgebung bereit. Prüfsummenprogramme scheinen jedoch völlig aus der Mode gekommen zu sein und sind nur noch bei 7 % vorhanden.

Die mittlere Update-Frequenz von Viren-Mustern beträgt bei Gateways und Serversystemen rund 21 Stunden; auf Desktops (unter Auslassung eines einzelnen Ausreißerwerts) erfolgt das Update im Mittel alle 30 Stunden, auf mobilen Systemen alle 39 Stunden. Die Angaben gehen jedoch weit auseinander und reichen von „in Echtzeit" bis hin zu „einmal in der Woche". Die häufigste Nennung lautet „täglich" und wurde bei Endgeräten von etwa der Hälfte der Befragten geäußert, bei Serversystemen von etwa 40 %.

Weniger dramatisch als die oftmals publizierten Zahlen vermuten ließen, zeigte sich die Spam-Flut bei den Teilnehmern. Obwohl die Systeme zur Abwehr unerwünschter E-Mails noch längst nicht vollständig realisiert sind (vgl. Tab. 19), liegt der Spam-Anteil im Mittel bei einem knappen Viertel – zwei Fünftel der Befragten haben unter 15 % Spam-Anteil, nur jeder Siebte erhält mehr als 50 % Spam (vgl. Abb. 21). Die weitaus meisten dieser Angaben beruhen zwar auf Schätzungen: Nur 12 % der Teilnehmer *ermitteln* den tatsächlichen Spam-Anteil. Angesichts der „Nervigkeit" des Spam-Phänomens dürften Schätzungen im Zweifel aber eher zu hoch als zu niedrig ausfallen.

Verschlüsselung & Signaturen

Die Bereitschaft, E-Mails zu chiffrieren, sofern ein Krypto-Schlüssel des Empfängers vorliegt, ist im Vergleich zur vorigen Studie leicht gestiegen: 47 % der Befragten würden dann zumindest sensitive Nachrichten verschlüsseln (+3 Prozentpunkte), 12 % die externe Kommunikation (-1 Prozentpunkt), 6 % alle Nachrichten (+2 Prozentpunkte). Auch dieses Jahr lag dabei OpenPGP als verwendeter Standard klar vor S/MIME – und zwar wiederum im Verhältnis 2:1.



Basis: 145 Antworten

Abbildung 20: Prüfintervall passiver Kanäle zu Sicherheits-Updates

Weiterhin eine Seltenheit sind elektronische Signaturen: Nur rund ein Viertel der Teilnehmer nutzt sie zur Authentifizierung interner Kommunikation, 22 % im B2B-Segment – Haupteinsatzort ist dabei der Webserver (vgl. Tab. 20). Betrachtet man die vorhandene und geplante Infrastruktur, so zeigen sich auch hier keine großen Veränderungen: Wo überhaupt signiert wird, sind Software-Lösungen deutlich dominant, Chipkarten und Hardware-Token folgen mit deutlichem Abstand und geringerem Realisierungsgrad. Höherwertige Chipkarten-Terminals mit gesicherter PIN-Eingabe oder eigenem Display sowie höherwertige Signaturen gemäß Signaturgesetz bleiben nach wie vor die große Ausnahme.

In Sachen Public Key Infrastructure hat sich mit knapp 29 % der

Elektr./dig. Signaturen sind im Einsatz bei...	E-Mail	WWW (SSL)	Applikationen	nein
zur Authentifizierung interner Kommunikation?	13%	12%	9%	75%
bei B2B-Kommunikation?	9%	13%	8%	78%
bei B2C-Kommunikation?	5%	13%	5%	83%
im E-Government?	5%	3%	1%	92%

Basis: Ø 145 Antworten

Tabelle 20: Einsatz elektronischer Signaturen

Logfile-Auswertung bei ... erfolgt...	min. 2x pro Woche	seltener, aber regelmäßig	anlass-bezogen	keine Auswertung/ Protokollierung
Antivirus-Lösungen	40%	20%	33%	7%
Firewall(s)	36%	22%	35%	7%
Netzkomponenten (Router, Switches etc.)	14%	17%	43%	25%
Betriebssysteme	12%	23%	48%	17%
Web-/E-Commerce-Applikationen	11%	22%	32%	35%

Basis: Ø 127 Antworten

Tabelle 21: Auswertung von Logfiles an der Schnittstelle zum Internet

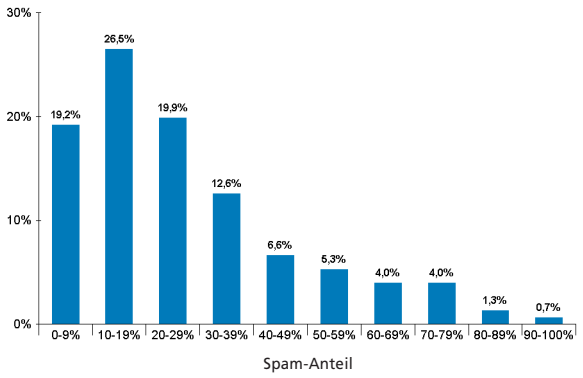


Abbildung 21: Anteil von Spam an der eingehenden E-Mail

Basis: 151 Antworten

Anteil der Teilnehmer wiederum etwas erhöht, die bereits eine PKI nutzen. Haupteinsatzbereiche bleiben dabei E-Mail-Verschlüsselung, VPN und die Sicherung von Telearbeitsplätzen und Remote Access sowie ferner Datei-Verschlüsselung; mit geringerem aktuellen Umsetzungsgrad folgen der Schutz von Web-Zugriffen sowie Zugriffsrechteverwaltung und Single-Sign-on.

Logfile-Auswertung

Eine regelmäßige Auswertung von Protokollen an der Schnittstelle zum Internet führen 60 % für (zentrale) Anti-Virus-Logfiles durch, 58 % tun dies bei Firewalls – Intranet-Firewalls und -Virenscanner werden zwar etwas seltener, aber dennoch von den meisten Teilnehmern regelmäßig geprüft. Für Netzwerkkomponenten und Betriebssysteme erfolgt die Auswertung hingegen überwiegend anlassbezogen (s. Tab. 21). Bedenklich erscheint, dass mehr als ein Drittel der Befragten an der Netzwerkgrenze keine Protokollierung oder Logfile-Auswertung von Web- und E-Commerce-Applikationen vornimmt.

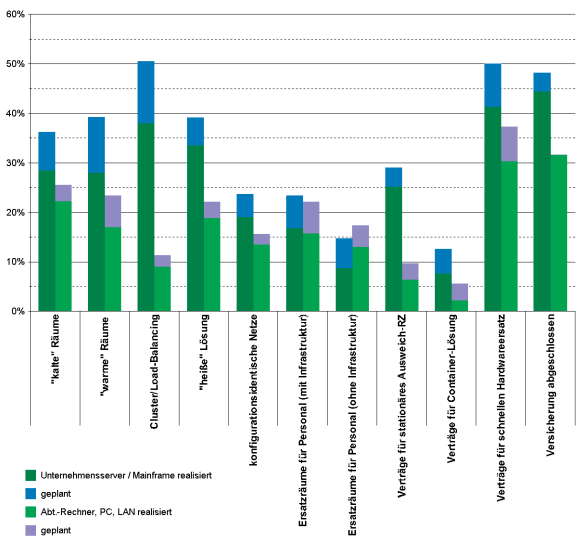


Abbildung 22: Bereitstellungen für längere Ausfälle bei Unternehmensservern und Mainframes

Basis: 148 Antworten

Notfallvorsorge

Die für Katastrophenfälle wesentliche räumliche Trennung wichtiger IT-Komponenten vollziehen die Teilnehmer vor allem durch Nutzung separater Gebäude: Beispielsweise haben 49 % ihr Auslagerungsarchiv in einem anderen Gebäude untergebracht, 20 % zumindest in einem getrennten Brandabschnitt, nur 14 % hingegen bei einem Kooperationspartner oder externen Dienstleister – 17 % haben keinerlei räumliche Trennung vorgesehen. Bei Robotersystemen, gespiegelten Daten und zusätzlichen Rechnern oder Clustern zeigte sich seltener eine räumliche Trennung (bei insges. 48–61 %), allerdings mit derselben Priorität der hierfür genutzten Örtlichkeiten.

Für längere Ausfälle haben rund 72 % bereits eine Vorsorgemaßnahme für Unternehmensserver oder Mainframes realisiert, 56 % auch für Abteilungsserver und PCs. Der größte Anteil von bereits umgesetzten Maßnahmen ist dabei jeweils der Abschluss einer entsprechenden Versicherung, gefolgt von Verträgen über die schnelle Lieferung von Hardware. Platz Drei unterscheidet sich hingegen: Für die zentrale IT wurden hier Cluster oder Load-Balancing-Lösungen eingerichtet, für Abteilungssysteme „kalte" Räume bereitgestellt (also Ersatzräume ohne Equipment).

Bezieht man geplante, aber noch nicht umgesetzte Vorsorgemaßnahmen mit ein, so stehen Cluster und Ersatzlieferungen für die zentrale IT auf Rang Eins und auch bei den Abteilungssystemen „überholen" Ersatzbeschaffungsvereinbarungen die klassische Ausfall-Versicherung (vgl. Abb. 22). Von 32 Teilnehmern, die auf unsere Frage nach der Inanspruchnahme eines Recovery-Vertrags geantwortet haben, mussten übrigens gleich zwei diese tatsächlich schon mehrfach nutzen – die anderen 30 blieben bislang jedoch vom „Ernstfall" verschont.

Bei der Notfall-Dokumentation dominiert nach wie vor das manuelle Handbuch, das bei 50 % der Teilnehmer im Einsatz ist (weitere 28 % haben es in Arbeit oder geplant). Der Anteil genutzter oder in Arbeit befindlicher Online-Anwendungen oder online-gestützer Handbücher ist zwar im Vergleich zur vorigen Studie um sechs beziehungsweise vier Prozentpunkte gestiegen, bleibt aber dennoch deutlich hinter den klassischen Systemen zurück, selbst wenn man jeweils das Fünftel der Befragten hinzuzählt, die ein entsprechendes Produkt für die Zukunft planen. Die Aktualisierung der Dokumentation erfolgt bei 87 % der Befragten nur anlassbezogen, bei 8 % niemals. Lediglich 5 % gaben an, dieses wichtige Dokument regelmäßig auf dem Laufenden zu halten. ■

Die Auswertung der /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.

InfoZoom®

Impressum

Sonderdruck aus <kes> – Die Zeitschrift für Informations-Sicherheit Nr. 2004#4 und 2004#5
für Microsoft Deutschland GmbH, Konrad-Zuse-Straße 1, 85716 Unterschleißheim

ISSN 1611-440X

Telefon +49 6725 9304-0, Telefax +49 6725 5994, E-Mail: info@secumedia.de
Web: www.kes.info
Verantwortlich i.S.d.P.: Norbert Luckhardt
Satz und Layout: Black Art Werbestudio Schnaas und Schweitzer, 55413 Weiler
Druck: Schmidt & more Drucktechnik, 65462 Ginsheim-Gustavsburg
Printed in Germany.

Für Ihre Sicherheit gibt es nicht die eine Lösung.

Aber eine Adresse, die Sie auf dem Laufenden hält.

Gehen Sie auf **www.microsoft.com/germany/security/isi** und bleiben Sie in Sachen Sicherheit immer up to date – mit stets aktuellen Informationen, Weiterbildungsangeboten, Leitfäden und Tools:

Microsoft® Windows® XP Service Pack 2 Installieren Sie das kostenlose Update für den größtmöglichen Schutz vor Viren, Würmern und anderen Angriffen auf PCs.

+ Kostenloser Sicherheitscheck für den Mittelstand Downloaden Sie unser Tool zur Risikoeinschätzung Ihrer IT-Infrastruktur und identifizieren Sie bestehende oder potenzielle Sicherheitsprobleme.

+ Kostenlose Informationsmedien Abonnieren Sie unseren Sicherheitsbenachrichtigungsdienst für aktuelle Sicherheitswarnungen und bestellen Sie unseren Newsletter für Tipps und Leitfäden zur Informationssicherheit.

+ Kostenlose Tools Nutzen Sie die Microsoft Software Update Services und den Microsoft Baseline Security Analyzer, um ein hohes Sicherheitsniveau Ihrer Systeme zu gewährleisten und regelmäßig zu überprüfen.

Der Weg zu optimaler Informationssicherheit verlangt Aktualität und Kontinuität – wir sind Ihnen dabei ein zuverlässiger Partner. Nutzen Sie jetzt die Angebote und Sicherheitslösungen in unserem Security Guidance Center auf
www.microsoft.com/germany/security/isi

Was Sie über **Phishing** wissen sollten:
http://www.microsoft.com/germany/security/phishing

Microsoft