<kes>
Die Zeitschrift für Informations-Sicherheit

special

Auszüge aus
<kes> 2006#4/6

Sonderdruck für Microsoft®

Lagebericht zur Informations-Sicherheit

SecuMedia

Vertrauen Sie uns

Als Hauptsponsor der <kes>/Microsoft-Sicherheitsstudie 2006 freuen wir uns, Ihnen heute diesen Sonderdruck zu Ihrer Information überreichen zu dürfen.

Sicherheit hat bei Microsoft – spätestens seit Beginn des Jahres 2002 – höchste Priorität. Damals war es Bill Gates selbst, der den Gedanken des „Trustworthy Computing" einführte. Der Begriff stand und steht für eine langfristig angelegte Initiative, deren Ziel es ist, das Vertrauen in die Sicherheit und Zuverlässigkeit von Computern zu stärken. Für Microsoft ist „Trustworthy Computing" bis heute ein zentraler Grundsatz, an dem alle Mitarbeiter ihr gesamtes Handeln orientieren.

Die Initiative basiert auf vier Säulen: Sicherheit, Datenschutz, Zuverlässigkeit von Software, Diensten und Produkten sowie Integrität im geschäftlichen Handeln. Im Bereich der Sicherheit liegt der Fokus auf Technologie-Investitionen, auf Bereitstellung von kostenfreien technischen Leitfäden und Tools sowie Sicherheits-Benachrichtigungen und auf Partnerschaften mit der Industrie und Behörden.

Die vorliegende Studie enthält nun eine Reihe von interessanten Ansatzpunkten, in welchen Bereichen sich eine Investition in Informations-Sicherheit lohnt. Lassen Sie mich hier bitte drei Punkte hervorheben, die stark im Fokus unseres Handelns stehen.

Direkt zu Beginn dieses Lageberichts ist vom Risiko durch „Irrtum und Nachlässigkeit eigener Mitarbeiter" die Rede. Hier gibt die Initiative „Deutschland-sicher-im-Netz" einige Hilfestellungen. Die Initiative, die Microsoft zusammen mit 14 Partnern seit rund 20 Monaten betreibt, richtet sich sowohl an Privatanwender als auch an kleine und mittelständische Unternehmen. Unser Bestreben und das unserer Partner ist es, durch eine Vielzahl von Kampagnen und Aktionen ein Bewusstsein für Informations-Sicherheit zu schaffen.

Die Bedrohung durch Malware hat erfreulicherweise wieder leicht nachgelassen. Diese Entwicklung ist auch damit zu erklären, dass Microsoft am 13. Januar 2005 die erste Version des „Windows-Tools zum Entfernen bösartiger Software" – engl.: „Windows Malicious Software Removal Tool (MSRT)" – herausgebracht hat. In den vergangenen 15 Monaten konnte mithilfe dieses Tools in 16 Millionen Fällen schädliche Software von rund 5,7 Millionen einzelnen Computern entfernt werden, darunter ausgewählte Backdoor-Trojaner und Rootkits. Entscheiden Sie selbst, ob dieses kostenfreie und regelmäßig aktualisierte Tool zumindest ein Basis-Schutz für die tägliche Arbeit am Computer (im Firmennetzwerk) ist, der selbstverständlich kein Ersatz für eine Antiviren-Lösung sein soll und kann.

Der Tendenz, dass Investitionen für mehr Informations-Sicherheit noch immer häufig wegen fehlender Geldmittel unterbleiben, versuchen wir bereits seit Jahren mit kostenfreien Tools, Leitfäden und Trainings zu begegnen. Es freut uns außerordentlich, dass unser diesbezügliches Angebot verstärkt angenommen wird, was die deutliche Zunahme der Abonnenten von E-Mail-Benachrichtigung zu Bulletins und Sicherheitsempfehlungen belegt.

Und letztlich unterstützen definierte Prozesse und Services Sie und uns in dem Bestreben, das Vertrauen in Computer zu stärken und Informations-Sicherheit zu gewährleisten. Hier spielen vor allem Prozesse zur Sicherstellung einer Kunden-Kommunikation im Krisenfall sowie der „Security Development Lifecycle (SDL)" – ein QA-Prozess, der den gesamten Lebenszyklus unserer Software begleitet – eine entscheidende Rolle.

Vertrauen Sie uns!

Thomas Mörgenthaler
Security Marketing Manager
Microsoft Deutschland GmbH

Weitere Informationen zu allen hier angesprochenen Themen finden Sie unter:
www.microsoft.com/germany/sicherheit/
www.sicher-im-netz.de

Unsere Geschäftskunden-Betreuung erreichen Sie unter:
Tel.: 01805 67 23 30 (0,12 Euro pro Min., deutschlandweit)
E-Mail: BtoB@microsoft.com

Lagebericht zur Informations-Sicherheit

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

Die vertrauensvollen und umfassenden Antworten der Teilnehmer und die Unterstützung der Sponsoren und Partner machen diese Studie möglich – dafür zunächst vielmals Dankeschön! In diesem Jahr sind 163 ausgefüllte Fragebögen eingegangen. Dabei war auch eine erfreulich hohe Beteiligung durch kleine und mittelständische Unternehmen (KMU) mit bis zu 500 Mitarbeitern zu verzeichnen (vgl. Abschnitt „Teilnehmer“ auf S. 21). Einige Kernpunkte der <kes>/Microsoft-Sicherheitsstudie 2006 lauten:

_____ „Irrtum und Nachlässigkeit eigener Mitarbeiter“ belegt einen wiedererstarkten ersten Platz – technische Mängel und Defekte steigen in der Bedeutung.

_____ Trendwende bei der Malware? Weniger mittlere bis größere Schäden, weniger Vorfälle und bei den Prognosen geringere Zuwachsraten könnten auf eine Entspannung hindeuten. Malware bleibt aber dennoch eine gefährliche Bedrohung und dominiert bei den größten Schadenereignissen.

_____ Verlust und Diebstahl mobiler Systeme sind die häufigste Ursache für Vertraulichkeitsbrüche – jeder sechste Befragte berichtet zudem von unbefugten Zugriffen auf schutzwürdige Daten durch klassischen Einbruch.

_____ Deutlich bessere Einschätzung der WLAN-Sicherheit, aber weiterhin unbefriedigende Sicherheitslage bei mobilen Endgeräten (Notebooks, PDAs, ...).

_____ Fehlende Geldmittel bleiben größtes Hindernis für mehr Informations-Sicherheit – größten Zuwachs hat die Klage, dass Anwendungen nicht für Sicherheitsmaßnahmen vorbereitet sind.

Risikosituation

Entsprechend der Bedeutung einer korrekten Bewertung von Gefahrenbereichen für die Sicherheit des eigenen Hauses steht diese Thematik sowohl in Fragebogen als auch in der Auswertung unserer Studie immer an erster Stelle. Die Teilnehmer wurden hierzu um Vergabe von insgesamt sechs Prioritätspunkten gebeten, wobei jeweils bis zu drei Punkte auf eine Gefährdung kumuliert werden konnten.

Auch 2006 landete hierbei „Irrtum und Nachlässigkeit eigener

	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	progn. Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,52	2	1,17	1	49%
Malware (Viren, Würmer, Troj. Pferde,...)	2	1,06	1	1,51	4	35%
Software-Mängel-/Defekte	3	0,60	5	0,58	2	46%
Hardware-Mängel-/Defekte	4	0,55	6	0,34	3	45%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	5	0,50	3	0,63	7	12%
unbeabsichtigte Fehler von Externen	6	0,39	7	0,32	5	30%
Hacking (Vandalismus, Probing, Missbrauch,...)	7	0,37	4	0,59	8	12%
Mängel der Dokumentation	8	0,27	9	0,27	6	20%
Manipulation zum Zweck der Bereicherung	9	0,26	8	0,29	10	11%
höhere Gewalt (Feuer, Wasser,...)	10	0,21	11	0,03	9	12%
Sabotage (inkl. DoS)	11	0,17	10	0,22	11	10%
Sonstiges	12	0,02	12	0,00	12	3%

Basis: 155 Antworten (Bedeutung), Ø 130 (Prognose), Ø 127 (Schäden)

Tabelle 1: Bedeutung der verschiedenen Gefahrenbereiche

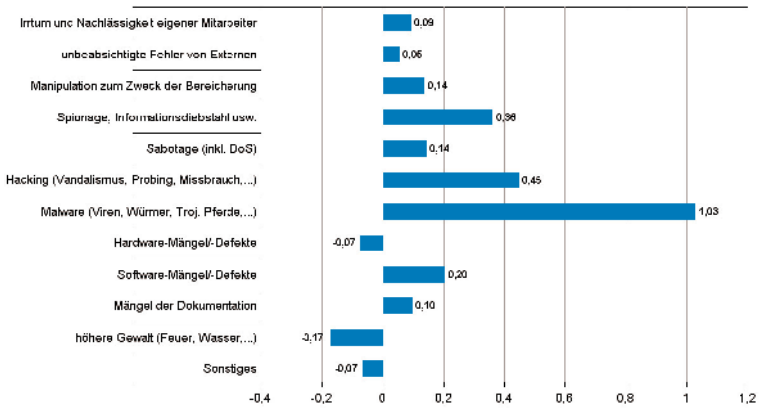


Abbildung 1: Prognostizierte Veränderung der Bedeutung der Gefahrenbereiche (Zusammenfassung)

Basis: Ø 130 Antworten

Mitarbeiter" auf Rang Eins – wie schon seit Beginn der <kes>-Sicherheitsstudien und entgegen allen Prognosen, die hier seit einigen Jahren eine Wachablösung durch die Malware vorhersagen (s. Tab 1). Im Gegenteil ist der Abstand sogar wieder deutlich gewachsen, sodass hier – im Lichte verschiedener analoger Beobachtungen bei anderen Indikatoren (s. u.) – eine Trendwende möglich erscheint.

Dennoch: Klar an zweiter Stelle priorisiert ist und bleibt die Malware. Technische Defekte und Qulitätsmängel bei Hard- und Software liegen mit deutlichem Rückstand auf den Rängen Drei und Vier und haben Spionage (sinkt von Rang 3 auf 5) und Hacking (von 5 auf 7) im Vergleich zur Bewertung von 2004 zurückgedrängt. Die absolute Priorität für Softwaremängel hat sich dabei kaum verändert, die Bedeutung von Hardwarefehlern jedoch stark erhöht: Mit einem Plus von 0,15 Punkten erzielte dieser Bereich das größte Wachstum. Gesteigerte Beachtung haben auch „Mängel der Dokumentation" erfahren und liegen jetzt auf Rang 8.

Der größte Rückgang im Vergleich zu 2004 ist bei der Malware zu verbuchen (–0,28 Punkte). Auch die Zahl der Teilnehmer, die hier überhaupt ein Kreuz gemacht haben, sank drastisch: Hatten vor zwei Jahren noch 81 % der Befragten mindestens einen Punkt ihrer „Prioritäts-Ressourcen" hierfür aufgewandt, so waren dies heuer nur noch 66 %. „Irrtum und Nachlässigkeit eigener Mitarbeiter" konnte indes einen Zuwachs von 7 Prozentpunkten verbuchen und genießt nun priorisierte Aufmerksamkeit von 90 % der Teilnehmer.

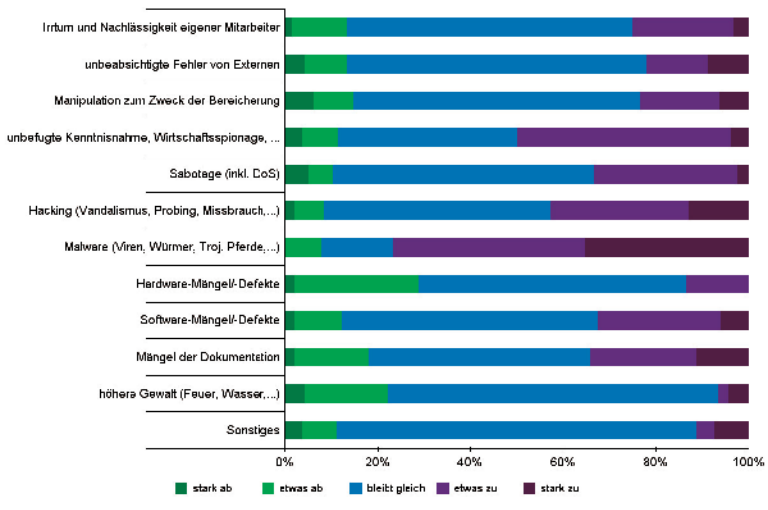


Abbildung 2: Prognosen zur Veränderung der Bedeutung von Gefahrenbereichen (Details)

Basis: Ø 130 Antworten

Hinterfragt man die Prognosen von 2004, so bleibt die Kategorie der Angriffe in ihrer aktuellen Bedeutung hinter den geäußerten schweren Befürchtungen erneut deutlich zurück. Die erhoffte leichte Entspannung der Lage bei „unbeabsichtigten Fehlern von Externen" und Hardwareproblemen blieb aus, im Gegenteil erhielten sogar beide Bereiche dieses Jahr mehr Bedeutung zugebilligt. Lediglich „höhere Gewalt" verlor tatsächlich etwas an Gewicht, wenngleich deutlich weniger als vorhergesagt. Als nahezu perfekt erwiesen sich die Erwartungen an steigende Probleme mit Software und Manipulationen zum Zwecke der Bereicherung.

Betrachtet man die neuen Prognosen, so zeigt sich einerseits ein gewohntes Bild (vgl. Abb. 1): Bei Malware, Spionage und Hacking wird das stärkste Wachstum befürchtet, gefolgt von Softwareproblemen und Betrügereien – die Hoffnungen in zukünftige stabilere Hardware sowie weniger Probleme durch höhere Gewalt sind ungebrochen. Vergleicht man hingegen die Stärke der erwarteten Änderungen und die Abweichungen der Prognosen von 2004 und 2006, so zeigen sich dieses Jahr moderatere Erwartungen, die hin zu mehr Ausgleich – und so vermutlich realistischeren Einschätzungen – tendieren: Die Prognosen für Unfälle (menschliches und technisches Versagen) liegen durch die Bank über den vor zwei Jahren vorhergesagten Werten, alle Angriffe erzielen schwächere Anstiege als in der Prognose von 2004. Am deutlichsten zeigt sich das erneut bei der Malware: Während vor zwei Jahren noch 91 % der Befragten einen Anstieg erwarteten (59 % stark, 32 % etwas), waren es jetzt „nur" noch 73 % (39 % stark, 34 % etwas – vgl. Abb. 2).

Dieses Bild kommt der Lageentwicklung also zumindest näher, die sich in der alternativen Zusammenfassung der Gefahrenbereiche zu Unfällen und Angriffen zeigt (Tab. 2),

wenngleich die erwarteten Zuwachsraten bei Attacken weiterhin der tatsächlich zu beobachtenden Bewertung zuwiderlaufen. Vergleicht man diese Tabelle mit den Werten von 2004, so zeigt sich nämlich eine gestiegene Bedeutung der Unfälle (jetzt 3,32 gegenüber 2,91 in 2004) gegenüber gesunkenen Prioritäten bei Angriffen (jetzt 2,35 vs. 2,70 in 2004).

Schadensstatistik

Diese Einschätzungen spiegeln sich dabei durchaus in den Angaben zu tatsächlich aufgetretenen „mittleren bis größeren Beeinträchtigungen“ (im Folgenden kurz als „Schäden“ bezeichnet) wider: Denn die Zahl der Befragten, die durch Unfälle zu Schaden kam (ohne höhere Gewalt), hat sich erhöht, während die Gruppe der durch Malware nennenswert Beeinträchtigten deutlich zurückging (jetzt 35 % gegenüber 54 % in 2004). Keine Verbesserung gab es hingegen bei gezielten Attacken, von denen weiterhin etwa ein Viertel der Teilnehmer (mit nennenswerten Folgen) betroffen war.

In den einzelnen Gefährdungen korrespondieren die meisten Schadenwerte mit der Rangfolge der zugebilligten Bedeutung (Priorität, s. Tab. 1). Dass Schäden durch Malware und Spionage dabei zwei Stufen „überbewertet“ sind, erscheint keineswegs unsinnig: Zum einen ist die Malware gerade erst von Rang 1 der Schäden (in 2004) zurückgefallen, zum anderen sind bei Vertraulichkeitsbrüchen (s. u.) sowohl eine hohe Dunkelziffer als auch drastische Auswirkungen zu erwarten, die eine besondere Vorsicht gerechtfertigt erscheinen lassen. Trotz der gestiegenen Beachtung in der Prioritätenliste noch immer etwas unterbewertet erscheint hingegen der Punkt „Dokumentationsmängel“: Hierdurch kam es bei deutlich mehr Teilnehmern zu tatsächlichen Schäden als durch das höher priorisierte Hacking. Insgesamt ergibt sich aber ein sehr konsistentes Bild mit erheblich geringeren Abweichungen als das 2004 der Fall war.

Bei der Freitextfrage nach dem größten Schadenereignis der vergangenen zwei Jahre dominiert die Malware allerdings immer noch: 34 % der Antworten gingen auf Viren und Würmer zurück. An zweiter Stelle landete – ebenfalls mit demselben Anteil wie schon 2004 – mit 13 % die Speicher-Technik. Sonstige Hardwareprobleme (ohne Speicher- und Netzwerk-HW) sorgten bei 10 % für den schlimmsten Schaden. Danach folgen gleichauf Software und Stromversorgung mit je 6 % und Angriffe (online wie offline zusammengenommen) mit 5 %, Netzwerktechnik 4% – immerhin 9 % der Antwortenden äußerten, es habe in den erfragten zwei Jahren kein hinreichend relevantes Schadensereignis gegeben. Der „durchschnittliche größte Vorfall“ schlug mit gut 100.000 € direkten und etwa 12.000 € Rekonstruktions-Kosten zu Buche und hat eine Ausfallzeit von 44 Std. nach sich gezogen – er war

	Priorität	Schäden min. 1 bei	Schäden Nennungen
Unfälle	**3,32**	**70%**	**259**
... menschliches Versagen	1,90	56%	115
... technisches Versagen	1,42	63%	144
Angriffe	**2,35**	**43%**	**102**
... ungezielt (Malware)	1,06	35%	49
... gezielt (Spionage, Hacker, Sabotage usw.)	1,30	24%	53

Basis: s. Tab. 1

Tabelle 2: Alternative Zusammenfassung der Gefahrenbereiche

damit deutlich teurer als in der vorigen Studie (allerdings basieren diese Mittelwerte erneut nur auf den Angaben von knapp 50 bzw. 73 Teilnehmern, die hierzu Angaben gemacht haben, einzelne große Werte haben daher starke Auswirkung auf den Durchschnitt).

Malware

Die Zahl der Befragten, die mindestens einen Malware-Vorfall zu vermelden hatten, unterbietet mit 72 % sogar den Wert der vorletzten Studie von 2002 (74 %, 2004: 88 %). Nimmt man die neu eingeführte Kategorie „Spyware“ hinzu, waren 78 % der Teilnehmer von mindestens einem Vorfall betroffen. Zwar gab es auch jetzt wieder Organisationen, die mehr Probleme als im Vorjahr hatten (vgl. Tab. 3), in drei Kategorien überwiegen aber – teils sehr deutlich – die sinkenden Tendenzen und auch insgesamt war in allen Malware-Kategorien dieses Jahr der Anteil der von Malware-Vorfällen Betroffenen geringer als 2004. Besonders deutlich war dieser Rückgang mit –

	Vorfälle ja, bei	Tendenz gestiegen	Tendenz gesunken
File-Viren	47%	42%	58%
Boot-Viren	18%	24%	76%
Makro-Viren	27%	30%	70%
Würmer	62%	53%	47%
Troj. Pferde / Backdoors	51%	54%	46%
Spyware	57%	57%	43%

Basis: Ø 107 Antworten (Vorfälle), Ø 67 (Tendenz)

Tabelle 3: Malware-Vorfälle

	häufig	selten	nie	Bedeutung*
E-Mail	53%	33%	14%	1,92
Internet-Download	28%	54%	18%	1,38
WWW-Seiten (aktive Inhalte)	21%	47%	32%	1,11
Internet (autom. Verbreitung)	21%	42%	36%	1,06
unbekannte Herkunft	11%	53%	36%	0,86
Datenträger (CD-ROM, Diskette, ...)	7%	56%	38%	0,76
internes Netz	7%	29%	64%	0,49

Basis: Ø 128 Antworten

* errechnet aus: häufig = 3, selten = 1, nie = 0

Tabelle 4: Infektionswege von Malware

	Ausfallzeit		Kosten	
	Durch-schnitt	max.	Durch-schnitt	max.
Virus-/Wurm-Infektion	47,8	1000	18.324	500.000
Spyware-Befall	16,4	300	3.372	30.000
Fehlalarm (unbegründete Fehlermeldung)	24,6	500	3.367	60.000
Hoax (unbegründete Warnung)	35,7	600	2.223	36.000
(erfolgreicher) Online-Angriff	3,1	25	5.600	50.000
Phishing-Vorfall	1,8	20	980	7.000

Basis: Ø 64 Antworten (Viren), 28 (restl. Vorfälle)

Tabelle 5: Aufwand durch Sicherheitsvorfälle

unbefugter Zugriff durch	ja (sicher)	vermutlich ja	vermutlich nein	nein (sicher)
Verlust oder Diebstahl mobiler Systeme	27%	9%	18%	46%
Einbruch in Gebäude	17%	1%	18%	64%
Missbrauch/Weitergabe durch Berechtigte	3%	15%	66%	16%
Verlust oder Diebstahl von Speichermedien	7%	5%	32%	56%
Abhören von Kommunikation	1%	8%	76%	15%
Online-Angriff (Hacking, Systemeinbruch...)	2%	4%	59%	34%
sonstiger Weg	2%	1%	11%	5%

Basis: Ø 154 Antworten

Tabelle 6: Vertraulichkeitsbrüche

	ja, bei
Strafanzeige gegen Verursacher	38%
Disziplinarmaßnahmen im Hause	26%
missbräuchliche Verwendung von Daten durch Dritte	25%
Imageschaden	17%
(externe) Sanktionen gegenüber dem Haus oder einem Mitarbeiter	11%
verlorene Kunden oder Aufträge	10%
Sonstiges	15%

Basis: Ø 100 Antworten

Tabelle 7: Konsequenzen aus Vertraulichkeitsbrüchen

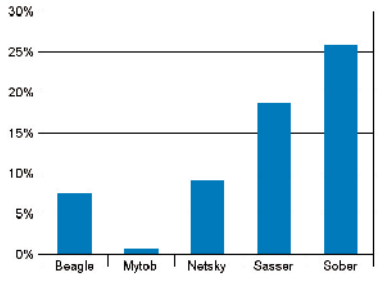


Abbildung 3: Nennenswerte Beeinträchtigung durch „Top-5"-Malware Basis: Ø 133 Antworten

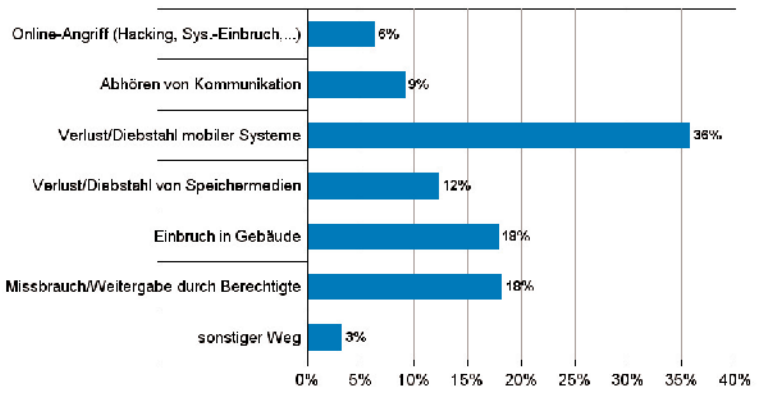


Abbildung 4: Sicher oder vermutlich durch Vetraulichkeitsbrüche Betroffene (Zusammenfassung zu Tab. 6)

Basis: Ø 154 Antworten

24 Prozentpunkten bei Makro-Viren und –22 Punkten bei Würmern.

Weniger Probleme hat auch die meistverbreitete Malware („Top-5", s. Abb. 3) verursacht: Hauptärgernis war hier in den vergangenen Jahren Sober, der bei 26 % der Befragten für nennenswerte Beeinträchtigungen gesorgt hat, Rang 2 belegt Sasser mit 19 % – die anderen drei ausgewählten Malwares ließen jeweils über 90 % der Teilnehmer „völlig kalt". Vor zwei Jahren sah das noch anders aus, als die Top-5 im Mittel 21 % der Teilnehmer „erwischt" haben (2006: 12 %).

Zieht man in Erwägung, dass die mittlere Häufigkeit von Malware-Infektionen ungefähr gleich geblieben ist (die allerdings in beiden Studien auf einer deutlich verringerten Stichprobe beruht) und zudem bei den Maximalschäden weiterhin ein gutes Drittel durch Viren und Würmer verursacht wurden, so ist sicherlich keine Entwarnung zu verkünden. Dennoch deuten die vorliegenden Daten in der Summe darauf hin, dass der Scheitelpunkt der Malware-Probleme überwunden sein könnte.

Keine Überraschungen gab es indes bei den Infektionswegen (s. Tab. 4): Klar vorne liegt weiterhin die E-Mail, gefolgt vom Internet. Eine auffällige Steigerung hat die – früher nachrangige – Kategorie „Infektion durch aktive Inhalte" erfahren, die sich auf den dritten Platz vorgekämpft hat.

Kosten/Aufwand bei Vorfällen

Wie schon angesprochen zeigte sich die mittlere Zahl von Viren-/Wurm-Infektionen mit jährlich 38 auf dem Niveau der vorigen Studie – lässt man die Maximalmeldung von 1000 Infektionen außer Acht, so bleibt noch immer ein Durchschnitt von 28. Ähnliches gilt für das Auftreten von Hoaxes (unbegründete Warnungen), die im Mittel 42 Mal zu be-

arbeiten waren (ohne Ausreißer: 12). Gleich drei Befragte schätzten das Auftreten technischer Fehlalarme pro Jahr auf 1000 – das ergäbe einen Schnitt von 59, ohne diese Maxima bleiben 7. Erstmals haben wir zudem nach Spyware-Befall, Phishing und erfolgreichen Online-Attacken gefragt: Nach Eliminierung der Ausreißerwerte bleibt ein Mittel von 22 Spyware- und 17 Phishing-Vorfällen. Erfolgreiche Online-Angriffe haben nur 8 von 33 Teilnehmern beklagt, die hierzu überhaupt Angaben gemacht haben.

Auch mit Schätz- oder Erfahrungswerten zu Ausfallzeit und Kosten taten sich die meisten Befragten schwer (vgl. Tab. 5) – stärkere Schwankungen durch die konkrete Zusammensetzung der Stichprobe sind somit leicht möglich. Die durchschnittlichen Kosten einer Viren-Infektion lagen heuer mit gut 18.000 € deutlich unter den Werten der vorigen Studien (ca. 26.000 €), die Angaben zu Fehlalarmen und Hoaxes über denen von 2004, aber deutlich unter den Werten von 2002. Die beste Basis zeigt hierbei die mittlere Ausfallzeit bei Viren-Infektionen, zu der immerhin 75 Teilnehmer einen Beitrag leisten konnten: Hier setzt der Mittelwert von knapp 48 Stunden den Trend zu kürzeren Ausfällen fort (2004: 54 Std., 2002: 94 Std.).

Vertraulichkeitsbrüche

Umfassende Angaben erhielten wir auf die neue Frage zum Zugriff Unbefugter auf schutzwürdige Daten in den zurückliegenden zwei Jahren. Hier erwiesen sich die „klassischen" Risiken des physischen Verlusts und

Vielen Dank für freundliche Unterstützung unserer Studie

Für zusätzliche Anregungen und Hinweise bedanken wir uns beim Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie bei der Hans-Joachim Gaebert Unternehmensberatung. Weiterhin gilt unser Dank den Verbänden und Anwendervereinigungen, die den Fragebogen der Studie ihren Mitgliedern zugänglich machen, sowie schon jetzt allen Teilnehmern an der Befragung, die durch ihre wertvolle Mitarbeit ein sinnvolles Gesamtbild entstehen lassen.

Bei der Verbesserung der ISi behindern am meisten:	
Es fehlt an Geld	55%
Es fehlt an Bewusstsein bei den Mitarbeitern	52%
Es fehlt an Bewusstsein und Unterstützung im Top-Managment	45%
Es fehlt an Bewusstsein beim mittleren Management	37%
Es fehlen verfügbare und kompetente Mitarbeiter	32%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	31%
Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	29%
Die Kontrolle auf Einhaltung ist unzureichend	27%
Anwendungen sind nicht für ISi-Maßnahmen vorbereitet	25%
Die vorhandenen Konzepte werden nicht umgesetzt	22%
Es fehlen realisierbare (Teil-)Konzepte	19%
Es fehlen geeignete Methoden und Werkzeuge	16%
Es fehlen geeignete Produkte	13%
Es fehlt an praxisorientierten Sicherheitsberatern	8%
Sonstiges	5%
keine Hindernisse	3%

Tabelle 8: Hindernisse für bessere Informations-Sicherheit

Basis: 158 Antworten

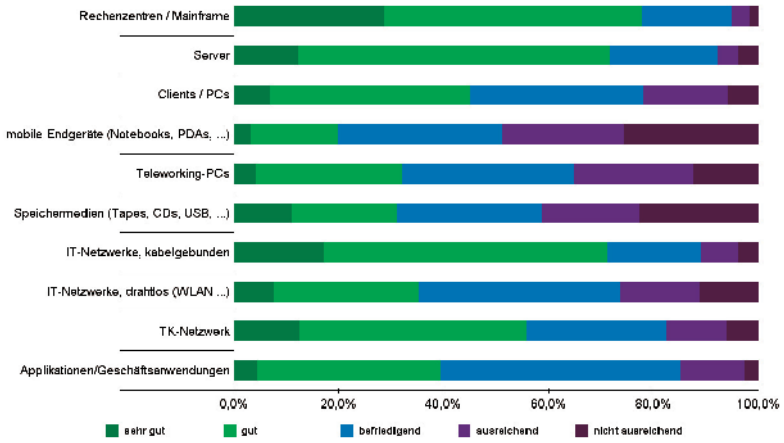


Abbildung 5: Einschätzung der Sicherheit

Basis: Ø 138 Antworten

Diebstahls sowie der unstatthaften Weitergabe oder Verwendung durch Berechtigte als größte Lecks (s. Tab. 6). Unliebsame Klarheit bestand bei 27% über verschwundene mobile Systeme und bei 17% über erfolgreiche Einbrüche in Gebäude.

Abbildung 6: Stellenwert der Informations-Sicherheit beim Top-Management

Basis: 141 Antworten

Eine erwartungsgemäß höhere Unsicherheit zeigt sich bei missbräuchlicher Verwendung von Daten durch Berechtigte und bei den Online-Attacken. Dennoch vermuten nur relativ wenige Teilnehmer in Letzteren die Ursache für unbefugte Zugriffe.

Eine grafische Zusammenfassung zu gesicherten und vermutlichen Brüchen der Vertraulichkeit über die erfragten Wege liefert Abbildung 4. Fasst man die verschiedenen genannten Möglichkeiten zusammen, so ergibt sich, dass 43% der Befragten in den letzten Jahren vermutlich auf die eine oder andere Weise mindestens einen Vertraulichkeitsbruch erlitten haben – 31% hatten hierüber gesicherte Erkenntnisse, 28% wurden sogar (zumindest vermutlich) mehrfach Opfer von Vertraulichkeitsbrüchen. 47% vermuten hingegen, dass in ihrem Hause *keinerlei* unbefugte Zugriffe erfolgt sind, aber nur 4% sehen das als völlig zweifelsfrei an (dass die Werte der vermutlich Geschädigten und vermutlich nicht Betroffenen sich nicht auf 100% addieren, liegt an offen gelassenen Teilfragen, wodurch für die entsprechenden Teilnehmer keine Aussage über alle Zugriffswege möglich war).

Bei Folgen der Vertraulichkeitsbrüche haben wir sowohl nach Konsequenzen gefragt, die das betroffene Haus hinnehmen musste, als auch nach solchen, welche die Betroffenen veranlasst haben (s. Tab. 7). Mit 38% hat eine erhebliche Zahl der Befragten Strafanzeige gegen den (möglicherweise unbekannten) Verursacher gestellt – bei den „sicher" Betroffenen steigt dieser Anteil sogar auf 68%. Bei den „passiven" Konsequenzen zeigte sich eine nachvollziehbar hohe Unsicherheit: Längst nicht jeder, der weiß, dass ein unbefugter Zugriff auf Daten erfolgt ist, kann auch sagen, ob diese durch Dritte tatsächlich missbräuchlich verwendet wurden. Hier fiel die Zahl der Angaben dementsprechend gering aus, ein Viertel hatte jedoch offenbar konkrete Anhaltspunkte für Datenmissbrauch. Beschränkt man die Antworten auf die „sicher Betroffenen", so steigt dieser Anteil auf zwei Fünftel.

Sicherheitslage

Ein gewohntes Bild zeigte die Selbsteinschätzung zum Stand der Informations-Sicherheit (s. Abb. 5): Zentrale Systeme erhalten dabei klassisch bessere Noten als Clients und Endgeräte außerhalb des direkten Zugriffs durch die Administratoren. Die meisten Bereiche zeigen hier in etwa dieselben oder leicht verbesserte Werte wie in der vorigen Studie, mit zwei Ausnahmen: Deutlich verbessert hat sich die Einschätzung der WLAN-Sicherheit, die im Schnitt um eine halbe Notenstufe gestiegen ist. Nur noch 26% der Befragten sind

hier der Meinung, die Sicherheit sei nicht oder gerade eben ausreichend (2004: 47 %). Sogar noch etwas weiter verschlechtert hat sich hingegen die (ohnehin unbefriedigende) Einschätzung der Sicherheit mobiler Endgeräte, die erneut das Schlusslicht bildet: Während mit 49 % der Teilnehmer hier ungefähr genauso viele wie vor zwei Jahren eine nicht oder gerade eben ausreichende Sicherheit sehen, ging der Anteil derjenigen, die eine sehr gute oder gute Sicherheit umgesetzt haben, um vier Prozentpunkte zurück.

Erstmals dabei sind die Fragen nach der Sicherheit von Speichermedien und Geschäftsanwendungen. Letztere befinden sich laut Angaben der Teilnehmer in etwa auf dem Niveau der Client-Systeme. Eine ungewohnt breit gestreute Verteilung der Sicherheitseinschätzungen erhielten hingegen die Speichermedien: Von „sehr gut" bis „nicht ausreichend" sind alle Noten relativ stark vertreten – durch den hohen Anteil der schlechtesten Note erzielen die Medien insgesamt aber das zweitschlechteste Ergebnis.

Die Aussagen der Teilnehmer zum Stellenwert der Informations-Sicherheit (ISi) beim Top-Management lassen eine weitere Polarisierung vermuten (Abb. 6): Der Anteil derjenigen Manager, denen man attestiert, Sicherheit eher als lästiges Übel anzusehen, ist um drei Prozentpunkt auf 34 % gestiegen (2004: +1 Punkt). Auf der anderen Seite ist auch die Fraktion der klaren Befürworter gewachsen, die in Informations-Sicherheit einen Mehrwert sehen: mit jetzt 14 % ein deutlicher Anstieg gegenüber der vorigen Studie (2004: 8,5 %). Zusammen mit denjenigen, die in der ISi ein vorrangiges Ziel sehen, ist die gesamte „Pro"-Gruppe jedoch nun wieder geschrumpft, und zwar von knapp 39 % in 2004 auf jetzt 34 %.

Bei der Beschaffung spielen Sicherheitsaspekte heute eine gestärkte Rolle (Abb. 7): 39 % der Befragten sehen hierin ein Hauptkriterium (2004: 35 %), nur noch 12 % äußerten, Sicherheit sei dabei eher unbedeutend (2004: 17 %). 47 % der Studien-Teilnehmer gaben zudem an, dass ISi-Anforderungen als Voraussetzung zur Inbetriebnahme verifiziert würden. Unsicher ist man sich hingegen noch in Bezug auf Trusted Computing: 51 % sind noch unentschieden, ob sie künftig derartig ausgestattete Systeme bevorzugt einsetzen wollen – nur 8 % wissen das jetzt schon mit „Ja" zu beantworten, 41 % verneinen es.

Das größte Problem, das einer Verbesserung der Informations-Sicherheit entgegensteht (s. Tab. 8), bleiben fehlende Gelder: Mit 55 % der Befragten haben zwar sieben Prozentpunkte weniger „mangelnde Mittel" beklagt, aber die Spitzenposition ist unangefochten. Mit einem Abstand von nun allerdings nur noch drei Prozentpunkten folgen die Awareness-Kategorien in der altbekannten Reihenfolge, auch wenn das mittlere Management diesmal etwas bessere Noten erhält. Der deutlichste Zuwachs folgt in der zweiten Hälfte der Liste, wo mit heuer 25 % das Argument „Anwendungen sind nicht für ISi-Maßnahmen vorbereitet" acht Prozentpunkte zugelegt hat.

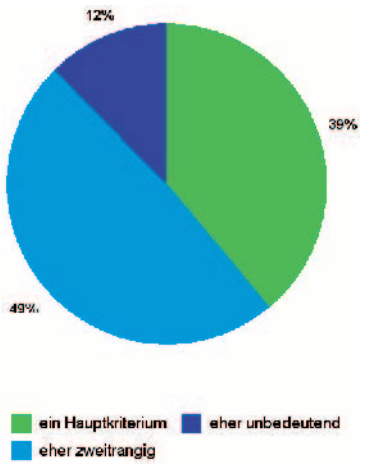


Abbildung 7: Bedeutung von Sicherheitsaspekten bei der Beschaffung von IT-Systemen

Basis: 162 Antworten

Konzepte

Erfreulicherweise gibt es erneut einen Zuwachs an Unternehmen und Behörden mit klaren Policies: Der Anteil der Teilnehmer mit schriftlich fixierter Strategie zur Informations-Sicherheit (ISi) stieg um vier Prozentpunkte auf jetzt 64 %. Bei den spezifischen Konzepten und Richtlinien waren ebenfalls wieder Steigerungen zu verzeichnen (s. Tab. 9). Die Bereitschaft, auch Maßnahmen festzuschreiben, ist hingegen weiter gesunken: Gaben 2002 noch 71 % der Befragten an, Sicherheits-Maßnahmen schriftlich zu fixieren, so sank dieser Anteil 2004 bereits auf 65 % und liegt nunmehr bei nur noch 57 %.

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

Tabelle 9: Strategien, Richtlinien und Konzepte

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

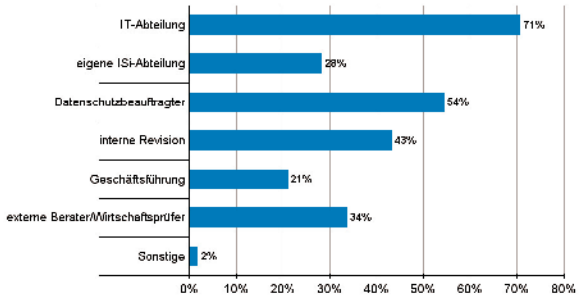


Abbildung 8: Wer prüft die Einhaltung vorgesehener ISi-Maßnahmen?

Basis: Ø 133 Antworten

Trotz dieser Zurückhaltung haben wieder erheblich mehr Studien-Teilnehmer als vor zwei Jahren eine Überprüfung der Einhaltung vorgesehener Maßnahmen bejaht: Nur 18 % verzichten auf derartige Prüfungen. Betrachtet man nur die befragten Häuser mit schriftlicher ISi-Policy, so bleiben sogar nur 5 %, die „blind" auf die Einhaltung der Maßnahmen vertrauen (dort liegt auch die generelle Bereitschaft für weitere schriftliche Festlegungen deutlich höher als im Durchschnitt – vgl. Tab. 9). Die Durchführung der Prüfungen obliegt dabei vorrangig den IT-Abteilungen (s. Abb. 8).

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

Der Anteil der Studienteilnehmer, in deren Häuser die private Nutzung des Internets am Arbeitsplatz generell *nicht* gestattet ist, stieg im Vergleich zu 2004 deutlich um zehn Prozentpunkte auf 23 %. Noch knapp zwei Drittel erlauben allen Mitarbeitern jedoch auch private Nutzung, 13 % haben teilweise Beschränkungen vorgesehen. Das Aufschalten privater Systeme ist hingegen überwiegend untersagt (Abb. 9). Die größte Toleranz gibt es hier bezüglich mobiler Speichermedien (32 %) und der Synchronisation privater Smartphones und PDAs mit dem Arbeits-PC (29 %). Eine technische Kontrolle dieser Beschränkungen erfolgt jedoch nur selten in umfassender Manier (s. Abb. 9).

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

Tabelle 10: Prüfung unter ISi-Aspekten

Basis: 154 Antworten

Ein Notfall-/Wiederanlaufkonzept liegt bei 78 % vor, allerdings nur bei knapp drei Viertel dieser Teilnehmer in schriftlicher Form (vgl. Abb. 10). Besondere Berücksichtigung erfahren dabei vor allem die spezifischen Anforderungen von Hardware-Ausfall und -Wiederbeschaffung (bei 79 % gegenüber 95 % in 2004) sowie physischen Einwirkungen (Brand, Naturkatastrophen, Terror – 77 %). Ferner berücksichtigt werden Software-Sicherheitsvorfälle (58 %), Malware-Epidemien (57 % gegenüber 74 % in 2004), das Zusammenbrechen externer Infrastrukturen (44 %), Hochverfügbarkeitsansprüche des E-Business (43 %) sowie Besonderheiten beim gezielten Eindringen von Einzeltätern (37 %) und Denial-of-Service-Angriffen (36 %).

Prüfungen

Eine fortdauernde Prüfung von Konzepten und Richtlinien auf ihre Eignung erfolgt weiterhin nur zögerlich: Wie schon vor zwei Jahren haben nur zwei Drittel aller Teilnehmer ein solches regelmäßiges Audit vorgesehen – von den Häusern mit schriftlicher ISi-Strategie allerdings immerhin 84 % (vgl. Tab. 9). Im Schnitt lag im Teilnehmerfeld die letzte solche Prüfung 8 Monate zurück und führte beim 69 % zur Aufdeckung von Schwachstellen. Zur Reichweite gaben 41 % an, dass alle geschäftskritischen Systeme geprüft wurden – 59 % prüften hingegen nur einzelne Systeme.

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

Im Rahmen sonstiger Prüfungen (z. B. durch interne Revision, Wirtschaftsprüfer, Berater oder Geschäftsführung) werden unter ISi-Aspekten vor allem Virenschutz (bei 76 %) und Berechtigungskonzept (71 %) geprüft; doch auch weitere Themenfelder werden hierbei verbreitet berücksichtigt (s. Tab. 10).

Inhouse vs. extern

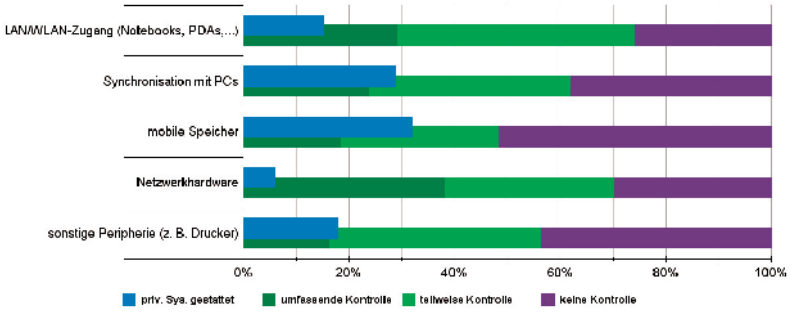
Einen expliziten Beauftragten für die Informations-Sicherheit haben von der gesamten Stichprobe

46 %, wobei größere Organisationen naheliegenderweise eher eine solche Position vorsehen: Von den Unternehmen und Behörden ab 500 Mitarbeitern haben 79 % einen ISi-Beauftragten, von kleinen und mittleren Unternehmen nur 29 %. Weitere vorhandene Positionen zeigt Tabelle 11. Ein eigenes Computer Emergency (CERT) oder Security Incident Response Team (CSIRT) unterhalten 21 % aller Teilnehmer – 31 % nutzen Dienste eines externen Teams, nur ein knappes Drittel davon allerdings auch kostenpflichtige Leistungen. Auch hier liegen größere Organisationen vorn: 29 % von ihnen haben ein eigenes Team, 42 % nutzen externe CERT/CSIRT-Dienste, wobei immerhin zwei Fünftel hierfür auch Geld ausgeben.

Der Anteil der Studien-Teilnehmer, die regelmäßig (8 %) oder gelegentlich (47 %) externe ISi-Beratung nutzen, ist gegenüber der Erhebung von 2004 um vier Prozentpunkte zurückgegangen. Die gefragtesten Aufgaben waren dabei erneut Risiko- und Schwachstellenanalysen sowie Konzeptentwicklung (s. Tab. 12). Die Zufriedenheit mit den Leistungen der Berater ist indes gesunken: Nur noch 32 % (2004: 51 %) äußerten sich uneingeschränkt, 62 % mit Einschränkungen (2004: 46 %) zufrieden – der Anteil der unzufriedenen Berater-Kunden verdoppelte sich auf 6 % (vgl. Abb. 11).

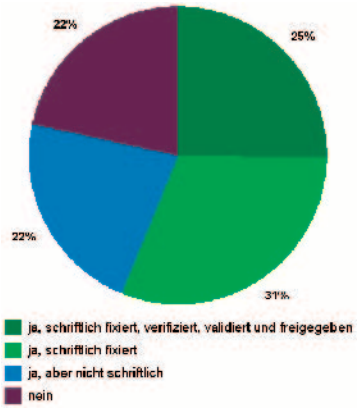
Die Leistungen von Outsourcern wurden sogar noch etwas zurückhaltender beurteilt: 28 % gaben an uneingeschränkt, 67 % mit Einschränkungen zufrieden zu sein. Insgesamt nutzen 56 % der Teilnehmer Outsourcing – die hierfür vorgesehenen Funktionen nennt Tabelle 13. Es zeigt sich ein ähnlich hoher Nutzer-Anteil wie bei Beratungsleistungen, die Schnittmenge liegt jedoch nur bei etwa zwei Dritteln. Auffällig ist, dass nicht etwa die kleineren und mittleren Unternehmen vorrangig Beratung und Outsourcing nutzen, um etwaige Kapazitäts- oder Know-how-Engpässe zu kompensieren: Im Gegenteil ist der Anteil der Nutzer externer Dienste bei den Unternehmen ab 500 Mitarbeitern deutlich größer (80 % Beratung, 73 % Outsourcing) als bei den KMU (43 % bzw. 46 %).

Ansprechpartner für (computer-)forensische Analysen suchen die meisten Teilnehmer naheliegenderweise bevorzugt im eigenen Haus (Tab. 14). Als wichtigster Externer fungieren dann schon die Strafverfolgungsbehörden, die immerhin fast ein Viertel der Befragten auf jeden Fall einbinden würden. Alle anderen externen Institutionen würden zudem jeweils über fünfzig Prozent nur „nachrangig“ oder keinesfalls einbeziehen. Bei immerhin 15 % der Stichprobe wurde übrigens 2005 ein Sicherheitsvorfall tatsächlich rechtlich verfolgt. Dies deckt allerdings nur knapp die Hälfte aller Vorfälle ab: Zwei Fünftel der Organisationen, die einen Vorfall angaben, sahen mangels Verfolgungsinteresse von



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

Abbildung 9: Gestattete Aufschaltung und Kontrolle privater Systeme



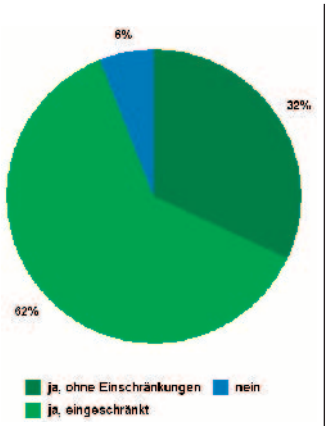
Basis: 162 Antworten

Abbildung 10: Vorhandensein eines IT-Notfall-/Wiederanlaufkonzepts

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

Basis: 109 Antworten

Tabelle 11: Vorhandene Positionen



Basis: 81 Antworten

Abbildung 11: Zufriedenheit mit Beratungsdienstleistungen

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

Basis: 87 Antworten

Tabelle 12: Genutzte Berater-Funktionen

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

Basis: 88 Antworten

Tabelle 13: Genutzte Outsourcing-Funktionen

rechtlichen Schritten ab – ein Siebtel nannte mangelndes Wissen um Ermittlungsmöglichkeiten als Grund für die Nichtverfolgung.

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

Risikobewertung

Dem Punkt „Verzögerungen von Arbeitsabläufen" wurde bei den Kriterien zur Risikobewertung in diesem Jahr ein höherer Stellenwert zugemessen – solche Störungen liegen jetzt an dritter Stelle der Werteskala (Tab. 15). Im Übrigen blieb alles in etwa beim Alten: Verstöße gegen Gesetze, Vorschriften und Verträge stehen unangefochten auf Rang 1, gefolgt von der Angst vor Imageverlusten. Zur Risikoanalyse haben – wie schon 2004 – 70 % der Teilnehmer Anwendungen und Systeme hinsichtlich der Bedeutung für die Aufgabenerfüllung und bestehender Risiken bewertet. Der Anteil, der hierbei alle Systeme einbezieht, ist um fünf Prozentpunkte auf 26 % gestiegen (s. Abb. 12).

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

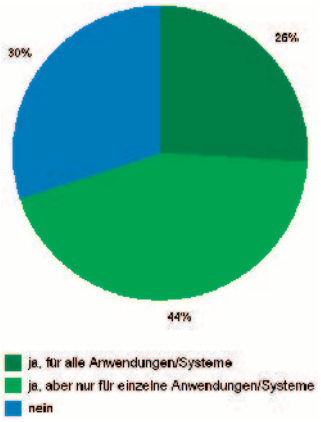
Gesetze und Regularien

Die erneut gestiegene Zahl von Teilnehmern, welche die Einhaltung von Gesetzen und Regularien als „sehr wichtig" ansehen, korrespondiert heuer mit gesteigerten Kenntnissen (potenziell) einschlägiger Regelwerke (Abb. 13): Die Bekanntheit stieg jeweils um 5–18 Prozentpunkte im Vergleich zur vorigen Studie; gleichzeitig sahen auch jeweils 10–18 Prozentpunkte mehr Befragte diese Regelungen als relevant an. Eine Ausnahme bildet lediglich die Signaturgesetzgebung: Die Zahl der Teilnehmer, die Signatur-Gesetz (SigG) und -Verordnung (SigV) inhaltlich kennen, sank um sieben Prozentpunkte, deren Relevanz um einen.

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

Basis: 144 Antworten (mind. einer Teilfrage)

Tabelle 14: Ansprechpartner für forensische Analysen



Basis: 159 Antworten

Abbildung 12: Reichweite der Risikobewertung

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

Basis: Ø 145 Antworten

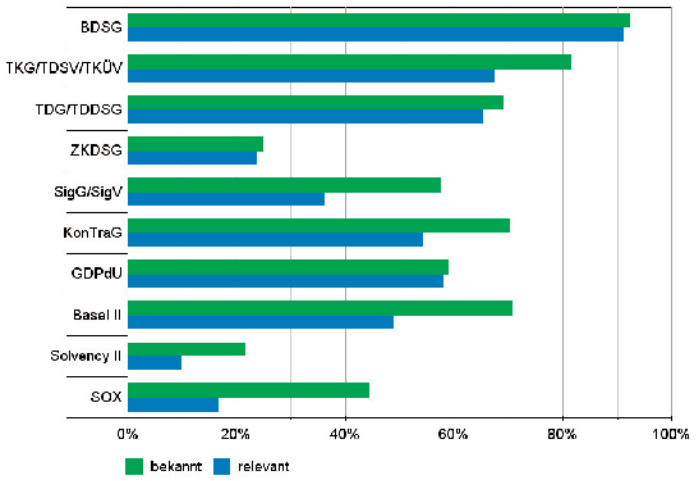
Tabelle 15: Kriterien zur Risikobewertung

Die durchweg höchste Steigerung erzielte hingegen – endlich – das Gesetz zur Kontrolle und Transparenz bei Aktiengesellschaften und publizitätspflichtigen Gesellschaften (KonTraG): Kenntnis und Relevanz legten um 18 Prozentpunkte zu und auch bei der Umsetzung machte das Gesetz den deutlichsten Sprung (s. Abb. 14) nach vorne. Ebenfalls nachgelegt wurde bei der Umsetzung der Telekommunikations-Regularien und bei Basel II (Eigenkapitalvorschriften für das Kreditgewerbe). Keine große Rolle spielen in der Praxis des deutschsprachigen Raums bislang offenbar die „Newcomer" Solvency II (EU-Projekt zum Rahmenwerk für die Versicherungsaufsicht) und der US-amerikanische Sarbanes-Oxley Act (SOX), der zwar schon 44 % der Befragten inhaltlich bekannt ist, aber nur von 17 % als relevant angesehen wird.

Erstmals haben wir zudem nach einer Beurteilung der Angemessenheit deutscher Gesetze und Regulierung gefragt (Tab. 16). Zwischen 49 % und 70 % attestierten dem hiesigen Gesetzgeber dabei jeweils gute Arbeit; die übrigen Befragten waren in den meisten Bereichen klar polarisiert. Die deutlichsten Kritikpunkte: 49 % sehen die Strafgesetze bezüglich der Computer-Kriminalität als unzureichend an – gleichzeitig nannten aber auch 38 % die TK- und Internet-Überwachung überzogen (obwohl diese ja überwiegend vom Interesse der Strafverfolgung getrieben wird). Gespalten zeigte man sich in Sachen Signaturgesetz: Dort bezeichneten fast so viele Studienteilnehmer diesen Bereich als überzogen wie als unzureichend reguliert.

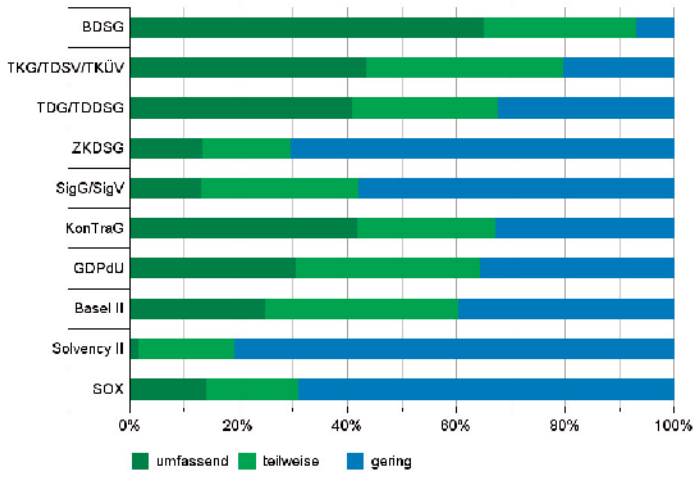
Kenntnisstand und Weiterbildung

Die Einschätzung des Kenntnisstands zur Informations-Sicherheit bei Management und Mitarbei-



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

Abbildung 13: Bekanntheit und Relevanz von Gesetzen und Regularien



Basis: Ø 94 Antworten

Abbildung 14: Umsetzungsgrad von Gesetzen und Regularien

Tabelle 16: Bewertung deutscher Gesetze und Regularien

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

Basis: Ø 144 Antworten

Tabelle 17: Genutzte Ausbildungsmethoden

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

Basis: Ø 134 Antworten *Vergleichszahl errechnet aus: häufig = 3, gelegentlich = 1, nie = 0

tern zeigt im Großen und Ganzen ein gewohntes Bild (Abb. 15). Lediglich die gewohnt guten Noten für die Sicherheits-Fachleute scheinen mit einem Gesamt-Schnitt von 1,9 etwas nachgegeben zu haben, was aber bei genauerer Betrachtung auf den höheren Anteil aus den kleinen und mittleren Unternehmen (KMU) zurückzuführen ist: In den großen Unternehmen schätzen 93 % die ISi-Kenntnisse ihrer Fachkräfte als „sehr gut" oder „gut" ein, die restlichen 7 % „befriedigend" (Durchschnitt: 1,6). Demgegenüber zeigt sich bei den KMU mit 77 % „sehr gut" und „gut" sowie 13 % „befriedigend" auch noch eine 10 % große Gruppe, die nur „ausreichend" oder „nicht ausreichend" bewertet wird, sodass sich hier nur ein Durchschnitt von 2,1 ergibt. Auch die Noten der Anwender hochsensitiver Bereiche liegen bei den KMU um eine Drittelnote schlechter als in großen Unternehmen.

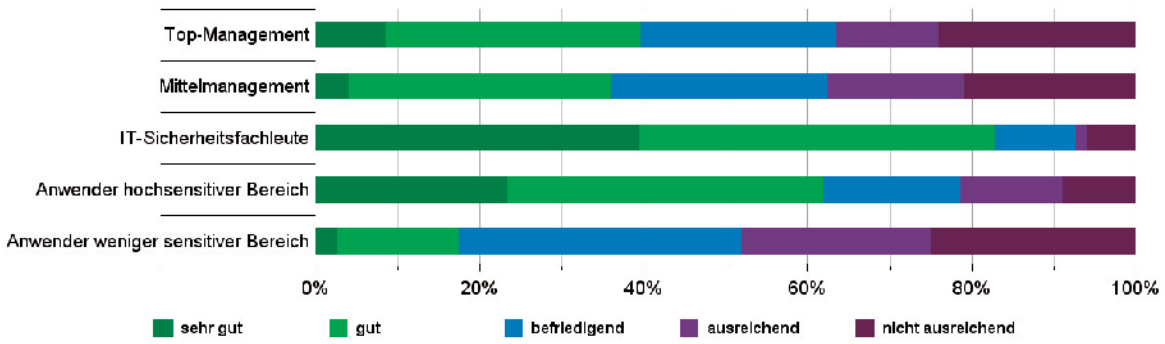
Betrachtet man Schulungsmethoden und -frequenz, so findet man wenig Veränderungen zur vorigen Studie. Nach wie vor stehen gelegentliche interne Weiterbildungen durch Frontalunterricht für Spezialgruppen sowie externe Schulungen am höchsten im Kurs (Tab. 17). Häufige externe Trainings sind zwar etwas seltener geworden (von 19 % in 2004 auf jetzt 13 %), gleichzeitig schrumpfte aber auch die Gruppe derer, die überhaupt nicht auf Derartiges zurückgreift um vier Prozentpunkte. Bei den Mitarbeitergruppen fällt auf, dass ISi-Beauftragte und vor allem Revisoren und Prüfer seltener geschult werden. Während die ISi-Spezialisten allerdings immer noch den Spitzenplatz bei der Weiterbildung innehaben, fallen die Prüfer hinter den Weiterbildungswert der Benutzer zurück, da über ein Drittel überhaupt keine Schulung mehr erfährt (vgl. Abb. 16).

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

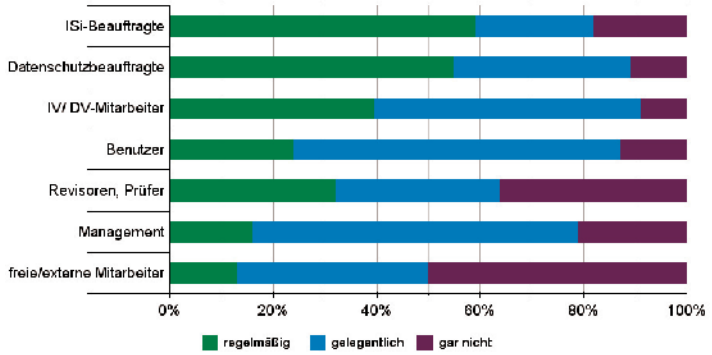
Informationsquellen

Zur allgemeinen Information über IT-Sicherheit auf Messen und Kongressen nutzen 65 % der Befragten die CeBIT, 45 % den BSI-Kongress, 38 % die IT-SecurityArea auf der SYSTEMS, 15 % die Essener SECURITY, 7 % die Infosecurity Europe (London) und 4 % die ISSE (wech-

Abbildung 15: Kenntnisstand der Manager und Mitarbeiter



selnde Orte). Bei den Zeitschriften stehen neben der <kes> vor allem die c't, DuD sowie Computerwoche und iX hoch im Kurs. Bei Mailing-Listen und Web-Angeboten dominieren klar das BSI sowie der Heise-Verlag die virtuelle Sicherheitslandschaft; auf dem dritten Platz liegt Security Focus (Bugtraq u. a.). Bei den bevorzugten Webseiten wurden zudem die Angebote von Microsoft und SANS.org gehäuft genannt.

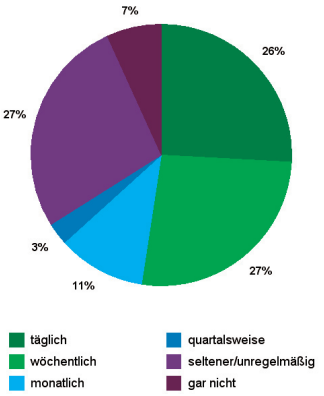


Abbbildung 16: Schulungsfrequenz verschiedener Mitarbeitergruppen

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

Generell ist die bevorzugte Informations-Art zu Sicherheits-Updates die aktive Aussendung durch den Hersteller: 75 % der Befragten nutzen diesen Weg, gefolgt von Mailing-Listen Dritter (45 %), Abfragen der Informationsseiten von Herstellern und Dritten (je 44 %) sowie aktiver Aussendung durch Händler oder Systemhäuser (33 %). Gut die Hälfte der Studienteilnehmer fragt dabei „passive" Kanäle täglich oder zumindest wöchentlich ab (Details s. Abb. 17).

Die Qualität der Herstellerinformationen kann dabei als befriedigend gelten (Abb. 18): Die größte Zufriedenheit findet man insgesamt bei den Sicherheitssystem-Anbietern sowie bezüglich Vollständigkeit und Verständlichkeit der Betriebssystem-Infos (Benotung jeweils 2,9), die größte Unzufriedenheit bei den Informationen zu Anwendungssystemen (Gesamtnote 3,2). Auffällig ist die kritische Beurteilung der Geschwindigkeit von Informationen der Betriebssystemanbieter, welche die in den anderen Kategorien besseren Noten auf das Niveau der Netzwerkanbieter „drückt" (beide insgesamt 3,0).



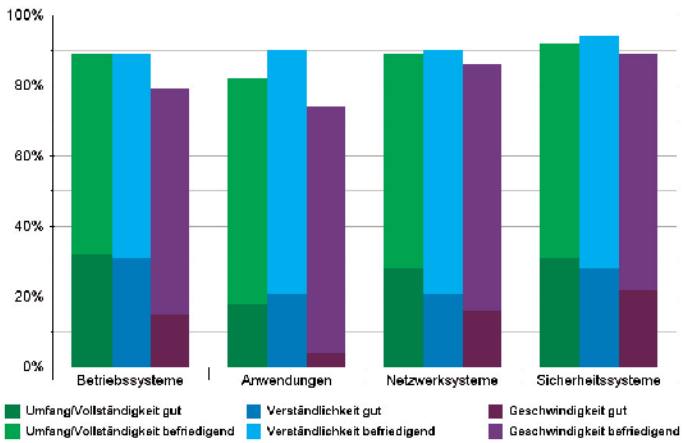
Basis: 147 Antworten

Abbildung 17: Prüfungsintervalle passiver Kanäle zu Sicherheits-Updates

Maßnahmen

Die „große Maßnahmen-Checkliste" (Tab. 18) belegt wie üblich eine eher serverzentrische Sicherheitsorganisation: Zum Client oder mobilen Endgerät hin nimmt der Umsetzungsgrad der meisten Sicherheitsmaßnahmen ab. Als heikel könnten sich dabei einige fehlende Schutzmechanismen bei mobilen Endgeräten erweisen, die auch die unbefriedigende Sicherheitseinschätzung (vgl. Abb. 5) dieser Systeme untermauert: Über ein Fünftel der mobilen Endgeräte ist derzeit (noch) ungeschützt gegen Malware; 13 % gaben sogar an, dass ein Virenschutz dort auch künftig nicht vorgesehen ist. (Personal) Firewalls sind ebenfalls noch selten: Bei 21 % der Studienteilnehmer ist diese Maßnahme geplant, aber noch nicht realisiert – 37 % wollen *keine* „mobilen Firewalls" einrichten. Und fast 60 % betreiben derzeit keine Datensicherung für mobile Systeme.

Eine Besserung ist bei der kryptographischen Sicherung von WLANs zu beobachten: Der Anteil



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

Abbildung 18: Qualität von Herstellerinfos

	Server / Zentrale			Clients / Endstellen			mobile Endgeräte		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
Firewalls	89%	6%	4%	52%	10%	38%	42%	21%	37%
Virenschutzmechanismen	94%	4%	3%	98%	1%	1%	79%	9%	13%
Datensicherung (Backup)	97%	1%	2%	50%	4%	46%	41%	6%	53%
Langzeit-Archivierung	62%	22%	16%	19%	5%	76%	14%	7%	80%
Intrusion Detection/Prevention Systems	47%	24%	29%	16%	11%	72%	13%	8%	80%
Benutzerverzeichnis mit Security Policy	57%	22%	22%	35%	15%	50%	31%	13%	56%
Authentifizierung									
... Hardware-Token	16%	7%	77%	18%	9%	72%	23%	13%	64%
... Passwort	93%	1%	6%	92%	3%	5%	82%	4%	15%
... Chipkarte	10%	13%	76%	14%	13%	73%	14%	6%	80%
... biometrische Verfahren	3%	4%	93%	5%	10%	85%	3%	8%	89%
Protokollierung unberechtigter Zugriffe	76%	13%	12%	36%	13%	51%	21%	11%	68%
Schnittstellenüberwachung/-schutz (USB, ser., par., Bluetooth, ...)	28%	22%	50%	23%	29%	48%	17%	30%	53%
Netzwerkzugangskontrolle (EAP, NAC, ...)	48%	16%	36%	22%	18%	60%	17%	15%	67%
Content Inspection/Filtering									
(Adress-/Inhaltsfilter)	56%	15%	29%	29%	13%	58%	17%	9%	74%
Spam-Abwehr	79%	13%	8%	59%	14%	27%	47%	10%	43%
Verschlüsselung									
... sensitive Daten	48%	13%	38%	34%	17%	49%	36%	16%	48%
... Festplatten (komplett/partitionsweise)	19%	17%	64%	17%	16%	67%	35%	22%	44%
... mobile Speicher (USB, Firewire, ...)	16%	14%	70%	18%	17%	65%	20%	23%	58%
... Archivdatenträger/Backups	19%	13%	68%	12%	8%	79%	9%	9%	82%
... drahtlose Peripherie (Funktastatur, Bluetooth, ...)	12%	9%	80%	13%	11%	75%	15%	10%	75%
... LAN/Intranet-Verbindungen	29%	17%	54%	23%	16%	61%	23%	9%	68%
... WLAN-Verbindungen	39%	11%	51%	31%	12%	57%	38%	10%	51%
... WAN/Internet-Verbindungen	46%	14%	40%	33%	14%	53%	38%	9%	53%
... Telefon	9%	6%	85%	8%	3%	89%	6%	2%	92%
... Voice over IP (VoIP)	11%	12%	77%	10%	12%	78%	11%	9%	80%
... Fax	8%	4%	88%	6%	2%	92%	3%	3%	94%
... E-Mail	31%	25%	45%	34%	23%	44%	32%	18%	50%
Elektronische Signaturen									
... E-Mail	26%	32%	42%	27%	33%	40%	23%	26%	51%
... Web (SSL/TLS)	48%	13%	40%	37%	19%	44%	29%	13%	58%
... Applikationen	18%	14%	69%	14%	15%	71%	13%	10%	77%
physische Sicherheit									
... Zutrittskontrolle, biometrisch	12%	5%	83%	7%	5%	89%			
... Zutrittskontrolle, sonstige	85%	3%	12%	54%	4%	43%			
... Bewachung	47%	2%	51%	25%	1%	73%			
... Video-Überwachung	38%	7%	55%	19%	1%	80%			
... Einbruchmeldeanlage	67%	7%	27%	39%	4%	58%			
... Schutz von Glasflächen gegen Durchbruch/-wurf	52%	5%	44%	22%	4%	74%			
... Sicherheitstüren	68%	6%	25%	27%	3%	71%			
... Brandmeldesysteme	81%	4%	15%	45%	1%	54%			
... Löschanlagen	54%	5%	41%	25%	1%	74%			
... andere Meldesysteme (Gas, Staub, Wasser, ...)	44%	5%	51%	11%	2%	87%			
... Datensicherungsschränke/-räume	80%	7%	13%	21%	4%	74%			
... Schutz gegen kompromittierende Abstrahlung (Tempest)	13%	4%	83%	5%	3%	92%	3%	3%	93%
... Maßnahmen gegen Hardware-Diebstahl	60%	6%	34%	36%	8%	56%	31%	13%	56%
physikalische Löschen von Datenträgern	64%	7%	29%	50%	12%	38%	44%	12%	44%
unterbrechungsfreie Stromversorgung (USV)	90%	5%	6%	21%	5%	74%	10%	5%	85%
Überspannungsschutz für Stromleitungen	84%	5%	10%	39%	4%	56%	18%	5%	78%
Überspannungsschutz für Daten-/TK-Leitungen	60%	7%	34%	25%	5%	70%	14%	4%	82%
Klimatisierung	85%	4%	11%	14%	1%	84%			
Rückrufautomatik bei Modemzugriff	47%	5%	48%	17%	3%	80%	10%	6%	83%
Reserve-Netzzugang (IT/TK) zur Ausfallüberbrückung	53%	15%	32%	18%	9%	73%	13%	5%	82%

Tabelle 18 Realisierte und geplante Sicherheitsmaßnahmen

Basis: Ø 147 Antworten (Server), Ø 138 (Clients), Ø 133 (mob. Endgeräte)

der „Nicht-Verschlüssler“ ist um rund zehn Prozentpunkte zurückgegangen, allerdings mit nach wie vor über 50 % der Teilnehmer immer noch recht hoch. Bei Voice-over-IP planen noch erheblich mehr Organisationen, auf Verschlüsselung völlig zu verzichten – immerhin liegen die entsprechenden Werte unter denen der „klassischen“ Telefonie.

Waren 2004 noch etliche Maßnahmen zur Spam-Abwehr in Planung, so sind diese nunmehr größtenteils umgesetzt – gut so, denn der mittlere Spam-Anteil ist heuer um gut acht Prozentpunkte auf 33 % gestiegen (vgl. Abb. 19). Weiterhin auf vielen „to-do“-Listen stehen Intrusion-Detection/Prevention-Systeme; ebenfalls erhebliches Planungspotenzial zeigen Benutzerverzeichnisse mit Security-Policy, Langzeitarchivierung, Schnittstellenüberwachung (USB, Bluetooth usw.) sowie allem voran Signatur- und Verschlüsselungsmaßnahmen für E-Mails sowie virtuelle Poststellen (12 % realisiert, 32 % geplant). Für mobile Endgeräte plant zudem noch eine größere Zahl von Organisationen Verschlüsselungsmechanismen für Festplatten und mobile Speicher einzurichten.

Ob bei zukünftigen Anschaffungen Produkte mit einer Sicherheitszertifizierung nach anerkannten Standards bevorzugt werden, ist weiterhin bei der Mehrheit der Befragten offen (56 %) – 16 % haben sich bereits dagegen entschieden. Der Anteil der klaren Befürworter zertifizierter Sicherheitssysteme liegt heuer bei 28 % – innerhalb der Teilnehmer-Gruppe, die bereits solche Produkte im Einsatz hat (41 %), verdoppelt er sich jedoch fast. Immerhin gaben auch 69 % an, ihre Erwartungen an Nutzen und Zuverlässigkeit dieser Systeme hätten sich erfüllt. Einen höheren Preis zertifizierter Produkte hielten insgesamt 50 % für gerechtfertigt. Zur Bekanntheit und Bedeutung verschiedener ISi-Kriterienwerke siehe Abbildung 20.

PKI und IDM

Als Dauer-Inverstitionsvorhaben erweisen sich Public-Key-Infrastrukturen (PKI): Weiterhin plant ein Drittel der Studienteilnehmer die Einrichtung einer PKI, aber nur ein gutes Viertel aller Befragten hat solche Pläne bereits umgesetzt – die vorgesehenen Einsatzzwecke nennt Tabelle 19. Noch eine richtige Seltenheit sind realisierte Identity-Management-Systeme (IDM) – bei nur 5 % der Befragten. 22 % planen für die Zukunft ein IDM. Die vorgesehenen Hauptziele dafür wären dann die Realisierung einer konsistenten Rechtevergabe, Sicherheitsgewinne durch Policy-Enforcement und eine bessere Revisionierbarkeit. Kostenersparnisse erwartet kaum jemand, dafür jedoch viele Probleme bei der Einrichtung: Nur 12 % beziehungsweise 14 % sehen die technische beziehungsweise organisatorische Komplexität eines IDM als unproblematisch an (vgl. Tab. 20).

PKI-Funktionen	realisiert	geplant	nicht vorgesehen
E-Mail-Verschlüsselung	41%	43%	16%
Dateiverschlüsselung	27%	41%	32%
Zugriffsrechte	17%	33%	49%
Single-Sign-On	17%	34%	49%
Virtual Private Networks	30%	30%	39%
Telearbeitsplätze / Remote Access	31%	29%	40%
Web-Zugriff	18%	30%	52%

Basis: Ø 89 Antworten

Tabelle 19: Realisierte und geplante PKI-Funktionen

Virtual Private Networks (VPNs)

Das verbreitetste VPN-Verfahren bleibt IPsec: 74 % haben bereits mindestens ein IPsec-VPN realisiert, weitere 9 % planen dies. Doch auch SSL-VPNs sind bereits bei 58 % im Einsatz und bei 13 % in Planung. Die weitaus meisten Studienteilnehmer (73 %) sehen keine grundsätzlichen Argumente gegen SSL-VPNs – 14 % gaben indes an, diese Variante decke sich nicht mit bestehenden Anforderungen, 8 % hatten Vorbehalte wegen der Kosten und 3 % äußerten, es fehle an einer passenden Lösung.

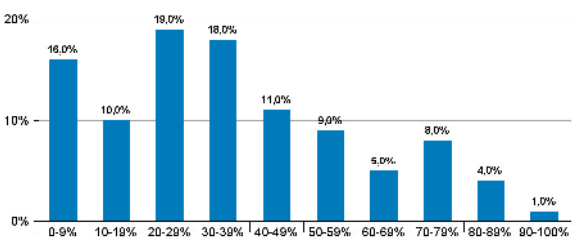
E-Mail-Verschlüsselung

Auch in diesem Jahr lässt sich eine leichte Steigerung der Bereitschaft erkennen, E-Mails verschlüsselt zu senden, sofern ein Krypto-Schlüssel des Empfängers verfügbar ist: Der Anteil derer, die dennoch *nicht* verschlüsseln würden, sank um zwei Prozentpunkte auf 42 % – gleichzeitig stieg die Zahl der Befragten, die dann alle externen (13 %) oder sogar generell alle Nachrichten

	sehr problematisch	problematisch	unproblematisch
technische Komplexität/ aufwändige Einführung	37%	51%	12%
organisatorische Komplexität/ aufwändige Einführung	38%	48%	14%
ROI schwer berechenbar/ nachvollziehbar	35%	44%	21%
hohe Produktkosten	29%	43%	28%
hohe Betriebskosten	23%	45%	32%
Herstellerabhängigkeit	22%	38%	41%

Basis: Ø 77 Antworten

Tabelle 20: Hemmnisse für den Einsatz von Identity-Management



Basis: 147 Antworten

Abbildung 19: Anteil von Spam an der eingehenden E-Mail

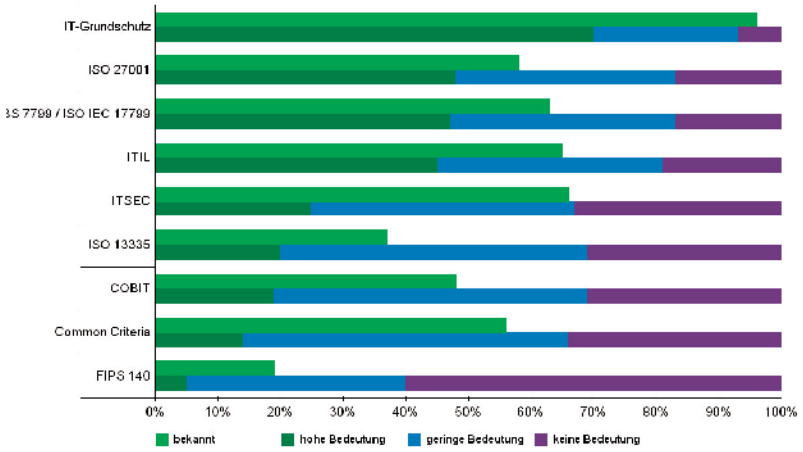


Abbildung 20: Bekanntheit und praktische Bedeutung von ISi-Kriterienwerken

Basis: Ø 138 Antworten (Bekanntheit), 141 (Bedeutung Grundschutz), Ø 84 (Bedeutung andere)

verschlüsseln würden (8 %). Erneut gaben 47 % an, zumindest sensitive Mails zu chiffrieren (Mehrfachnennungen). Klar aufgeholt hat dabei S/MIME: (Open)PGP liegt zwar mit 66 % Nutzung immer noch vorn, die Zahl der (zumindest auch-) S/MIME-Anwender stieg aber sprunghaft auf 57 % (2004: 34 %).

Elektronische Signaturen

Klar an erster Stelle bei elektronischen Signaturen liegen weiterhin reine Softwarelösungen, die allerdings auch nur 44 % der Befragten bereits nutzen (vgl. Tab. 20 – zu den Einsatzzwecken vgl. Tab. 18). Eine gewisse Steigerung des Interesses scheint bei den weniger streng reglementierten Varianten gemäß Signaturgesetz (SigG) vorzuliegen: Lösungen für fortgeschrittene und qualifizierte Signaturen (ohne Anbieterakkreditierung) gaben jeweils rund ein Fünftel der Befragten als bereits realisiert an – nur noch etwa 60 % erteilen diesen eine pauschale Absage. Bei qualifizierten Signaturen mit Anbieterakkreditierung bleibt jedoch weiterhin eine große Zurückhaltung festzustellen, die zu weniger als zehn Prozent bestehender Umsetzung und 75 % dauerhafter Ablehnung führt.

Open-Source-Software

Der Anteil der Studienteilnehmer, die Open-Source-Software (OSS) für sicherer halten als Programme mit nicht-offengelegtem Quellcode, ist im Vergleich zu 2004 um sechs Prozentpunkte gesunken – gleichzeitig verbuchten die ausgesprochenen Kritiker Zuwachs (s. Abb. 21). Dennoch ist OSS bei 68 % der Studienteilnehmer im Einsatz, und zwar weiterhin überwiegend aus Kostengründen (50 %) statt aus Sicherheitserwägungen (38 %). OSS erleichtert zudem naturgemäß den Einsatz verschiedenartiger Lösungen auf verschiedenen Netzsegmenten oder Systemebenen (Multi-Vendor-Strategie), vor allem im Bereich der Server-Betriebssysteme. Die Umsetzung im Teilnehmerfeld zeigt Tabelle 21.

Content Security

Die größte bewusst aus Sicherheitsgründen eingesetzte Heterogenität findet man jedoch bei der Malware-Abwehr: Nur 41 % vertrauen hier noch auf einen einzigen Anbieter (vgl. Tab. 22), was in etwa dem Wert von 2004 entspricht. Der Anteil derjenigen, die sogar auf *drei* oder mehr unterschiedliche Lösungen setzen, hat sich jedoch im Vergleich zur vorigen Studie noch um vier Prozentpunkte erhöht.

Generell ist eine umfassende Lösung gefragt: Jeweils deutlich über 80 % erwarten von einer Content-Security-Solution außer der Abwehr von Viren auch Schutz vor Spyware und Spam. Monitoring und Alerting fordern etwa drei Viertel und jeweils knapp zwei Drittel wollen auch

Folgende Infrastruktur ist ...	realisiert	geplant	nicht vorgesehen
nur Software	44%	15%	41%
Hardwaremodule	2%	8%	89%
Hardware-Token	10%	15%	75%
Chipkarten	20%	18%	62%
Klasse-2-Chipkarten-terminal (sichere PIN-Eingabe)	12%	13%	75%
Klasse-3-Chipkartenterminal (mit eigenem Display)	7%	7%	85%
gemäß Signaturgesetz (SigG)			
... fortgeschrittene Signatur	22%	17%	61%
... qualifizierte Signatur	18%	24%	59%
... qualifizierte Signatur mit Anbieterakkreditierung	9%	16%	75%
nichts von alledem	24%	17%	

Tabelle 21: Realisierte und geplante Infrastruktur für elektronische Signaturen

Basis: Ø 96 Antworten

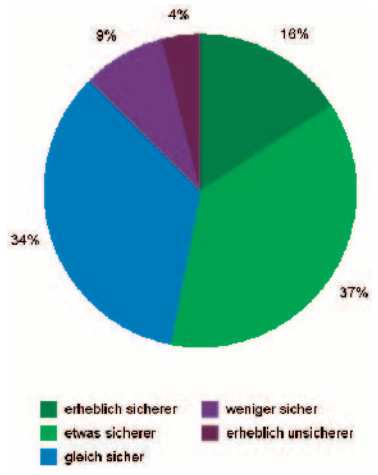


Abbildung 21: Einschätzung der Sicherheit von Open-Source-Software

Basis: 151 Antworten

gleichzeitig Phishing-Abwehr, Inhaltsfilter und Reporting-Tools darin vorfinden.

Außer bei mobilen Systemen haben die Befragten die Update-Frequenz für Malware-Signaturen deutlich erhöht: Die mittleren Werte (Tab. 23) sind auf zentralen Systemen, PCs und Workstations heuer um jeweils rund sechs Stunden kürzer als vor zwei Jahren. Meistgenannt bleibt ein tägliches Update – bei den zentralen Systemen (Gateway und Server) gibt es aber mittlerweile genauso viele Teilnehmer, die ein stündliches Update vorsehen. Nochmals deutlich gestiegen ist zudem die Verbreitung von Online-Virenwächtern: Über zwei Drittel haben jetzt einen solchen Schutz auf den PCs ihres Hauses eingerichtet (2004: 52 %). Eine isolierte Test-Umgebung für Malware steht 48 % zur Verfügung.

Device-Management

Der erheblichen Gefährdung durch Plug&Play-(P&P)-Peripherie steht offenbar nur selten eine erwünschte Nutzung gegenüber: Auf die Frage nach der Bedeutung für die Wertschöpfungskette ihres Hauses antworteten die weitaus meisten Befragten, diese sei gering (37 %) oder vernachlässigbar (32 %) – 5 % sehen darin überhaupt keinen Nutzen, bei 10 % ist die Nutzung generell untersagt. Nur eine eher kleine Gruppe von Unternehmen und Behörden (15 %) gab eine „große“ Bedeutung an. Eine Intensivierung des P&P-Einsatzes planen 25 %. Zur Sicherung der Schnittstellen gegen unerwünschte Aufschaltung von P&P-Devices dienen vor allem organisatorische Mittel (Verbot, Dienstanweisung usw.) – nur ein starkes Viertel nutzt „mitgelieferte“ Sicherungsfunktionen der BIOS- oder Betriebssystem-(OS)Anbieter, noch weniger eine spezielle Schutzsoftware (s. Abb. 22).

Security-Management

Die Einschätzung der Wichtigkeit verschiedener Komponenten im Security-Management entspricht in etwa den Angaben der vorigen Studie. An erster Stelle stehen eine zentrale Überwachung eingesetzter Sicherheitssysteme und eine plattformübergreifende Benutzerverwaltung (s. Tab. 24). Häufiger als 2004 wurde hingegen der Einsatz von Management-Lösungen zur System-Administration bejaht: 64 % nutzen für Netzwerksysteme Management-Lösungen der jeweiligen Hersteller (+14 Prozentpunkte), bei Host-/PC-Systemen sind es 55 % (+16). Mit zentralen Management-Lösungen arbeiten 44 % im Netzwerk (+8) beziehungsweise 50 % auf Hosts und PCs (+9). Dennoch verwalten aber heute 77 % der Befragten ihre Netzwerksysteme (auch) in nennenswertem Umfang manuell, bei Host-/PC-Systemen sind es 74 % (2004: 69 %/72 %). Ein Mehr an Management-Lösungen scheint also wider Erwarten keine Entlastung bei der „Handarbeit“ zu bedeuten.

Im Einsatz sind Lösungen von ...	einem Anbieter	zwei Anbietern	drei und mehr Anbietern
Anti-Virus-Software	41%	42%	17%
Firewalls	59%	35%	6%
Router	61%	27%	13%
Server-Betriebssysteme	47%	36%	18%
Web-Server	63%	30%	7%
Applikation-Server	55%	26%	19%

Basis: Ø 144 Antworten

Tabelle 22: Heterogenität aus Sicherheitsgründen (Multi-Vendor-Strategie)

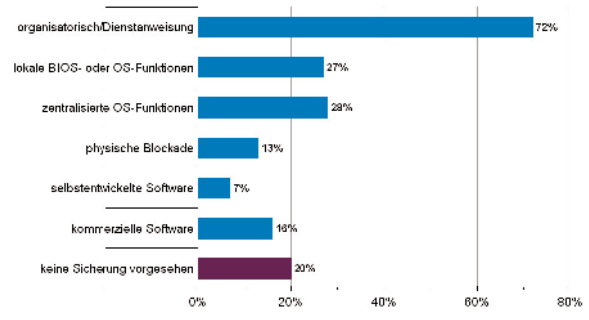
Viren-Scanner	Update-Frequenz [Std.]
an der Firewall/Internet-Gateway	14,5
auf dem Mail-/File-/Applikationsserver	13,3
auf den PCs/Workstations	23,9
auf mobilen Systemen	40,6

Basis: Ø 104 Antworten (mob. Systeme: 81)

Tabelle 23: Updatefrequenz von Viren-Scannern (Mittelwert)

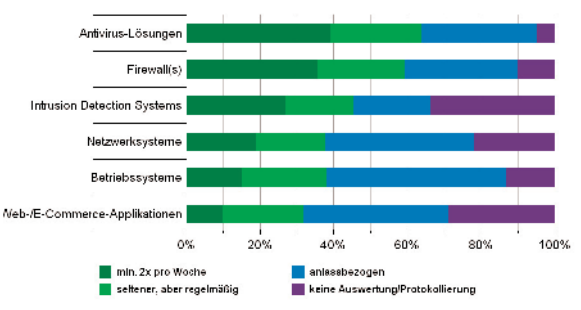
Die meistgeprüften Log-Files sind weiterhin jene von Anti-Malware-Lösungen, gefolgt von Firewall- und Intrusion-Detection-Protokollen – Meldungen von Netzkomponenten, Betriebssystemen und Applikationen werden hingegen überwiegend nur bei Bedarf ausgewertet (Details s. Abb. 23).

Für den „Fall der Fälle“, dass ein System nicht mehr wie vorgesehen startet oder arbeitet, verlassen sich die meisten Studienteilnehmer zum System-Recovery auf die Mechanismen der Betriebssystemhersteller oder auf das Wiedereinspielen von Images – mit 46 % auch ein hoher Anteil unter Inkaufnahme eines eventuellen Datenverlusts seit der letzten Sicherung (Details s. Tab. 25).



Basis: 158 Antworten

Abbildung 22: Mechanismen zur Schnittstellen-Sicherung (USB, seriell, parallel usw.)



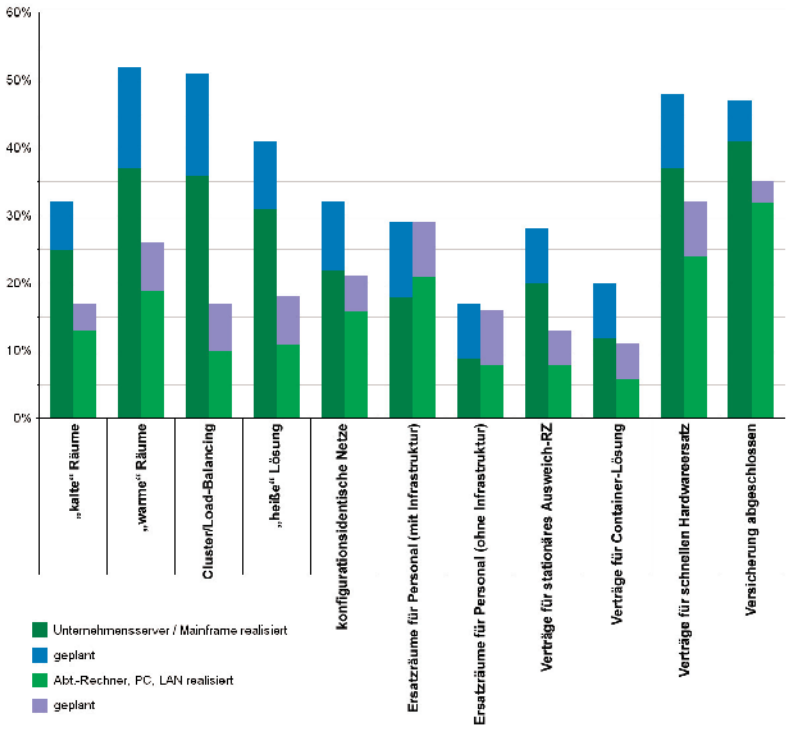
Basis: Ø 149 Antworten

Abbildung 23: Auswertung von Log-Daten

Folgende Komponenten sind...	sehr wichtig	wichtig	unwichtig	Vergleichszahl
zentrale Überwachung der eingesetzten Security-Systeme	64%	32%	3%	1,61
plattformübergreifende Benutzerverwaltung	59%	37%	4%	1,54
Virtual Private Networks (VPN)	47%	46%	7%	1,4
Alarm- und Eskalationssystem	42%	52%	6%	1,35
Intrusion Detection Systems (IDS)	27%	55%	18%	1,09
Single-Sign-on	26%	50%	23%	1,03
Public Key Infrastructure (PKI)	24%	56%	20%	1,03
Kontrolle und Überwachung von Internet-Missbrauch	21%	57%	22%	0,99

Basis: Ø 153 Antworten

Tabelle 24: Security-Management



Basis: Ø 120 Antworten

Abbildung 24: Bereitstellungen für längere Ausfälle bei IT-Systemen

Notfallvorsorge

Bei der räumlichen Trennung wesentlicher Komponenten der Informationsverarbeitung überwiegt erneut die Unterbringung in einem anderen Gebäude eine Separation durch Brandabschnitte. Vor allem Auslagerungsarchive (37 %) und gespiegelte Daten (35 %), aber auch zusätzliche Rechner/Cluster (31 %) werden auf verschiedene Gebäude verteilt – andere Brandabschnitte genügen 26 % (Archive), 21 % (Mirror) beziehungsweise 18 %. Weiterhin eher selten ist die Auslagerung zu Partnern oder kommerziellen Anbietern (14 % / 8 % / 8 %). Für Robotersysteme überwiegt hingegen mit 58 % die Zahl der Befragten, die *keine* räumliche Trennung vorsehen.

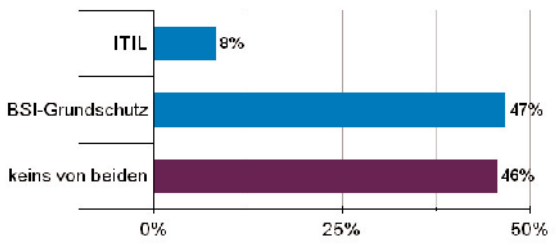
Vergleicht man die Bereitstellungen beziehungsweise Planungen für längere Ausfälle (Abb. 24) mit den Angaben von 2004, so zeigt sich für Unternehmens-Server und Mainframes – neben einer höheren Vorsorgequote „in der Breite" – vor allem ein klarer relativer Bedeutungszuwachs so genannter „warmer" Lösungen, also von Räumen mit bereitstehender (wichtiger) Hardware. Lagen diese vor zwei Jahren noch mit „heißen" Backup-Systemen auf einem geteilten vierten Platz, so stehen sie jetzt unter Berücksichtigung geplanter Vorhaben an erster Stelle (52 %). Auch bei den realisierten Bereitstellungen (37 %) haben sie mit den Verträgen zur schnellen Ersatzlieferung gleichgezogen und landen hinter abgeschlossenen Versicherungen (41 %) auf Platz Zwei. „Kalte" Räume haben hingegen an Gewicht verloren.

Dass Recovery-Verträge auch tatsächlich genutzt werden mussten, berichteten diesmal gleich acht Studien-Teilnehmer, die Hälfte von ihnen erlebte sogar mehrere Ernstfälle; 46 Teilnehmer gaben hingegen an, einen bestehenden Recovery-Vertrag bislang noch nicht in Anspruch genommen zu haben.

Maßnahme	ja
Bordmittel des Betriebssystems	72%
Image-Restore mit „ausgespartem" Datenbereich	54%
Rettungs-/Live-CD des Betriebssystemanbieters	50%
Image-Restore unter Inkaufnahme eines evtl. Datenverlusts	46%
selbst erstellte Rettungs-/Live-CD	34%
frei erhältliche Unix-/Linux-Rettungs-/Live-CD	22%
Rettungs-/Live-CD eines kommerziellen Drittanbieters	20%
Sonstiges	6%
nichts dergleichen	1%

Basis: 158 Antworten

Tabelle 25: Vorgesehene Maßnahmen zum System-Recovery



Basis: 90 Antworten

Abbildung 25: Berücksichtigung von Rahmenwerken bei Notfalldokumentationen

Auch heuer bleiben „manuelle“ Systeme bei der Notfall-Dokumentation führend: 64 % der Befragten haben ein solches „Handbuch“ für den Notfall in (elektronischer) Textform vorliegen, weitere 19 % planen das; online-gestützte Dokumentationen findet man bei 31 % (20 % in Planung), ausgewachsene Online-Anwendungen nur bei 13 % (16 % i. P.). Die Aktualisierung von Notfall-Dokumentationen erfolgt weiterhin vorrangig anlassbezogen (82 %) – nur 11 % gaben an, dies regelmäßig zu tun (im Mittel etwa halbjährlich), 7 % erneuern ihre Pläne/Vorbereitung nie. Knapp die Hälfte der vorliegenden Dokumentationen deckt die Anforderungen des IT-Grundschutz' ab (s. Abb. 25) Zu den Inhalten der Notfall-Dokumentation siehe Tabelle 26.

	ja	teilweise	nein
Aktionspläne für den K-Fall	50%	33%	17%
Recovery Units mit			
... Aktionsplan	39%	38%	23%
... Benötigte Ressourcen (HW,SW, etc.)	40%	31%	29%
Aktionspläne Störungen im Tagesbetrieb	41%	33%	26%
IT-Dokumentation (Arbeitsanweisungen)	52%	37%	12%
Allgemeine Dokumentationen	50%	39%	11%
Inventarisierung			
... Hardware	55%	30%	15%
... Software	52%	32%	16%
... Infrastruktur (Klima, etc.)	42%	31%	27%

Basis: Ø 124 Antworten

Tabelle 26: Umfang der Notfalldokumentation

Teilnehmer

Der „durchschnittliche Befragte“ dieser <kes>/Microsoft-Sicherheitsstudie arbeitet für ein Haus mit insgesamt 4019 Mitarbeitern, dessen IT-Abteilung 337 Köpfe zählt und 10 ausgewiesene ISi-Spezialisten hat. Wie eingangs erwähnt hat sich dieses Jahr mit rund 60 % eine erfreulich große Zahl an kleineren und mittleren Unternehmen (KMU) mit bis zu 500 Mitarbeitern beteiligt. Im Mittel beschäftigen diese KMU 140 Menschen, 10 % davon in der IT-Abteilung, in der sich zwei Mitarbeiter speziell mit der Informations-Sicherheit befassen. Bei den großen Häusern mit 500+ Mitarbeitern ergibt sich folgender Schnitt: 10 159 Mitarbeiter insgesamt, 862 in der IT, 25 ISi-Spezialisten.

Die Verteilung der vertretenen Branchen zeigt Tabelle 27. Die KMU haben dabei einen überproportionalen Anteil an Beratern, Handel, IT-Unternehmen und dem akademisch/schulischen Umfeld. 28 % der Teilnehmer tragen explizite Verantwortung für die Sicherheit (vgl. Tab. 28), 20 % sind als RZ-/IT-Leiter tätig, weitere 12 % als Geschäftsführer, wobei diese letzte Gruppe ausschließlich den KMU entspringt.

	Prozent
Behörden	19%
Berater	14%
Kreditwirtschaft	10%
übrige Industrie (ohne chem. Ind.)	8%
Handel	6%
sonstige IT (ohne andere Rubriken)	6%
Outsourcing-Dienstleister	5%
Wissenschaft/Forschung/Schulen	5%
Verlage/Medien	4%
Energieversorgung	3%
Versicherungen	3%
Gesundheitswesen	3%
TK-Dienstleister/-Provider	3%
chemische Industrie	2%
Transport/Verkehr	2%
Sonstiges	8%

Basis: 160 Antworten

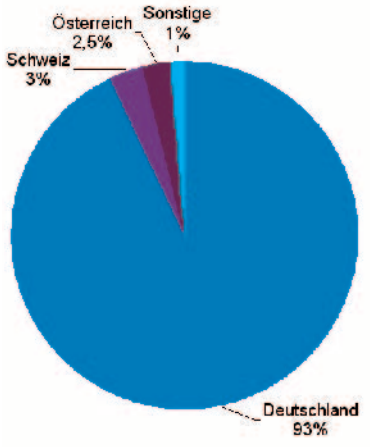
Tabelle 27: Branchenzugehörigkeit der Studien-Teilnehmer

Die durchschnittliche IT-Ausstattung der befragten Häuser umfasst 6 Mainframes (KMU: 4 / „Große“: 10), 833 Server (27 / 2139), und 2040 Clients (126 / 5187) sowie 293 Heim-/Telearbeitsplätze (15 / 759) und 860 mobile Endgeräte (42 / 2240). Damit sind nunmehr in der „gemittelten Unternehmung“ über ein Viertel aller Endgeräte mobil; inklusive der Heimarbeitsplätze befindet sich sogar mehr als ein Drittel zumindest zeitweise außerhalb der Unternehmensgrenzen. Selbst unter Ausschluss von Maximalwerten blieben mittlerweile noch mehr als 20 % mobiler Endgeräteanteil übrig. Angesichts der oben genannten schlechten Sicherheitseinschätzung dieser Systeme ein bedenklicher Zustand.

Bei den Netzwerken ergeben sich nach Ausschluss zweier „Ausreißer“ mit ungewöhnlich hohen Werten folgende Mittel: 31 Weitverkehrsnetze (WAN, inkl. VPN und Mietnetze – bzw. unterschieden nach Unternehmensgröße: 12/62), 32 LANs (5/84) und 4 WLANs (2/9).

Budgets

76 Studien-Teilnehmer haben Angaben zu Umsatz oder Bilanzsumme ihres Hauses gemacht; 38 weitere gaben an, dieser Wert sei irrelevant, da es sich um Behörden oder Ähnliches handele. Der durchschnittliche Umsatz lag bei 2,6 Mrd. € (567 Mio. €/5,1 Mrd. €), die mittlere Bilanzsumme betrug 21,8 Mrd. (6,2 Mrd. €/35,3 Mrd. €). Von den KMU, die Zahlen genannt haben, erwirtschaften 44 % über 10 Mio. € Umsatz jährlich.



Basis: 157 Antworten

Abbildung 26: (Haupt-)Sitz der teilnehmenden Unternehmen und Behörden

	Prozent
Sicherheitsverantwortlicher	28%
RZ-/IT-Leiter	20%
Geschäftsführer	12%
Datenschutzbeauftragter	7%
Administrator/Systemtechniker	7%
DV-/Orga-Leiter	6%
Revisor	6%
Sicherheitsadministrator	4%
IT-Mitarbeiter	4%
Sonstige	6%

Basis: 160 Antworten

Tabelle 28: Funktion der Teilnehmer

Datenwert/Verlust	Nennungen
unter 10.000	4
10.000 bis 100.000	8
100.000 bis 1 Mio.	15
1 Mio. bis 100 Mio.	26
100 Mio. bis 500 Mio.	5
500 Mio. bis 1 Mrd.	1
ab 1 Mrd.	5

Basis: 64 Antworten

Tabelle 29: Geschätzter Verlust bei Vernichtung aller elektronisch gespeicherten Daten

Angaben zum IT-Budget (inkl. Personalkosten) haben 95 Befragte gemacht: Mit 51,7 Mio € (1,5 Mio. €/134 Mio. €) lag der Durchschnitt dabei deutlich über den Zahlen von 2004; selbst nach Ausschluss des maximal angegebenen Budgets ergibt sich noch ein Mittelwert von 20,3 Mio. € (bzw. 52,1 Mio. € bei den „Großen"). Der mittlere Anteil der Informations-Sicherheit (ISi) an diesen Töpfen liegt bei 9 % (10%/6%). Lässt man den genannten Ausreißer-Wert außer Betracht, lag das errechnete absolute ISi-Budget im Mittel bei 498.110 € (72 Tsd. €/1,2 Mio. €). Eine Staffelung aller Angaben zeigt Abbildung 27.

Stolze 31 % der Studien-Teilnehmer konnten sich heuer bei den IT-Budgets auf ermittelte Werte verlassen und mussten keine Schätzung abgeben (2004: 17 %), auch bei den ISi-Daten war mit 15 % eine deutliche Steigerung des „ermittelten Anteils" zu beobachten (2004: 9 %, 2002: 5 %). Dabei zeigte sich der Prozentsatz der verlässlicheren Daten bei den KMU und großen Unternehmen als praktisch gleich groß.

Datenwert

Eine Schätzung zum Wert aller elektronisch gespeicherten Daten haben dieses Jahr mit 64 Befragten nur recht wenige gewagt. Die Verteilung der Angaben entspricht dabei dem gewohnten Bild (s. Tab. 29). Es ergibt sich – erneut unter Auslassung des Ausreißerwerts, der sich auch im IT-Budget gezeigt hat – ein mittlerer geschätzter Datenwert von knapp 558 Mio. € (bzw. 5,2 Mrd. € über alle Angaben). Für die KMU lag der Durchschnitt bei 3,8 Mio. €, für die Unternehmen ab 500 Mitarbeitern bei knapp 1,6 Mrd. €. ■

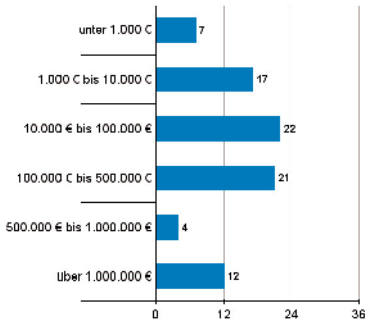


Abbildung 27: Budget für Informations-Sicherheit (Anzahl Nennungen) Basis: 83 Antworten

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

Impressum

Sonderdruck aus <kes> – Die Zeitschrift für Informations-Sicherheit Nr. 2006#4, 2006#5 und 2006#6 für

Microsoft Deutschland GmbH
Konrad-Zuse-Straße 1
85716 Unterschleißheim
Tel.: +49-89-3176-0
Fax: +49-89-3176-1000
E-Mail: kunden@microsoft.com

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.

Verantwortlich für die IT-Sicherheit…

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

<kes>

- liefert Ihnen strategisches Know-how, damit Sie eine solide Grundlage zur Entscheidungsfindung haben
- berichtet über Trends und Neuentwicklungen
- gibt Hilfen zum Risikomanagement
- erläutert einschlägige Gesetze im Umfeld der IT und TK
- informiert über die wichtigsten Messen und Kongresse
- ermöglicht es Ihnen durch Anwenderberichte von den Erfahrungen anderer zu profitieren
- gibt mit Marktübersichten einen Überblick über ausgewählte Produkte und Dienstleistungen

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

ABONNEMENT-BESTELLUNG

☐ **Ich abonniere die Zeitschrift <kes> ab Heft Nr.....**
Als Dankeschön erhalte ich das erste Heft gratis.

Das Abonnement enthält ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info mit allen aktuellen Beiträgen und dem <kes>-Archiv.
Ich kann das Abonnement bis 14 Tage nach Erhalt des ersten Exemplars formlos widerrufen.

Nach Ablauf der Widerrufsfrist wird das Abonnement zu den regulären Bedingungen gültig:

Jahresbezugspreis (6 Ausgaben) € 122,00 inkl. MwSt. und Versandkosten (Schweiz SFr 238,00 / restl. Ausland € 137,00).

Der Jahresbezugspreis wird jeweils für ein Jahr im Voraus berechnet. Eine Kündigung des Abos ist dennoch jederzeit zur nächsten nicht gelieferten Ausgabe möglich. Überbezahlte Abogebühren werden rückerstattet.

Ich bin einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weitergibt.

PROBEHEFT-ANFORDERUNG

☐ Bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Datum | Zeichen | Unterschrift

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim

Lieferung bitte an

Telefon Durchwahl

MALWARE

STEHT AUF DER ABSCHUSSLISTE

MICROSOFT.COM/GERMANY/SICHERHEIT/ISI

Microsoft

Microsoft hilft Ihnen, Ihr Netzwerk mit aktuellen, wirkungsvollen und kostenlosen Programmen zu schützen:

Mit dem monatlich aktualisierten „Windows-Tool zum Entfernen bösartiger Software", dem „Malicious Software Removal Tool" (MSRT), wurde bereits in über 16 Millionen Fällen schädliche Software, so genannte „Malware", aufgespürt und beseitigt. Lesen Sie mehr dazu in unserem White Paper, welches auf der Auswertung aktueller Daten basiert und die positiven Auswirkungen beim Einsatz effektiver Sicherheitsprogramme wie dem MSRT belegt. Das White Paper sowie die aktuellste Version des „Windows-Tools zum Entfernen bösartiger Software" stehen für Sie zum **kostenlosen Download** bereit.
Erfahren Sie mehr unter **www.microsoft.com/germany/sicherheit/isi**

Microsoft

103360