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 – daher 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"). Wichtige Kernpunkte dieses ersten Teils der Auswertung 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.

	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

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 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.

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.

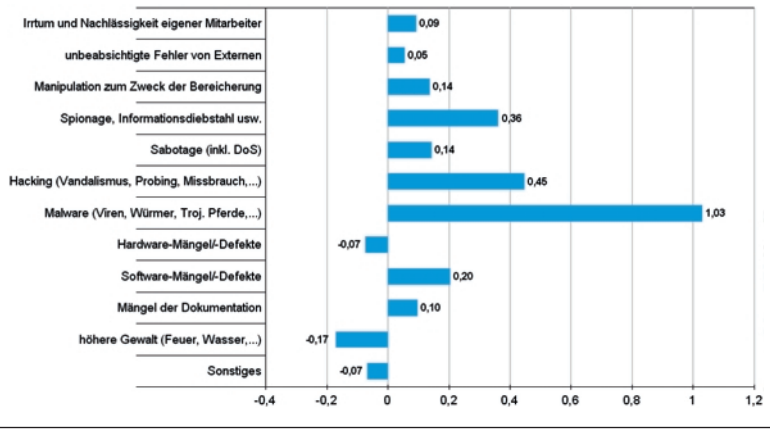


Abbildung 1: Prognostizierte Veränderung der Bedeutung der Gefahrenbereiche (Zusammenfassung)

Basis: Ø 130 Antworten

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,

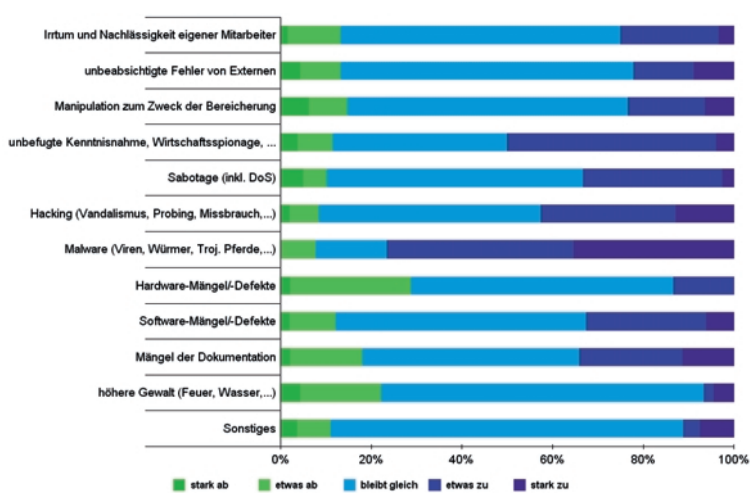


Abbildung 2: Prognosen zur Veränderung der Bedeutung von Gefahrenbereichen (Details)

Basis: Ø 130 Antworten

	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

Tabelle 2: Alternative Zusammenfassung der Gefahrenbereiche

Basis: s. Tab. 1

die sich in der alternativen Zusammenfassung der Gefahrenbereiche zu Unfällen und Angriffen zeigt (vgl. 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.

	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%

Tabelle 3: Malware-Vorfälle

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

	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

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

Tabelle 4: Infektionswege von Malware

Basis: Ø 128 Antworten

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 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).

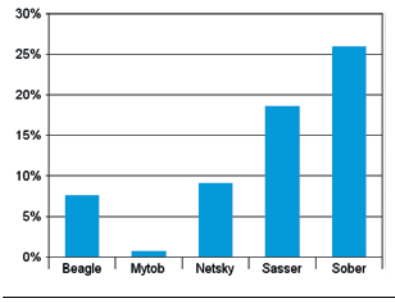
Malware

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 –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 Mal-



Basis: Ø 133 Antworten

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

Vielen Dank für freundliche Unterstützung unserer Studie

Microsoft
ASTRUM IT
itWatch GmbH
ROG
BorderWare
Jürgen Jakob Software-Entwicklung
AVG Anti-Virus
SAP
TRUST
PGP
»|secaron e.security solutions
entrada IT-Security
phion
SONICWALL
ibas Datenrettung Datenlöschung Computer Forensics
it.sec security for your information
proRZ professioneller Rechenzentrumsbau
TESIS SYSware

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.

	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

Tabelle 5: Aufwand durch Sicherheitsvorfälle

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

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%

Tabelle 6: Vertraulichkeitsbrüche

Basis: Ø 154 Antworten

	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%

Tabelle 7: Konsequenzen aus Vertraulichkeitsbrüchen

Basis: Ø 100 Antworten

ware-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.

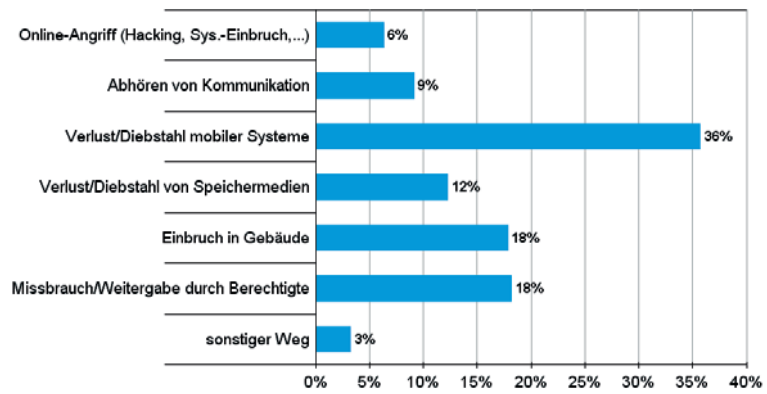


Abbildung 4: Sicher oder vermutlich durch Vetraulichkeitsbrüche Betroffene (Zusammenfassung zu Tab. 6)

Basis: Ø 154 Antworten

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 bearbeiten 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 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. 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.

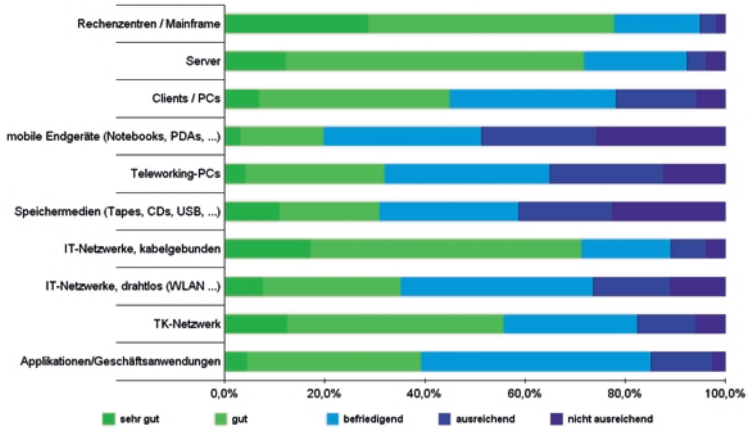
Eine grafische Zusammenfassung zu gesicherten und vermutlichen Brüchen der Vertraulichkeit über die erfragten Wege liefert Abbildung 4. Fasst man die verschiedenen genannten Möglichkeiten zusammen, so ergibt sich, dass 43 % der Befragten in den letzten Jahren vermutlich auf die eine oder andere Weise 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.

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%

Basis: 158 Antworten

Tabelle 8: Hindernisse für bessere Informations-Sicherheit

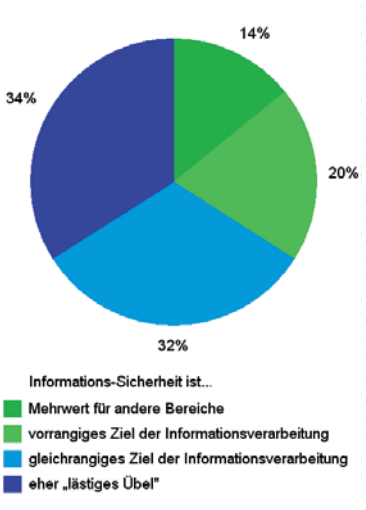


Basis: Ø 138 Antworten

Abbildung 5: Einschätzung der Sicherheit

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 ver-



Basis: 141 Antworten

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

bessert 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.

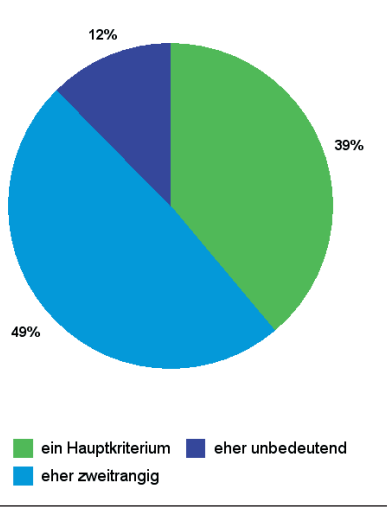


Abbildung 7: Bedeutung von Sicherheitsaspekten bei der Beschaffung von IT-Systemen

Basis: 162 Antworten

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.

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

	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%

Tabelle 9: Branchenzugehörigkeit der Studien-Teilnehmer

Basis: 160 Antworten

	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%

Tabelle 10: Funktion der Teilnehmer

Basis: 160 Antworten

Mitarbeiter insgesamt, 862 in der IT, 25 ISi-Spezialisten.

Die Verteilung der vertretenen Branchen zeigt Tabelle 9. 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. 10), 20 % sind als RZ-/IT-Leiter tätig, weitere 12 % als Geschäftsführer, wobei diese letzte Gruppe ausschließlich den KMU entspringt.

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.

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 9.

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.

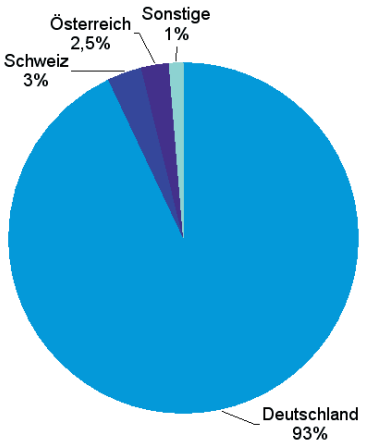


Abbildung 8: (Haupt-)Sitz der teilnehmenden Unternehmen und Behörden

Basis: 157 Antworten

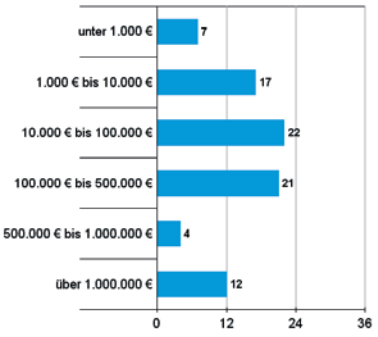


Abbildung 9: Budget für Informations-Sicherheit (Anzahl Nennungen)

Basis: 83 Antworten

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. 11). 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. €. ■

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

Tabelle 11: Geschätzter Verlust bei Vernichtung aller elektronisch gespeicherten Daten

Basis: 64 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.