Die Zeitschrift für Informations-Sicherheit

special

Auszüge aus <kes> 2014#4/6

Sonderdruck für apec applied security

IT-Landschaften 2014: Lagebericht zur Sicherheit

SecuMedia

Sehr geehrte Leserinnen und Leser der <kes>/Microsoft-Sicherheitsstudie,

seit mehr als 25 Jahren stellt die <kes>/Microsoft-Sicherheitsstudie Zahlen und Fakten zur Verfügung, die in ihrer Gesamtheit ein hervorragendes Lagebild der Informationssicherheit bei KMUs und Großunternehmen in Deutschland liefern.

Ein paar besonders interessante Fakten: 69% aller Opfer von Malware-Attacken geben an, dass der Vorfall durch ein anderes Verhalten von Mitarbeitern hätte verhindert werden können. Noch deutlicher sieht die Sache bei Informationsabflüssen und Datenlecks aus: 79% der befragten Unternehmen meinen, dass eigene Mitarbeiter zumindest eine Mitverantwortung an einem Datenabfluss gehabt hätten. Mangelndes Sicherheitsbewusstsein und mangelnde Mittelausstattung nehmen erneut Top-Positionen bei den Gründen für lückenhafte Informationssicherheit ein, sogar in steigender Tendenz gegenüber der letzten Studie von 2012. Ebenso, wenn auch ganz leicht rückläufig, wird mangelnde Unterstützung im Top-Management für Themen der Informationssicherheit beklagt.

Solche Einschätzungen zu liefern ist eine besondere Eigenschaft der Studie. Sie erhebt nicht nur die reinen Fakten etwa über Sicherheitsvorfälle, Budgets für IT-Sicherheit oder eingesetzte technische Maßnahmen, sondern fragt auch nach Einschätzungen über die Bedrohungslage und deren zukünftige Entwicklung. Diese subjektiven Einschätzungen offenbaren einen ganz wesentlichen Aspekt der Informationssicherheit: die menschliche Komponente. Insbesondere die Gefühlslage der Protagonisten im Umgang mit einem sperrigen Thema wie Informationssicherheit lässt sich in den zählbaren Fakten selten messen. Jedoch sind Gefühle ein wichtiges Leitsystem des menschlichen Handelns. Die Motivation, etwas zu tun oder auch nicht zu tun, hängt sehr stark davon ab, wie wir uns dabei fühlen.

Die Gefühle besonders in Wallung brachten seit 2013 die Snowden-Enthüllungen zur NSA-Überwachung. Wer jedoch glaubte, diese hätten für ein gesteigertes Sicherheitsbewusstsein gesorgt, sieht sich getäuscht.

Mich überrascht das nicht. Eine menschliche Grundtendenz ist der Glaube an das Gute. „Mich wird's schon nicht treffen", denken die meisten von uns, wenn es um Risiken geht. Vor allem dann, wenn die persönliche Betroffenheit nicht evident ist und wenn die Konsequenzen eines Schadensfalls nicht unmittelbar eintreten. Das ist einerseits gut, denn Angst ist ein schlechter Ratgeber und übertriebene Angst verhindert, dass wir überhaupt handeln. Andererseits erhöht ein wenig Angst die Wachsamkeit und verhindert, dass wir in Fallen tappen. Der CISO, der es schafft, seinen Mitarbeitern und auch seinen Managern das Gefühl zu vermitteln, dass alles gut wird, wenn alle im Umgang mit IT-Systemen und Daten wachsam sind, findet den heiligen Gral der Informationssicherheit. Unternehmen sollten darüber nachdenken, als Kernqualifikation für den oder die CISO weniger Technik und mehr Kenntnisse in Psychologie zu fordern.

In diesem Sinne wünsche ich Ihnen wertvolle Erkenntnisse beim Lesen der Studie. Es lohnt sich.

Ihr Dr. Volker Scheidemann

Für Fragen stehen wir Ihnen jederzeit gerne zur Verfügung unter:

Applied Security GmbH, Einsteinstraße 2a, 63868 Großwallstadt, Tel. +49 (6022) 263380, www.apsec.de

IT-Landschaften 2014:
Lagebericht zur Sicherheit

Verlässliche und neutrale Zahlen zur Informations-Sicherheit (ISi) im deutschsprachigen Raum sind selten – konkrete Angaben zu aufgetretenen Schäden und Budgets erst recht. Die Grundlage für die hier vorliegenden Daten haben die Teilnehmer an der diesjährigen <kes>/Microsoft-Sicherheitsstudie im Rahmen einer selbstkritischen Bestandsaufnahme durch ihre Arbeit mit dem Studien-Fragebogen gelegt.

Die umfassenden und vertrauensvollen Angaben aller Studienteilnehmer sind ebenso wie die Unterstützung durch Sponsoren und Partner der <kes>/Microsoft-Sicherheitsstudie unabdingbare Voraussetzung für die vorliegende Auswertung. Daher zunächst erstmal herzlichen Dank für diese Mithilfe! In diesem Jahr sind erneut 133 verwertbare Fragebögen eingegangen – die „größere Hälfte" davon kam dieses Mal aus Organisationen ab 500 Mitarbeitern (50 %), doch auch kleine und mittlere Unternehmen (KMU) sind mit 45 % stark vertreten – 5 % haben keine Angabe zu Mitarbeiterzahlen gemacht (vgl. Abschnitt „Teilnehmer" ab S. 25).

Einige Kernaussagen lauten zusammengefasst:

_____ Malware verdrängt „Irrtum und Nachlässigkeit eigener Mitarbeiter" auf Platz Zwei der bedeutendsten Gefährdungen – Hacking-Attacken steigen erheblich in der Beachtung.

_____ Die Malware-Abwehr musste in den vergangenen zwei Jahren offenbar Rückschläge hinnehmen: Trotz tendenziell sinkender Vorfallszahlen gab es bei einem gestiegenen Anteil der Befragten nennenswerte Probleme mit Malware.

_____ Es fehlt wieder häufiger an Geld/Budget, um die Informations-Sicherheit zu verbessern – häufigstes Hindernis bleibt jedoch mangelndes Bewusstsein bei Mitarbeitern.

_____ Die schlechteste Sicherheitseinschätzung erhalten erneut mobile Endgeräte sowie Speichermedien – industrielle IT-Systeme liegen auf dem Niveau von Telearbeitsplätzen.

_____ Erneut war mehr als die Hälfte der Befragten mutmaßlich Opfer von Vertraulichkeitsbrüchen – als wichtigste Ursache trat die neue Kategorie „Datenlecks/Probleme bei Partnern" auf, gefolgt vom Verlust und Diebstahl von Speichermedien sowie mobilen Systemen.

Risikosituation

Die vorliegende Studie ist nicht repräsentativ für alle Unternehmen im deutschsprachigen Raum – und will das auch gar nicht sein, denn die zu vermutende Betonung auf Organisationen, die sich besonders um die Informations-Sicherheit bemühen, liefert letztlich sogar passendere Zahlen für unsere Zielgruppe. Dass sich dabei wechselnde Stichproben über die Jahre hinweg immer wieder großenteils gegenseitig bestätigen, belegt einerseits einen „Common Sense" in der Teilnehmerschaft und untermauert andererseits die Qualität der erhobenen Daten.

In 13 von 14 früheren Studien hätte diese Vorbemerkung die Aussage eingeleitet, dass die aktuelle Auswertung entgegen anderslautenden Erwartungen der vorherigen Teilnehmer weiterhin „Irrtum und Nachlässigkeit eigener Mitarbeiter" als Top-Bedrohung nennt. Nicht so dieses Jahr, wo sich zum nunmehr zweiten Mal – wie regelmäßig prognostiziert – die Malware tatsächlich auf Rang 1 schiebt (Tab. 1 „Bedeutung"). In den vergangenen zwei Jahren haben sich also die massiven Befürchtungen der Studienteilnehmer hinsichtlich einer verstärkten Bedrohung durch Malware (und auch anderer Angriffe) verfestigt und zu einer fortwährend hohen Priorisierung geführt.

Anders als 2008, als das erstmalig geschah, führt heuer die Malware auch die Rangliste der von tatsächlichen Schäden Betroffenen in der Stichprobe an: Nunmehr 31 % der Teilnehmer (+3 %-Pkt.) hatten in den Jahren 2012 und 2013 mittlere bis größere Beeinträchtigungen durch diese Gefährdung zu verzeichnen (vgl. Tab. 1 „Schäden") – auch der Anteil der generell von Malware-Vorfällen Betroffenen, liegt mit +11 Prozentpunkten deutlich über dem Wert der vorausgehenden Stichprobe (siehe Abschnitt „Malware" ab S. 6).

	Vorhersage 2012		Bedeutung heute		akt. Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Malware (Viren, Würmer, Troj. Pferde, ...)	1	1,04	1	1,03	1	1,06	1	31%
Irrtum und Nachlässigkeit eigener Mitarbeiter	2	0,82	2	0,81	2	0,76	2	30%
Hacking (Vandalismus, Probing, Missbrauch, ...)	4	0,66	3	0,70	4	0,70	6	20%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,66	4	0,68	3	0,73	8	10%
Software-Mängel/-Defekte	5	0,63	5	0,53	5	0,51	3	26%
Mängel der Dokumentation	6	0,51	6	0,50	6	0,51	5	21%
unbeabsichtigte Fehler von Externen	9	0,32	7	0,40	7	0,42	7	20%
Sabotage (inkl. DoS)	8	0,34	8	0,35	8	0,37	11	8%
Manipulation zum Zweck der Bereicherung	7	0,48	9	0,34	9	0,35	10	9%
Hardware-Mängel/-Defekte	10	0,32	10	0,31	10	0,33	4	25%
höhere Gewalt (Feuer, Wasser, ...)	11	0,11	11	0,14	11	0,12	9	10%
Sonstiges	12	-0,01	12	0,04	12	0,01	12	4%

Tabelle 1: Bedeutung der verschiedenen Gefahrenbereiche

Basis: 133 Antworten (Bedeutung), Ø 132 (Prognose), Ø 128 (Schäden), Ø 128 (Vorhersage 2012)

Nennenswerte Schäden gab es zwar auch weiterhin nicht selten durch „Irrtum und Nachlässigkeit eigener Mitarbeiter“ (bei 30 %); ein Rückgang um –10 %-Pkt. gegenüber der vorigen Studie lässt die beschriebene Veränderung in der Top-Priorität jedoch als durchaus angemessen erscheinen. Betrachtet man die anderen Priorisierungen, so erfahren – wie üblich – die Angriffskategorien eine höhere Beachtung als ihr Rang in der Schadensstatistik erwarten ließe. Hier sei erneut darauf hingewiesen, dass naturgemäß eine gute Vorsorge das Auftreten tatsächlicher Schäden begrenzt haben könnte, sodass nicht automatisch eine Überbewertung zu unterstellen ist.

Dass hier kein allgemeiner Übereifer in der Bewertung aller Angriffsszenarien vorliegt, zeigt sich auch in der geringeren Priorisierung von „Manipulationen zum Zweck der Bereicherung“ (–2 Ränge), der – zusammen mit einer ebenfalls geringeren Bedeutung für Hardware-Mängel/-Defekte – auch der Aufstieg von Sabotageakten in der Rangfolge geschuldet ist (+2 Ränge). Tatsächlich bleibt die normierte Priorität (s. u.) dieser Gefährdungsklasse auf nahezu demselben Wert wie 2012 (Ähnliches gilt für „unbeabsichtigte Fehler von Externen“).

Der größte Zuwachs in der Bedeutung ist bei der Klasse „Hacking“ (inkl. Vandalismus, Probing, Missbrauch, ...) zu beobachten, die gleich um drei Ränge aufgestiegen ist. Durch eine leichtere Aufmerksamkeitssteigerung konnten Spionageakte („unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage“) dennoch ihren vierten Rang in der Bedeutung halten, während Software-Mängel und -Defekte etwas schwächer bewertet auf Platz 5 (–2 Ränge) absacken – und somit etwas hinter ihrer Bedeutung in der Schadensstatistik zurückbleiben. Auch Dokumentationsmängel werden bei nahezu gleicher Bewertung um einen Rang verdrängt.

Riskanter erscheint jedoch die schwache Beachtung von Hardware-Problemen (–2 Ränge), die noch immer bei einem Viertel der Befragten auch mindestens einmal zu nennenswerten Schäden geführt haben (allerdings –10 %-Pkt. vs. 2012) und zudem in der Frage zum größten Schadensereignis (s. S. 31) auf einem klaren dritten Platz landeten.

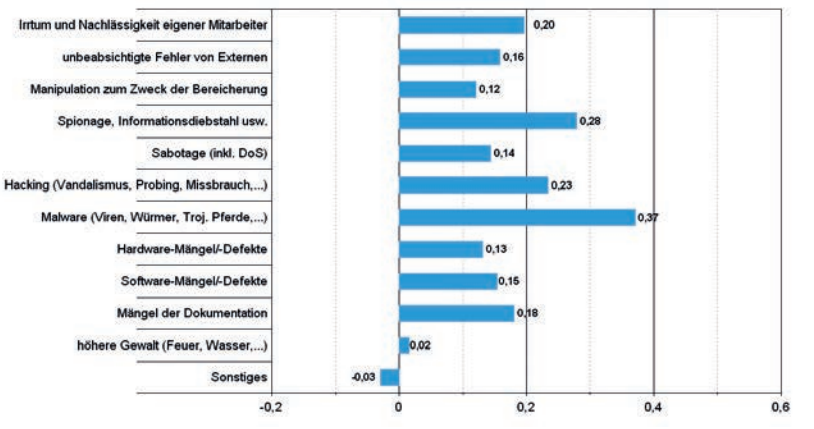


Abbildung 1: Prognostizierte Veränderung der Bedeutung der Gefahrenbereiche (Zusammenfassung)

Basis: Ø 132 Antworten, 100 (Sonstiges)

Unfälle vs. Angriffe

Vergleicht man die aufsummierten Prioritäten von „Unfällen“ (menschliches oder technisches Versagen) mit denen der „Angriffe“ (vorsätzliche Handlungen und Malware), so zeigt sich wieder einmal das in den meisten <kes>-Studien zu beobachtende „Übergewicht“ der aggressiven Kategorien (Tab. 2).

Dieses Mal ist der Unterschied mit 2,54:3,10 sogar noch deutlicher als im ebenfalls „malwarebetonten“ Jahr 2008 (2,68:2,94). Das korrespondiert allerdings auch mit einem geringeren „Überhang“ der mindestens einmal von Unfallschäden Betroffenen: In vergangenen

Studien war die summierte Zahl der „Jas“ bei nennenswerten Schäden durch Unfallkategorien meist mehr als doppelt so hoch wie diejenige der mittleren bis größeren Beeinträchtigungen durch Angriffskategorien – dieses Mal liegt hier das Verhältnis „nur“ bei ungefähr 3:2.

Die summierten Angaben von KMUs und großen Unternehmen unterscheiden sich dabei übrigens nur in geringem Maße. Allerdings legen die „Großen“ eine noch etwas stärkere Betonung auf die Abwehr gezielter Angriffe und achten bei den „Unfällen“ etwas mehr auf den Menschen als auf die Technik (bei den KMU ist das umgekehrt). Auch in den Einzelangaben zur Bedeutung genießen menschliche Irrtümer bei den Großen mehr Aufmerksamkeit als bei KMU – dennoch bleibt auch dort die Malware knapp an der Spitze der Bedrohungen. Den KMU liegen indessen Hardware-Mängel und -Defekte noch deutlich stärker am Herzen als den großen Unternehmen und auch Sabotageakte erhalten mehr Aufmerksamkeit.

Hintergrund der genannten Prioritäten ist die Annahme, dass man bei begrenzten Ressourcen für die Informationssicherheit immer Schwerpunkte setzen muss. Früher hatten wir daher die Teilnehmer direkt gebeten, sechs „Prioritätspunkte“ auf die einzelnen Gefahrenklassen zu verteilen und dabei nicht mehr als drei auf einen Bereich zu kumulieren. Um das Verfahren einfacher und flexibler zu gestalten, fragen wir seit 2008 nach „höchster“, „erhöhter“ oder „normaler/keiner“ Priorität für jeden Bereich – diese Angaben werden dann mit 3/1/0 Punkten bewertet. Im Mittel haben die Teilnehmer dieser Studie auf diese Weise (wie schon in den Vorjahren) 8–9 Punkte vergeben, die anschließend für jeden Fragebogen individuell auf sechs Punkte normiert wurden; deren Durchschnitt findet sich in den Tabellen 1 und 2 als „Priorität“.

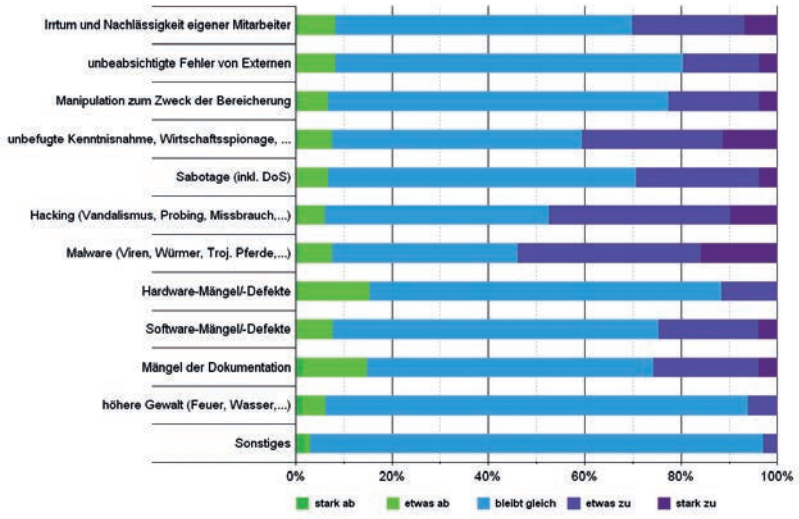


Abbildung 2: Prognostizierte Veränderung der Bedeutung der Gefahrenbereiche (Details)

Basis: Ø 132 Antworten, 100 (Sonstiges)

Prognosen damals und heute

Wie schon angemerkt stimmen die Prognosen von 2012 mit den aktuellen Prioritäten sehr stark überein (vgl. Tab. 1 „Vorhersage“) – die größte Abweichung zeigen Betrügereien (Manipulationen zum Zweck der Bereicherung), die zwei Ränge hinter den Erwartungen zurückgeblieben sind. „Unbeabsichtigte Fehler von Externen“ wurden hingegen stärker bewertet und die fast gleich prognostizierten Kategorien Hacking und Spionage tauschen bei weiterhin geringer Differenz die Plätze.

Ähnliches gilt für den Ausblick in die Zukunft (Tab. 1 „akt. Prognose“), wo ebenfalls nur an einer Stelle zwei nah beieinanderliegende Gefährdungen die Ränge tauschen. Angesichts dessen, dass die aktuelle Einschätzung sehr gut den üblichen Prognosen entspricht, verwundert es denn auch kaum, dass die fortan erwarteten Veränderungen in Summe deutlich geringer ausfallen als üblich (Abb. 1) – die jeweils erwarteten Zu- und Abnahmen der einzelnen Gefährdungen zeigt Abbildung 2 auch im Detail.

Kosten und Aufwand von Vorfällen

Betrachtet man alle Angaben zur geschätzten Häufigkeit von Sicherheitsvorfällen und Fehlalarmen sowie der damit verbundenen Kosten und Ausfallzeit, so zeigen sich extreme Unterschiede, da alle Kategorien mit Null-Schätzungen beginnen, die Maximalwerte teils aber in enorme Höhen schnellen (Tab. 3).

Daher ergänzen wir seit einiger Zeit für die Fallzahlen eine Alternativrechnung unter Auslassung der „Optimisten“ (Nullwerte) sowie der „Problemfälle“ (2–3 schlimmste Einzelangaben). Damit ergeben sich aus den Angaben der aktuellen Stichprobe im jährlichen Mittel 41 Virus-/Wurm-Infektionen (2012: 16,

	Priorität	Schäden	
		min. 1 bei	Nennungen
Unfälle	**2,54**	**73%**	**158**
... Mensch	1,21	41%	65
... Technik	1,33	44%	93
Angriffe	**3,10**	**51%**	**102**
... ungezielt	1,03	31%	41
... gezielt	2,07	35%	61

Tabelle 2: Zusammenfassung der Gefahrenbereiche

Basis: siehe Tab. 1

Tabelle 3: Geschätzter Aufwand durch Sicherheitsvorfälle

	Häufigkeit		Ausfallzeit		Kosten	
	Durchschnitt	max. Wert	Durchschnitt	max. Wert	Durchschnitt	max. Wert
Virus-/Wurm-Infektion	76 p.a.	2.500 p.a.	87 Std.	1.600 Std.	5.702 €*	15.000.000 €
Malware-Fehlalarm	52 p.a.	2.000 p.a.	9 Std.	160 Std.	620 €	10.000 €
unbegründete Warnung (Hoax)	31 p.a.	1.500 p.a.	55 Std.	2.400 Std.	1.644 €	50.000 €
gezielter Angriff auf / über / mit IT	1.291 p.a.	100.000 p.a.	27 Std.	1.000 Std.	15.861 €	300.000 €

Basis: Ø 92 Antworten (Häufigkeit), Ø 64 (Ausfallzeit), Ø 52 (Kosten)

* unter Auslassung des Maximalwerts

2010: 40, 2008: 70), 22 Fehlalarme (2012: 20, 2010: 24, 2008: 40), 14 Hoaxes (2012: 9, 2010: 20, 2008: 20) sowie 10 gezielte Angriffe (2012: 13, 2010: 4, 2008: 3).

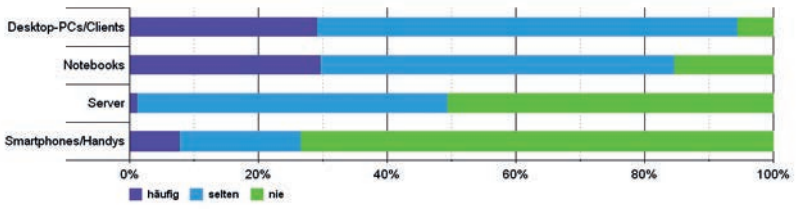
Die Fallzahlschätzungen der großen Unternehmen liegen naturgemäß deutlich über denen der KMU – auch höhere Kosten und Ausfallzeiten sind zu erwarten: Während Unternehmen mit unter 500 Mitarbeitern für eine Malware-Infektion im Mittel nur 634 € veranschlagt haben, schlägt das bei den Großen schon mit fast 11 Tsd. € zu Buche. Ein Fehlalarm kostete KMU durchschnittlich geschätzte 233 € (Große 1062 €), ein Hoax sogar nur 86 € (Große 3493 €) und ein gezielter Angriff 1765 € (Große knapp 33 Tsd. €). Wie immer ist hierbei zu bedenken, dass die Schätzungen zu Kosten und Ausfallzeiten nur auf den Angaben relativ weniger Teilnehmer beruhen, was eine höhere Abhängigkeit von der jeweiligen Stichprobe bedeuten kann.

Tabelle 4: Konsequenzen aus „größten" Schadensfällen

	ja, bei
organisatorische Konsequenzen gezogen	72%
bestehende Mechanismen verstärkt	71%
Angriffspunkte beseitigt	70%
Sicherheitsmechanismen neu eingerichtet	67%
Produkt-/Anbieterwechsel vollzogen	20%

Basis: Ø 90 Antworten

Abbildung 3: Betroffene Systeme in Organisationen mit Malware-Vorfällen



Basis: Ø 81 Antworten

Größtes Schadensereignis

Neun Teilnehmer gaben an, dass es in ihrem Haus in den vorangegangenen zwei Jahren kein oder kein nennenswertes Schadensereignis gegeben hat; 88 weitere waren nicht in dieser glücklichen Lage und schilderten entsprechende Vorfälle. Bei fast einem Drittel von ihnen ging das schlimmste Vorkommnis auf Malware zurück (26 Nennungen – nachträglich aus Freitextangaben kategorisiert), ungewöhnlicherweise direkt gefolgt von verschiedenen Arten von Angriffen bei insgesamt 16 Teilnehmern (inkl. vier Insider-Attacken).

Probleme mit Hardware standen an dritter Stelle (10 Nennungen), fünfmal waren Unterbrechungen der Stromzufuhr Schuld am schlimmsten Schaden, je vier Vorfälle gingen auf menschliches Versagen, Softwareprobleme und Elementarschäden zurück. Ferner verzeichneten immerhin zwei Teilnehmer die größten Schäden der jüngeren Vergangenheit aufgrund von Fehlalarmen oder Hoaxes – 17 Angaben waren auf sonstige Ursachen zurückzuführen oder nicht kategorisierbar.

Im Mittel haben diese schlimmsten Schäden unter Auslassung eines extremen Ausreißerwerts rund 54 Tsd. € an direkten Kosten verursacht (KMU 8 Tsd. € / Große 105 Tsd. €) – die durchschnittliche Ausfallzeit betrug 18 Stunden (16 Std. / 22 Std.). Die jeweils in der Folge der Vorfälle getroffenen Konsequenzen zeigt Tabelle 4.

Malware

Wie bereits erwähnt ist die Malware-Lage in der aktuellen Erhebung kritischer als in den vorigen Studien: 74 % generell von Malware-Vorfällen Betroffene (58 % KMU / 89 % Große) sind deutlich mehr als vor zwei Jahren (+11 %-Pkt. – KMU +5 %-Pkt. / Große +12 %-Pkt.). Hier wurde nun wieder das Niveau von 2006 (72 %) und 2002 (74 %) erreicht, auch wenn der Spitzenwert von 2004 (88 %) noch unangefochten bleibt. Die mittleren bis größeren Beeinträchtigungen durch Malware haben ebenfalls nach langer Zeit erstmals wieder etwas deutlicher zugelegt (+3 %-Pkt.).

Gleichzeitig haben mehr Befragte als zuvor für das fragliche Jahr einen *Rückgang* der Vorfallszahlen angegeben: Bei 67 % gab es 2013 weniger Malware-Incidents als 2012 (KMU 60 % / Große 70 %) – zum Vergleich: Vor zwei Jahren war das bei 52 % der Fall, 2010 und 2008 bei 54 %. Die Fallzahlschätzungen erreichen ebenfalls „nur" das Niveau von 2010 (s. o.) – und die Schätzungen der vorigen Studie hatten ohnehin ein unerwartetes Tief markiert und sind zudem mutmaßlich größeren Schwankungen aufgrund der Stichprobe unterworfen.

Dennoch muss man einen Rückschlag in der Malware-Abwehr konstatieren – die seit 2006 in unseren Studien vertretene These

„erhebliches Problem, aber der viele Aufwand trägt zunehmend Früchte“ gerät zumindest für die vergangenen zwei Jahre ins Wanken. Vielmehr lassen sich die aktuellen Zahlen so interpretieren, dass hier die Angreifer auf „Klasse statt Masse“ setzen und bei tendenziell weiterhin rückläufigen Fallzahlen nun eine größere Zahl von Attacken wieder die Abwehr durchbricht, sodass insgesamt ein größerer Anteil der Befragten als zuvor von mindestens einem Malware-Vorfall betroffen war – und auch etwas mehr Teilnehmer nennenswerte Schäden zu verbuchen hatten.

	häufig	selten	nie	Bedeutung*
E-Mail	30%	50%	20%	1,40
WWW-Seite (aktive Inhalte)	27%	55%	18%	1,37
unerwünschte Anwendungen	23%	46%	30%	1,16
Speichermedien	21%	42%	38%	1,04
Internet (Würmer)	17%	44%	39%	0,95
mobile Endgeräte	10%	43%	47%	0,72
unbekannte Herkunft **	5%	26%	21%	0,42
internes Netz / Intranet (Würmer)	2%	27%	71%	0,32

Basis: Ø 112 Antworten, 59 (unbekannte Herkunft, prozentuiert auf Mittel der anderen Antworten)**

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

Tabelle 5: Infektionswege von Malware

Betrachtet man die Infektionswege in die Unternehmen hinein (Tab. 5), so liegt die E-Mail weiterhin an der Spitze – WWW-Inhalte, die eine Infektion über aktive Inhalte oder „Drive-by“-Attacken bewirken, gewinnen deutlich an Bedeutung (+12 %-Pkt. „häufig“ oder „selten“)

Wir danken den Sponsoren unserer Studie

Weiterhin gilt unser Dank den Verbänden und Anwendervereinigungen, die den Fragebogen der Studie ihren Mitgliedern zugänglich machen, sowie allen Teilnehmern an der Befragung, die durch ihre wertvolle Mitarbeit überhaupt erst ein sinnvolles Gesamtbild entstehen lassen.

Für technisch-organisatorische Unterstützung bedanken wir uns bei der OTARIS Interactive Services GmbH (Hosting von Onlinefragebogen und Erfassung) sowie der humanIT Software GmbH (Software für Auswertung und Grafikerstellung).

unbefugter Zugriff durch	ja		nein		sicher oder vermutlich ja	
	sicher	vermutlich	vermutlich	sicher	2014	2012
Datenlecks/Probleme bei Partnern	7%	22%	59%	12%	29%	–
Verlust/Diebstahl von Speichermedien	10%	18%	41%	31%	28%	22%
Verlust/Diebstahl mobiler Systeme	12%	16%	31%	42%	27%	23%
Social Engineering / Phishing / Unachtsamkeit	8%	17%	65%	10%	25%	25%
Missbrauch/Weitergabe durch Berechtigte	4%	13%	66%	17%	18%	24%
Online-Angriff	7%	8%	60%	24%	15%	14%
Abgehörte Kommunikation	2%	12%	70%	16%	15%	10%
Einbruch in Gebäude	9%	2%	28%	62%	10%	8%

Tabelle 6: Vertraulichkeitsbrüche

Basis: Ø 123 Antworten (2012: Ø 130)

und landen nunmehr auf Platz Zwei. Speichermedien (+8 %-Pkt. „nie“) und Internet-Würmer (+7 %-Pkt. „nie“) waren hingegen seltener ein Problem.

Auf die Frage, ob abweichendes Nutzer-Verhalten einen nennenswerten Teil der Vorfälle hätte vermeiden können, antworteten erneut über zwei Drittel aller Teilnehmer mit Ja (69 % – 2012: 67 %). Von den großen Unternehmen waren sogar 78 % dieser Meinung – bei den KMU immerhin noch 59 %. Die Verteilung der häufig, selten oder nie von Infektionen betroffenen Systeme in Organisationen mit Malware-Vorfällen zeigt Abbildung 3 (S. 6).

Vertraulichkeitsbrüche

Erneut war etwas mehr als die Hälfte aller Befragten vermutlich von mindestens einem Vertraulichkeitsbruch betroffen – wie schon vor zwei Jahren haben bei 53 % mindestens einmal „vermutlich“ oder „sicher“ Unbefugte Zugriff auf schutzwürdige Daten erlangt. Tabelle 6 zeigt als „Spitzen-Leck“ die erstmals erfragten Probleme bei Partnern – auch mobile Speichermedien und Systeme sind in der Bedeutung gestiegen. Einen Rückgang im Vergleich zu 2012 zeigte die aktuelle Stichprobe nur bei „Missbrauch und Weitergabe durch Berechtigte“.

Positiv ist zu vermelden, dass dieses Mal ein etwas kleinerer Anteil der Teilnehmer *sicher* von einem Datenleck betroffen war: Heuer gaben nur 27 % in mindestens einer Kategorie „sicher ja“ an (2012: 32 %, 2010: 30 %, 2008: 26 %, 2006: 31 %). Und immerhin sechs Teilnehmer hatten in *allen* Kategorien gesicherte Erkenntnisse, dass *kein* Problem aufgetreten war (2012: drei).

Die Konsequenzen nach Datenlecks zeigt Tabelle 7: Technische und organisatorische Maßnahmen führen diese Liste weiterhin mit Abstand an. Auch Imageschäden blieben mit 28 % auf dem hohen Niveau der beiden letzten Studien (2012: 27 %, 2010: 26 %, 2008: 20 %, 2006: 17 %). Wieder angestiegen sind externe Sanktionen gegenüber dem betroffenen Haus oder Mitarbeiter, die jetzt von 12 % angegeben wurden (2012: 6 %, 2010: 7 %, 2008: 13 %, 2006: 11 %). Auffällig hoch ist dieses Jahr der Anteil der Teilnehmer, in deren Haus es nach mutmaßlichen oder tatsächlichen Vorfällen *keinerlei* Konsequenzen gab: Fast ein Viertel (23 %) gab an, es hätte sich nichts getan (2012: 12 %).

	ja, bei
technische/organisatorische Maßnahmen	53%
Imageschaden	28%
Strafanzeige gegen Verursacher	27%
personelle Maßnahmen	23%
missbräuchliche Verwendung durch Dritte	20%
verlorene Kunden/Aufträge	13%
externe Sanktionen gegenüber eigenem Haus/Mitarbeiter	12%
Sonstige	15%
keinerlei Konsequenzen	*23%*

Tabelle 7: Konsequenzen aus Vertraulichkeitsbrüchen

Basis: 60 Antworten

Mitschuld von Mitarbeitern

Erstmals haben wir in einem weiteren Fragenkomplex versucht, Gründe für Vertraulichkeitsbrüche näher zu erörtern. Auf die Frage, ob eigene Mitarbeiter für die meisten Datenlecks (mit-)verantwortlich sind, antwortete mit 79 % eine erschlagende Mehrheit „ja“ – dabei gab es auch keine größeren Unterschiede zwischen KMU (77 %) und großen Unternehmen (81 %).

Als Hauptgrund für diese Mitschuld vermuteten 91 %, dass sich die betreffenden Mitarbeiter der Konsequenzen nicht bewusst waren. Auch Datenschutz- und Sicherheitslösungen standen in der Kritik: 73 % glauben, dass eine Mitverantwortung für Datenlecks entsteht, weil die Mitarbeiter die komplizierten Systeme nicht verstehen – mangelnde Kenntnis von Firmen-Policies sahen 53 % als Grund. Dass Mitarbeiter dem Unternehmen bewusst schaden wollen, vermuteten immerhin noch 14 % der Befragten.

Ebenfalls erstmalig haben wir nach der dienstlichen Nutzung von Filesharing-Diensten gefragt, die eher auf den privaten Gebrauch zugeschnitten sind (z. B. Dropbox): Nur exakt die Hälfte der Teilnehmer meint, das würde „nie“ passieren (KMU 55 % / Große 44 %) – „häufig“ geschehe das hingegen bei 7 % der KMU und 18 % der großen Unternehmen (13 % über das ges. Teilnehmerfeld). Die verbleibenden Angaben plädierten auf „selten“ (KMU und Große je 38 % – alle 36 %). Dabei ist eine solche Nutzung in 44 % der KMU und 69 % der großen Unternehmen explizit verboten (58 % über die ges. Stichprobe).

Sicherheitslage

Kaum Überraschungen liefert wie üblich die Frage nach der Selbst-Einschätzung der Sicherheit verschiedener Infrastruktur-Teile (Abb. 4): Wie üblich erhielt die zentrale IT (Mainframes/RZ und Server) als Durchschnittsnote eine knappe Zwei, gefolgt von kabelgebundenen Netzen und klassischen Client-/PC-Systemen – letztere mit einem leichten Plus gegenüber der vorigen Studie (+9 %-Pkt. „gut"/„sehr gut"). Die nächste Gruppe bilden Applikationen/Geschäftsanwendungen, TK-Netze, Notebooks (+7 %-Pkt. „gut"/"sehr gut") sowie drahtlose IT-Netze (WLAN, UMTS usw.) mit einer „Drei Plus".

Die viel gescholtene Prozess-, Automations- und Leittechnik, die wir erstmals in diese Frage aufgenommen haben, konnte sich mit einer guten Drei gar nicht einmal so schlecht positionieren. Eine glatte Drei erhalten zudem im Mittel die Teleworking-PCs, die nach einem besseren Abschneiden in der vorigen Stichprobe nun wieder auf die Bewertung von 2010 zurückfallen (–11 %-Pkt. „gut"/„sehr gut" vs. 2012). Mit weniger als einem Viertel „gut" oder „sehr gut" landen Smartphones und Tablets („Drei minus") sowie Speichermedien („Drei bis Vier") erneut am Ende der Skala – beide erhielten von rund der Hälfte aller Teilnehmer keine befriedigenden Bewertungen.

Vergleicht man die Antworten aus KMU und großen Unternehmen, sehen sich die KMU fast durchweg minimal sicherer als der Durchschnitt aller Teilnehmer. Lediglich bei Mainframes/Rechenzentren sowie TK-Netzen (ggf. inkl. VoIP-Systemen) haben große Unternehmen leicht die Nase vorn – die größten Differenzen nach unten zeigten sich bei Teleworking-PCs und Speichermedien, wo die Großen sich etwa eine Viertelnote schlechter einschätzen als die KMU.

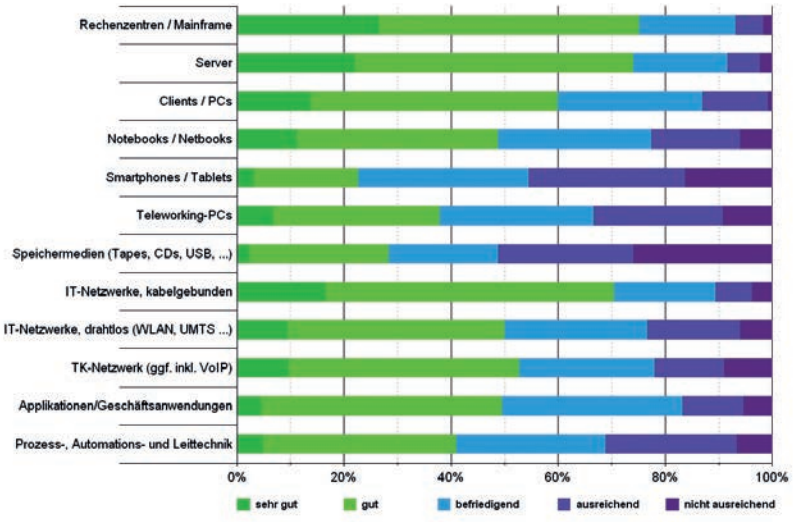


Abbildung 4: Einschätzung der Sicherheit im eigenen Hause

Basis: Ø 126 Antworten, 87 (Teleworking-PCs), 61 (Industrial-IT)

Konzepte

Einen neuerlichen Spitzenwert im langjährigen Vergleich zeigt der Anteil der Teilnehmer, in deren Haus eine schriftliche ISi-Strategie existiert (Tab. 8): Nunmehr 81% über das gesamte Feld bedeuten einen nochmaligen Zuwachs von +7 %-Punkten gegenüber der vorangegangenen Studie (Große 91 %/+2 %-Pkt. – KMU 69 %/+5 %-Pkt.).

Der größte Zuwachs spezifischer Konzepte und Richtlinien war bei Cloud- und Web-Services zu beobachten (+15 %-Pkt.). Auch bezüglich der Nutzung mobiler Endge-

Gibt es im Unternehmen... ?	ja	bei Unternehmen mit ISi-Strategie	bei Unternehmen ohne ISi-Strategie
schriftliche Strategie zur Informations-Verarbeitung (IT-Betrieb)	78%	93%	12%
schriftliche Strategie zur Informations-Sicherheit	81%	100%	0%
spezifische Konzepte/Richtlinien			
... zur Handhabung sensitiver/kritischer Daten	71%	85%	12%
... zur Weitergabe/Bereitstellung von Daten an berechtigte Dritte	70%	84%	12%
... zur Nutzung von Cloud-/Web-Services (inkl. SOA, SaaS, ...)	41%	48%	12%
... zur E-Mail-Nutzung	81%	90%	44%
... zur Nutzung von Web 2.0, Social Networks, ...	52%	60%	20%
... zur Gestaltung/Nutzung von Passwörtern	79%	92%	24%
... zum Softwareeinsatz auf PCs	77%	88%	32%
... zum Einsatz von Verschlüsselung / elektronischen Signaturen	57%	66%	16%
... zur Nutzung mobiler Endgeräte	71%	81%	29%
... zur Nutzung mobiler Speicher und Plug&Play-Peripherie	64%	75%	20%
... zur dienstlichen Nutzung privater IT-Systeme	66%	74%	32%
... Sonstige	12%	14%	0%
Die (fortdauernde) Eignung von Konzepten/Richtlinien wird geprüft	91%	97%	68%
schriftlich formulierte ISi-Maßnahmen	70%	83%	20%
Die Einhaltung vorgesehener Maßnahmen wird geprüft	88%	95%	56%
Übereinstimmung von Richtlinien und Praxis			
... organisatorisch [Schulnote]	3,00	2,93	3,25
... technisch [Schulnote]	2,46	2,39	2,71

Tabelle 8: Strategien, Richtlinien und Konzepte

Basis: Ø 130 Antworten, 100 (schriftl. Maßnahmen)

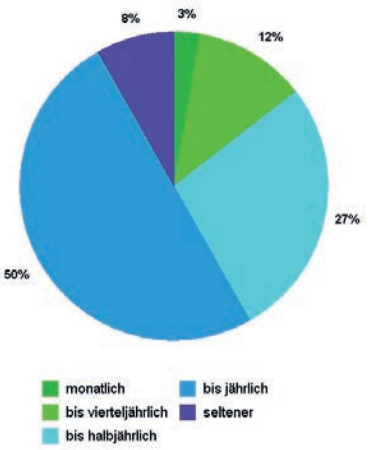


Abbildung 5: Häufigkeitsintervalle von Eignungsprüfungen für Konzepte und Maßnahmen (nachträglich klassifiziert)

Basis: 110 Antworten

räte sowie Social Media / Web 2.0 gab es bei mehr Teilnehmern konkrete Regeln (jeweils +8 %-Pkt.). Bedenklich erscheint, dass die bereits in der vorigen Studie abgesackte Zahl der Häuser mit Policies zur dienstlichen Nutzung privater IT-Systeme erneut um einen Prozentpunkt nachgegeben hat – allen Debatten um „Bring your own Device" (BYOD) zum Trotz.

Der Anteil von Teilnehmern mit schriftlich formulierten ISi-Maßnahmen hat hingegen zum dritten Mal in Folge etwas zugelegt und jetzt nach langjährig rückläufigen Zahlen mit 70 % wieder den Wert von 2002 erreicht (2012: 68 %, 2010: 61 %, 2008: 52 %, 2006: 57 %, 2004: 65 %).

Prüfungen

Fortdauernde Prüfungen der *Eignung* von Konzepten und Richtlinien stehen weiterhin hoch im Kurs (Tab. 8). Auch wenn der Anteil der regelmäßigen Prüfungen im Vergleich zur vorigen Studie etwas nachgegeben hat (45 %/–4 %-Pkt. – KMU 37 %, Große 54 %), stellen nur 9 % aller Teilnehmer bestehende Policies „nie" auf den Prüfstand – 46 % prüfen zumindest anlassbezogen. Abbildung 5 zeigt, wie häufig in den vergangenen Jahren im Teilnehmerfeld geprüft wurde – im Durchschnitt war das alle 9,7 Monate (KMU 9,4 Mon. / Große 10,1 Mon.).

Hauptsächlich eingesetzte Methodiken sind bei solchen Überprüfungen erneute Risiko- (78 %) und Schwachstellenanalysen (72 %). Rund die Hälfte der Teilnehmer setzt zudem auf Penetrationstests (51 %) sowie Notfall-, Wiederanlauf- oder sonstige Übungen (49 %). Simulationen oder Szenarien sind weiterhin eher selten (20 %). Dass die letzte Prüfung Schwachstellen aufgedeckt hat, wurde diesmal von gut drei Vierteln (77 %) aller Teilnehmer bejaht – bei 38 % hat die letzte Prüfung alle geschäftskritischen Systeme erfasst, bei 53 % ging es nur um einzelne Systeme (9 % antworteten „nicht bekannt" bzgl. der Reichweite).

Mit 88 % der Teilnehmer, welche die *Einhaltung* vorgesehener Maßnahmen prüfen, wird der gute Wert der vorigen Stichprobe sogar noch knapp übertroffen (+1%-Pkt. vs. 2012 – Ø 80 % in den Jahren 2006–2010). Auch der Anteil regelmäßig prüfender Organisationen liegt insgesamt mit 42 % um +5 %-Punkte höher als 2012. Große Unternehmen prüfen dabei häufiger regelmäßig (45 % vs. 39 % bei KMU) und seltener gar nicht (8 % vs. 17 % bei KMU).

Die Zuständigkeit für die Überwachung vorgesehener ISi-Maßnahmen obliegt im gesamten Teilnehmerfeld vor allem den IT-Abteilungen (54 % – KMU 69 % / Große 42 %), bei den großen Unternehmen der aktuellen Stichprobe jedoch vorrangig der eigenen ISi-Abteilung (67 % / KMU 37 %). Das war 2012 anders und lässt die ISi-Abteilungen nun auch im Gesamtschnitt auf einen geteilten ersten „Prüfer-Rang" aufschließen (54 %). Die weitere Bedeutung verschiedener Prüfer zeigt sich im Wesentlichen wie gehabt: Datenschutzbeauftragte (KMU 43 % / Große 58 %), interne Revision (31 % / 53 %), externe Berater und Wirtschaftsprüfer (31 % / 48 %), die zuständige Fachabteilung (22 % / 22 %) sowie die Geschäftsführung (22 % / 5 %).

Bei der Übereinstimmung von „gelebter Praxis" und den Vor-

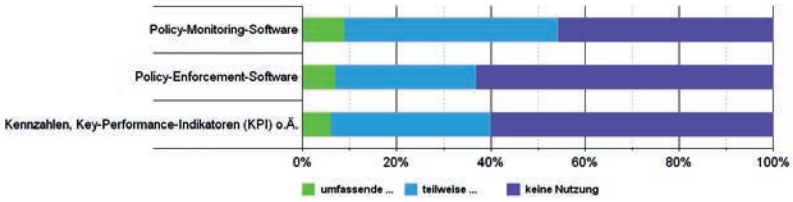


Abbildung 6: Einsatz von Hilfsmitteln zum Richtlinien-Management

Basis: Ø 122 Antworten

Folgende Kriterien sind ...	sehr wichtig	wichtig	unwichtig	Vergleichszahl *
Verstöße gegen Gesetze / Vorschriften / Verträge	59%	36%	5%	1,54
Imageverlust	57%	36%	7%	1,50
Schaden bei Dritten / Haftungsansprüche	38%	50%	12%	1,26
direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	35%	51%	14%	1,20
indirekte finanzielle Verluste	29%	50%	21%	1,08
Verzögerung von Arbeitsabläufen	22%	60%	18%	1,03
Verlust oder Schaden von oder an Hardware u. Ä.	20%	58%	23%	0,97
Verstöße gegen interne Regelungen	12%	65%	23%	0,89

Tabelle 9: Kriterien zur Risikobewertung

Basis: Ø 126 Antworten

* Vergleichszahlen errechnet aus: sehr wichtig = 2, wichtig = 1, unwichtig = 0

gaben durch Konzepte und Richtlinien lag die Technik (Abdeckung, Implementierung, Konfiguration, ...) erneut vor der Organisation (Tab. 8) – die Bewertungen von KMU und großen Unternehmen wichen hier nur um eine Zehntelnote voneinander ab (2,4 / 2,5). Heikler sahen die Großen indessen im Vergleich ihre Lage bei organisatorischen Fragen (Mitarbeiterverhalten, Kommunikation, ...), wo die Teilnehmer die Sollerfüllung mit durchschnittlich 3,2 deutlich schlechter bewertet haben als die KMU (2,8). Zudem lagen, wie schon 2012, auch dieses Jahr die Bewertungen der Teilnehmer mit ISi-Strategie über denen ohne (siehe Tab. 8). Den Einsatz von Hilfsmitteln zur Überwachung und Durchsetzung von Richtlinien und Maßnahmen zeigt Abbildung 6.

Risikobewertung

In der aktuellen Stichprobe haben mit 24 % insgesamt weniger Teilnehmer auf eine Klassifizierung von Anwendungen und Systemen hinsichtlich ihrer Bedeutung für Geschäftsprozesse sowie bestehende Risiken *verzichtet* – zuvor waren das während einer vollen Dekade regelmäßig 29–30 %. Die im Mittel höhere Bereitschaft zur Risikoeinschätzung geht jedoch ausschließlich auf die KMU zurück (jetzt 29 %, 2012: 42 %) – bei den großen Organisationen gab es sogar eine Verschlechterung (jetzt 19 %, 2012: 14 %). Insgesamt 36 % der Teilnehmer klassifizieren dabei *alle* Assets (KMU 37 % / Große 36 %), die verbleibenden 40 % nur einzelne Anwendungen und Systeme (34 % / 45 %). Eine Einbindung der IT-Risiken in ein ganzheitliches Risikomanagement ist erneut etwa bei der Hälfte aller Teilnehmer vorgesehen (52 % – 46 % / 56 %).

Die Rangfolge der Kriterien zur Risikobewertung zeigt Tabelle 9 – hier gab es keine nennenswerten Veränderungen zur vorigen Studie. Ähnliches gilt für die dabei eingesetzte Methodik (Mehrfachnennungen): 64 % der Teilnehmer nutzen standardisierte Verfahren, 36 % eigene Methoden oder Software. Etwas zugelegt hat mit 11 % die Nutzung spezifischer Risikomanagement-Software (+3 %-Pkt.) – möglicherweise zu Lasten der Verfahren von Herstellern oder Beratern (7 %, –2 %-Pkt.) sowie sonstigen Methoden (3 %, –2 %-Pkt.). Mit 7 % ist der Anteil aller Teilnehmer, die *kein* strikt methodisches Vorgehen verwenden, insgesamt gesunken, was allerdings ausschließlich auf die Großen in der Stichprobe zurückgeht, von denen dieses Mal niemand auf methodisches Vorgehen verzichtete (0 % vs. 6 % in 2012) – bei den KMU stieg der Anteil indes um 4 %-Punkte auf jetzt 17 %.

Versicherungen

Auch weiterhin sind Spezial-Versicherungen als Mittel zur Abwälzung von IT-Risiken nur bedingt im Einsatz: Insgesamt 40 % der Befragten haben irgendeine derartige Police abgeschlossen (KMU: 45 % / Große 33 %). Wie schon in den vorigen Studien waren dafür in aller Regel keine ISi-Audits oder -Zertifikate notwendig: Erneut war dies nur bei 8 % eine Vorbedingung (2010/2012: 8 %). Eine freiwillige Auditierung oder Zertifizierung führte bei 15 % zu günstigeren Konditionen (2012: 11 %, 2010: 16 %).

Standards

Abbildung 7 zeigt die Einschätzung verschiedener Kriterienwerke im ISi-Umfeld. Der IT-Grundschutz ist zwar weiterhin das bekannteste Rahmenwerk, in der praktischen Bedeutung fällt er jedoch erstmals auf den zweiten Platz hinter die ISO 2700x zurück. Die weitere Reihenfolge der zuvor erfragten Standards bleibt beim gewohnten Bild – erstmals erfragt haben wir die ISO-Normen zu Risikomanagement (ISO 31000) und BCM (ISO 22301) sowie den Sicherheits-Standard der Payment Card Industry (PCI DSS).

21 % der Teilnehmer gaben an, dass mindestens ein Teil ihrer Or-

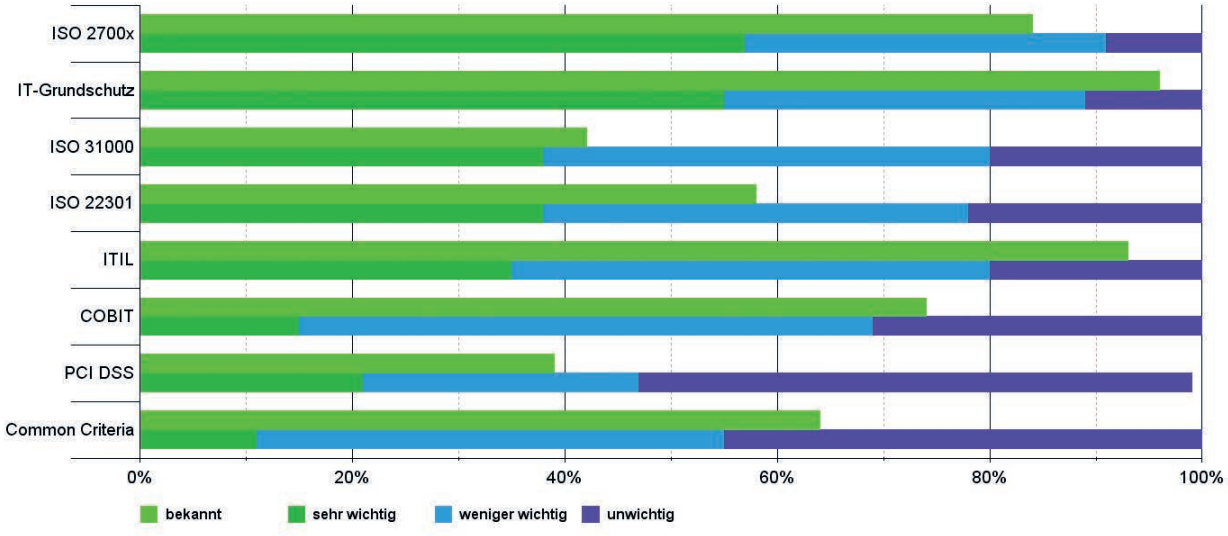


Abbildung 7: Bekanntheit und praktische Bedeutung von ISi-Kriterienwerken (sortiert nach Bedeutung)

Basis: Ø 119 Antworten, Ø 79 (Bedeutung)

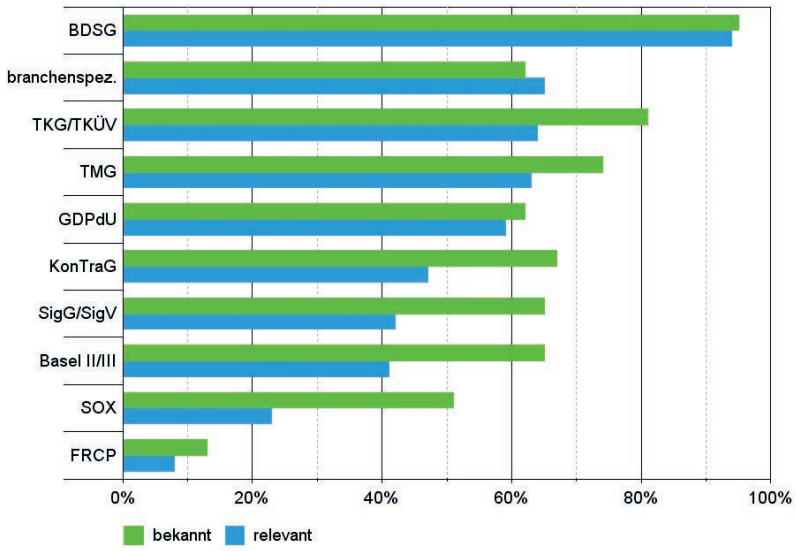


Abbildung 8: Bekanntheit und Relevanz von Gesetzen und Regularien (sortiert nach Relevanz)

Basis: Ø 111 Antworten, Ø 97 (Relevanz)

ganisation nach einem der erfragten Kriterienwerke zertifiziert ist (ein Vergleich mit 2012 ist aufgrund der veränderten Normen-Auswahl nicht möglich). Mit zwölf Nennungen führt auch hier die ISO 2700x deutlich vor den IT-Grundschutz-Zertifizierungen (7 Nennungen). Abgeschlagen folgen ITIL (3 Nenng.) sowie PCI DSS und CC (je 2 Nenng.).

Gesetze und Regularien

Die Bekanntheit einschlägiger Gesetze und Regularien sowie die Einschätzung ihrer Relevanz (Abb. 8) zeigen dieselbe Rangfolge wie in früheren Studien. Im Einzelnen war fast durchweg ein leichter Zuwachs der inhaltlichen Kenntnisse zu verzeichnen. Besonders stark war dies beim Sarbanes-Oxley-Act (SOX) der Fall, der jedoch in der vorigen Stichprobe geschwächelt hatte und nun wieder in etwa den Wert von 2010 erreicht. Dem deutschen Telemediengesetz (TMG) haben die Befragten hingegen zum zweiten Mal in Folge mehr Aufmerksamkeit gewidmet (+11 %-Pkt. Bekanntheit, +9 %-Pkt. Relevanz).

Betrachtet man den Umsetzungsgrad der Regularien (Abb. 9), zeigt sich beim TMG jedoch diese gesteigerte Beachtung noch nicht – im Gegenteil verharrt sie grob auf dem Wert der vorigen Studie und bleibt somit zwei Ränge hinter ihrer Bedeutung zurück. Stärker als ihre mittlere Bedeutungseinschätzung zeigt sich hingegen dieses Mal die Umsetzung der „wirtschaftlichen Gesetze“: die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU – +7 %-Pkt. „umfassend“) sowie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG – +14 %-Pkt. „umfassend“). Letzteres geht nicht zuletzt auf den im Vergleich zu 2012 höheren Anteil großer Unternehmen in dieser Studie zurück, die das KonTraG doppelt so häufig als relevant ansehen wie KMU-Teilnehmer und hier dementsprechend auch mehr tun; bei den GDPdU ist dieser Unterschied indessen deutlich geringer.

Weiterhin bleiben zwischen rund der Hälfte und zwei Drittel der Befragten der Meinung, dass die deutschen Gesetze rund um ISi, Netze und E-Commerce angemessen sind (Tab. 10). Ein zuvor deutlicher Überhang von Kritikern der TK-/Internet-Überwachung ist jedoch in diesem Jahr nicht mehr zu beobachten. Auch in Sachen Datenschutz und Signaturgesetz ist die Menge an Befürworten und Kritikern weiter reichender Regelungen ähnlich groß. Defizite werden auch dieses Mal wieder bei Gesetzen zu E-Business, Risikomanagement und vor allem Strafgesetzen zur Computer-Kriminalität gesehen.

Hindernisse

An erster Stelle der schlimmsten Hindernisse einer Verbesserung der Informations-Sicherheit (Tab. 11) steht weiterhin mangelndes Bewusstsein bei den Mitarbeitern – 68 % der Befragten haben dieses Problem benannt (+4 %-Pkt. vs. 2012). Stark zugelegt und damit auf Rang 2 platziert haben sich fehlende Geldmittel (+9 %-Pkt.). Das in der vorigen Studie historisch schlecht bewertete Sicherheits-Bewusstsein (bzw. Unterstützung) der Top-Manager hat die aktuelle Stichprobe zwar wieder etwas weniger beklagt (–3 %-Pkt.), es bleibt jedoch vor den Problemen mit dem mittleren

Angemessenheit deutscher Gesetzgebung	überzogen	angemessen	unzureichend	Vergleichszahlen * 2014	2012	2010
Signaturgesetz	23%	58%	19%	+ 0,05	- 0,02	+ 0,01
TK-/Internet-Überwachung	24%	49%	27%	- 0,02	+ 0,20	+ 0,30
Datenschutz	15%	63%	21%	- 0,06	- 0,08	- 0,06
E-Business (Verträge, Haftung, ...)	7%	64%	29%	- 0,22	- 0,29	- 0,16
Risikomanagement	8%	57%	35%	- 0,26	- 0,20	- 0,26
Strafgesetze (bzgl. Computer-Kriminalität)	5%	51%	44%	- 0,39	- 0,23	- 0,23

Tabelle 10: Angemessenheit deutscher Gesetzgebung

Basis: Ø 115 Antworten (2012: Ø 119, 2010: Ø 125)

* Vergleichszahlen errechnet aus: überzogen = +1, angemessen = 0, unzureichend = –1

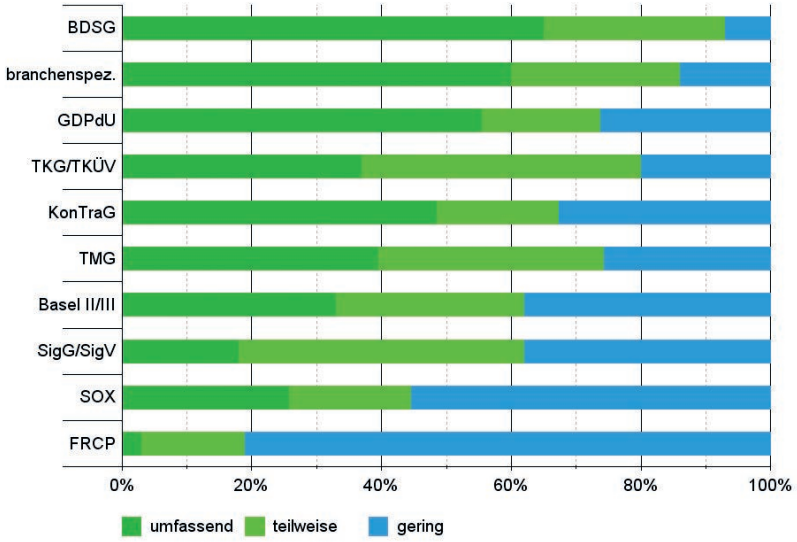
Management auf Rang 3 und einer weiterhin vergleichsweise schlechten Einschätzung.

Größere Probleme als vor zwei Jahren haben in der aktuellen Erhebung das Fehlen verfügbarer und kompetenter Mitarbeiter (+8 %-Pkt.) sowie fehlende Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen (+9 %-Pkt.) gemacht – beide steigen einen Rang in der Bedeutungskala.

Deutlich besser als vor zwei Jahren schneiden (nur) strategische Grundlagen und Gesamt-Konzepte ab (–8 %-Pkt.). Hier setzt sich ein langjähriger Trend fort (vgl. frühere Ergebnisse in Tab. 11): 2006 lag der Anteil der Teilnehmer, die über Probleme in diesem Bereich geklagt hatten, zwar geringer als in den nachfolgenden Studien – damit wurde damals aber dennoch der 7. Platz in der Problemhitliste erreicht, während die seither sinkenden Prozentzahlen 2008 bis 2012 jeweils Rang 8 bedeuteten.

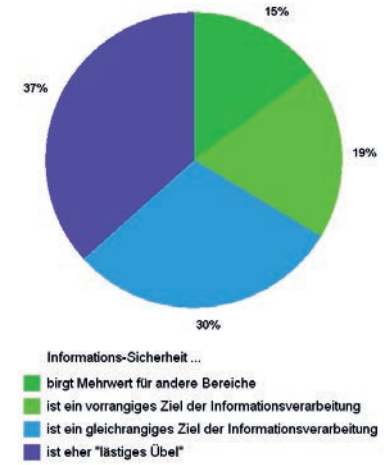
Zum ersten Mal haben wir zwei neue Problembereiche erfragt: Dass die nicht mehr beherrschbare Komplexität heutiger IT-Landschaften eine Verbesserung der ISi massiv behindere, beklagten (nur) 22 % (Rang 10). Auch die große Menge der verarbeiteten Daten sehen nicht sonderlich viele Befragte als Problem an: Mit 18 % steht „Big Data“ auf einer Stufe mit der Klage über das Fehlen geeigneter Produkte und damit fast am Ende der „benannten“ Skala.

Vergleicht man die Angaben aus KMU und großen Organisationen, so stimmt die Rangfolge der Top-8-Probleme komplett überein, auch wenn bei den Großen zumeist höhere Anteile der Befragten die bewussten Hindernisse beklagen – allem voran in Sachen mangelnder Management-Unterstützung, doch



Basis: Ø 73 Antworten

Abbildung 9: Umsetzungsgrad von Gesetzen und Regularien (sortiert nach Umsetzungsgrad: umfassend = 3, teilweise = 2, gering = 1)



Basis: 123 Antworten

Abbildung 10: ISi-Stellenwert beim Top-Management

Bei der Verbesserung der Isi behindern am meisten (Mehrfachnennungen möglich)	2014	2012	2010	2008	2006
Es fehlt an Bewusstsein bei den Mitarbeitern	68%	64%	59%	69%	52%
Es fehlt an Geld/Budget	58%	49%	57%	43%	55%
Es fehlt an Bewusstsein und Unterstützung im Top-Managment	53%	56%	47%	55%	45%
Es fehlt an Bewusstsein beim mittleren Management	52%	49%	54%	45%	37%
Es fehlen verfügbare und kompetente Mitarbeiter	45%	37%	41%	43%	32%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	43%	34%	35%	38%	31%
Die Kontrolle auf Einhaltung ist unzureichend	35%	38%	38%	41%	27%
Anwendungen sind nicht für ISi-Maßnahmen vorbereitet	31%	26%	27%	27%	25%
Die vorhandenen Konzepte werden nicht umgesetzt	27%	25%	27%	27%	22%
Die Komplexität heutiger IT-Landschaften ist nicht mehr beherrschbar	22%	–	–	–	–
Es fehlen geeignete Methoden und Werkzeuge	21%	17%	14%	16%	16%
Es fehlen realisierbare (Teil-)Konzepte	21%	20%	21%	25%	19%
Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	19%	27%	31%	36%	29%
Die Menge der verarbeiteten Daten ist nicht mehr beherrschbar	18%	–	–	–	–
Es fehlen geeignete Produkte	18%	16%	13%	16%	13%
Es fehlt an praxisorientierten Sicherheitsberatern	13%	11%	16%	14%	8%
Sonstige	5%	2%	4%	3%	5%
Keine	1%	3%	2%	1%	3%

Basis: 131 Antworten (2012: 133, 2010: 133, 2008: 143, 2006: 158)

Tabelle 11: Hindernisse für bessere Informations-Sicherheit

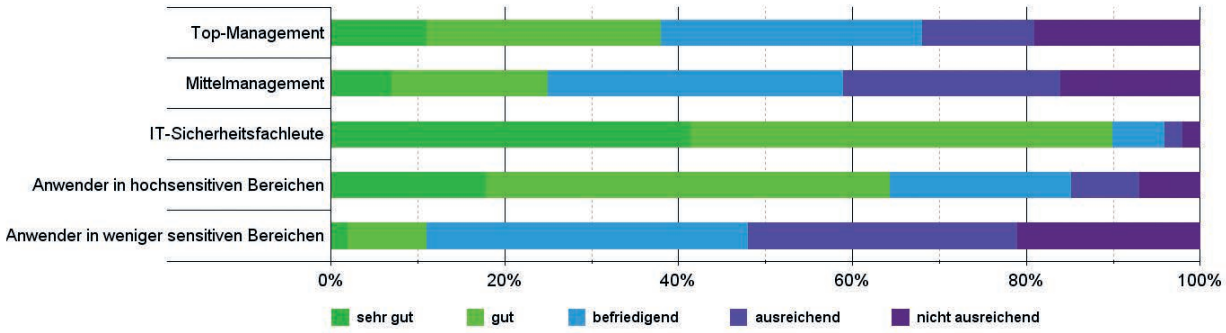


Abbildung 11: Kenntnisstand der Manager und Mitarbeiter

Basis: 124 Antworten

auch bei den Budgets. In der zweiten Tabellenhälfte zeigen sich indes Unterschiede: Während die Großen (erneut) stärker unter mangelnder *Umsetzung* von Konzepten leiden, beklagen die KMU stärker das Fehlen geeigneter Methoden, Werkzeuge, Konzepte und Produkte.

Die Einschätzung der Befragten zum Stellenwert der ISi bei ihrem Top-Management (Abb. 10) zeigt ein gewohntes Bild: Auch wenn der Anteil der „Skeptiker", welche die ISi eher als lästiges Übel ansehen, mit +4 %-Punkten (zu Lasten der neutral Eingestellten) dieses Mal etwas höher ausfällt als vor zwei Jahren, bleibt es doch bei der groben Drittelung. Die Angaben zu den „ISi-Freunden", die Security als Mehrwert oder vorrangiges Ziel ansehen, erreichen identische Werte wie 2012.

Kenntnisstand und Weiterbildung

Kaum Veränderungen gab es auch bei der Einschätzung des ISI-Kenntnisstands verschiedener Mitarbeitergruppen (Abb. 11): Die Fachleute erhalten eine „Zwei plus", das Top-Management im Mittel eine glatte Drei (Große 3,2 / KMU 2,9), das mittlere Management eine „Drei minus" (Große 3,4 / KMU 3,0). Anwender in hochsensitiven Bereichen landen erneut auf einer „Zwei Minus" (Große 2,3 / KMU 2,5), sonstige Anwender bei „Drei bis Vier" (Große 3,7 / KMU 3,5).

Auch die Schulungsfrequenz der Mitarbeiter in Sachen Sicherheit (Abb. 12) bleibt in etwa bei den Werten von 2012. ISi-Beauftragte werden in der aktuellen Stichprobe etwas öfter geschult (+7 %-Pkt. „häufig"), Datenschützer etwas seltener (–7 %-Pkt. „häufig"). Die in der vorigen Studie konstatierte Verbesserung der Manager-Trainings scheint sich fortzusetzen: +5 %-Punkte „häufig" und fast derselbe Wert „nie" (+1 %-Pkt.) bedeuten erneut ein leichtes Plus – aber dennoch bilden die Manager in Sachen ISI-Fortbildung noch immer das Schlusslicht der internen Mitarbeiter.

Bei den genutzten Ausbildungs-Methoden (Tab. 12) zeigt sich in dieser Studie ein deutlicher Zuwachs bei der Verwendung von Online-Trainings und -Tools: +10 %-Punkte „häufiger" Einsatz lässt das bisherige Schlusslicht in unserer Vergleichsrechnung auf Rang 2 aufsteigen und damit über die gesamte aktuelle Stichprobe sogar eine größere Bedeutung einnehmen als externe Schulungen – auch wenn weiterhin mehr als ein gutes Drittel der Teilnehmer diese Verfahren „nie" einsetzt. Solche Systeme sind vor allem bei den großen Organisationen beliebt: Dort setzen 37 % der Befragten „häufig" auf Online-Trainings, bei den KMU nur 21 %. Die Angaben zu den anderen Schu-

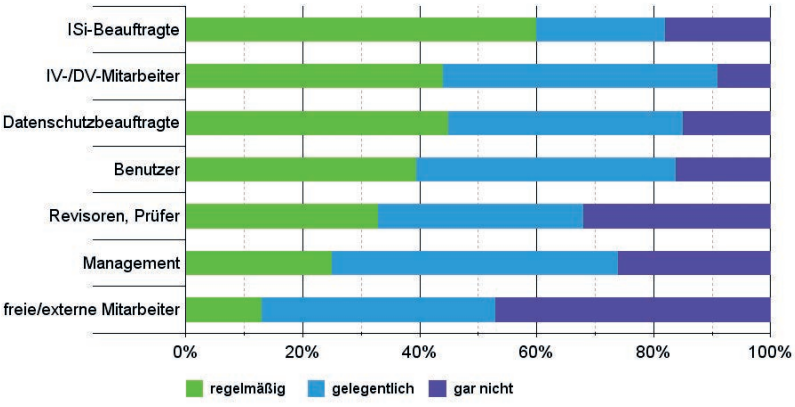


Abbildung 12: ISi-Schulungsfrequenz verschiedener Mitarbeitergruppen

Basis: Ø 109 Antworten

	häufig	gelegentlich	nie	Vergleichszahl*
interne Schulungen	37%	53%	10%	1,65
Online-Trainings-Anwendungen/-Tools	32%	32%	36%	1,27
externe Schulungen	19%	63%	19%	1,19
Materialien (Unterlagen, CDs/DVDs) zum Selbstlernen	20%	47%	33%	1,07

Tabelle 12: Genutzte Ausbildungsmethoden

Basis: Ø 119 Antworten

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

Sicherheit im Abonnement

WIK-Leser kennen alle relevanten Informationen

WIK Zeitschrift für die Sicherheit der Wirtschaft

WIK liefert 6 Mal im Jahr aktuelle Informationen und Basiswissen zum Thema Sicherheit. Sie wird seit über 30 Jahren von einer unabhängigen und hochqualifizierten Fachredaktion zusammengestellt.
Unsere Redakteure bereiten in jeder Ausgabe für Sie wichtiges Know-how auf, führen Interviews mit relevanten Vertretern der Branche, geben Hinweise zu Risiken, machen Lösungsvorschläge und zeigen praxisnahe Strategien und Anwendungsbeispiele. Dazu erhalten Sie regelmäßig: Einkaufsführer für den Sicherheitsverantwortlichen, Produktneuheiten, einen Branchenüberblick und Informationen aus den Sicherheitsverbänden.

WIK-Leser erfahren mehr:

- Aktuelle Beurteilung der Sicherheitslage
- Sicherheitstechnik: Ideen und Produkte
- Lösungen für den Unternehmensschutz
- Infos über und für Sicherheitsdienstleister
- Praxis und Anwenderbeispiele
- Checklisten, Marktübersichten
- ASW - Informationen

Web: www.wik.info
E-Mail: vertrieb@secumedia.de
Fax: +49 6725 5994

Sie haben Fragen? Ihr telefonischer Ansprechpartner im SecuMedia Verlag: Heidrun Jung, Tel. +49 6725 9304-0

Abonnement-Bestellung

Abonnenten werden zusätzlich zu den 6 regulären Ausgaben mit Sonderheften zu Spezial-Themen informiert. Diese sind im Abonnementspreis inbegriffen. Außerdem sind sie berechtigt auf das Archiv der Zeitschriften WIK und SicherheitsMarkt unter www.wik.info sowie www.sicherheits-markt.info zuzugreifen. Im Abopreis enthalten ist der SecuPedia Newsletter mit vielen Tipps und News aus der Sicherheitsbranche.

Bitte senden an E-Mail:

_____

Per Fax oder per Post im Fensterumschlag an:

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 1234
55205 Ingelheim

Fax an +49 6725 5994

☐ Ich abonniere die Zeitschrift WIK ab Nr. _____

Als Dankeschön erhalte ich das erste Heft gratis.
Das Abonnement enthält ein Passwort zur Nutzung des Abo-Bereichs auf www.wik.info und www.sicherheits-markt.info mit allen aktuellen Beiträgen und dem Heft-Archiv sowie Bezug des SecuPedia Newsletters.

Jahresbezugspreis (6 Ausgaben) € 108,00 inkl. MwSt. und Versandkosten (Schweiz SFr 205,50 / restl. Ausland € 129,80).

Der Jahresbezugspreis wird jeweils für ein Jahr im Voraus berechnet. Ich kann das Abonnement bis 14 Tage nach Erhalt des ersten Exemplars widerrufen. 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.

Unterschrift

Rechnung und Lieferung an

Telefon Durchwahl

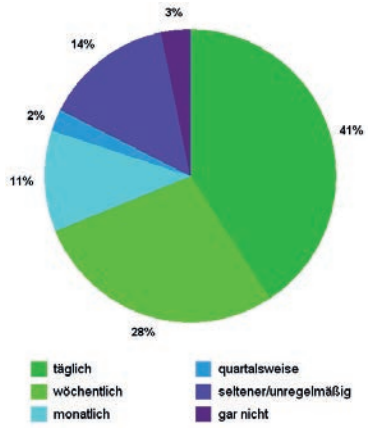


Abbildung 13: Prüfung passiver Kanäle

Basis: Ø 125 Antworten

lungsmethoden bleiben hingegen in etwa auf dem Niveau von 2012.

Zertifikate

Bei den Berufszertifikaten betonen die Befragten verstärkt die Aussagekraft von herstellerunabhängigen Prüfungen: 47 % halten diese für „sehr wichtig“ (+4 %-Pkt.) – herstellerspezifische Zertifikate erhalten diese Bewertung lediglich von 19 % der Teilnehmer (–4 %-Pkt.). Erneuter Spitzenreiter in der Bekanntheit (Mehrfachnennungen) ist wieder mit großem Abstand der IT-Grundschutz-Auditor (92 %), gefolgt von ISO-27000-Lead-Auditor (78 %), CISM (59 %), CISA (56 %), CISSP (56 %), dem eher unspezifischen „CISO“ (41 %), TISP (40 %), SSCP (26 %), CRISC (18 %), CGEIT (16 %), CSSLP (9 %), CCFP (7 %) und CPP (4 %).

Informationsquellen

68 % der Befragten nutzen die it-sa zur Information in Sachen ISi (+11 %-Pkt.) – 46 % die CeBIT (–15 %-Pkt.) und 37 % den BSI-Kongress (–10 %-Pkt.). In etwa denselben Wert wie vor zwei Jahren erreichten die „security essen“ (14 %), die Infosecurity (10 %) und die ISSE (2 %) – erstmals erfragt wurde die RSA-Conference, die 1 % der Teilnehmer nutzen.

Bei den Fachzeitschriften lag erneut die c‘t klar auf Platz zwei (nach der <kes>), gefolgt von iX, DuD und „IT-Sicherheit“. Bei den Online-Angeboten waren heise online / heise security wieder mit großem Abstand die meistgenannte Quelle für ISi-Informationen, gefolgt von Websites des BSI und golem.de (aufgezählt sind Quellen mit mind. fünf Freitext-Nennungen). Die Top-3 ISi-Bulletins sind – wie schon in den vorigen Studien – heisec.de (64 %), CERT-Bund (62 %) und Microsoft (46 %).

Aktiv vom Hersteller gelieferte Angebote bleiben die erste Wahl zur Information über Sicherheits-Updates (79 %), gefolgt von „Push“-Angeboten Dritter (z. B. Mailingslisten – 57 %). Jeweils 52 % der Befragten nutzen hierfür Informationsseiten der Hersteller oder Dritter, 45 % setzen auf aktiv ausgelieferte Informationen von Anbietern (z. B. Systemhäusern, Händlern usw.). Die Häufigkeit, in der passive Kanäle von den Befragten geprüft wurden, zeigt Abbildung 13 – die Einschätzung der Qualität von Herstellerinfos Tabelle 13.

Maßnahmen

Tabelle 14 zeigt den Realisierungs- und Planungsstand verschiedener Sicherheitsmaßnahmen auf Servern, Clients sowie mobilen Endgeräten. Den größten Zuwachs durchgängig realisierter Maßnahmen im Vergleich zur vorigen Studie zeigt ein zentralisiertes System- und Patch-Management (+11/+12/+11 %-Pkt.). Auch in Sachen Netzwerkzugangskontrolle (NAC, EAP, NAP & Co.) gab es deutlich mehr fertige Implementierungen (+6/+8/+9 %-Pkt.). Ein zentralisiertes Schwachstellenmanagement war bei Servern, Virtualisierung bei Client-Systemen erheblich stärker verbreitet (je +12 %-Pkt.).

Darüber hinaus hat sich der Trend zu mehr Verschlüsselung bei der Datenspeicherung weiter fortgesetzt: Serverseitig wurden vor allem Archivdatenträger und Backups (+15 %-Pkt.), mobile Speichermedien (+14 %-Pkt.) und ganze Festplatten oder Partitionen (+13 %-Pkt.) deutlich häufiger chiffriert. Bei den Endgeräten haben die Befragten in Sachen selektiver Verschlüsselung sensitiver Daten nachgeholt (+7/+11/+14 %-Pkt.) – 2012 hatte es hier vorrangig bei zentralen Systemen einen Zuwachs gegeben.

Bei verschlüsselten Verbindungen gab es eine deutlich geringere VPN-Nutzung der aktuellen Stichprobe bei LAN-/Intranet-Verbindungen (–10/–6/–10 %-Pkt.) sowie weniger VoIP-Verschlüsselung (–5/–4/–4 %-Pkt.) zu beobachten – WAN-VPNs und chiffrierte Telefonate/Faxe blieben in etwa auf demselben Niveau wie 2012. E-Mails wurden zentral häufiger, aber auf mobilen Systemen etwas seltener chiffriert (+8/+2/–4 %-Pkt.); jeweils rund ein Fünftel der Befragten hat hier aber noch Pläne für die Zukunft.

Ein geringerer Realisierungsgrad zeigte sich im Übrigen vor allem beim Application-Management (–6/–13/–5 %-Pkt.) sowie ferner bei der Inhaltsfilterung / Content-Inspection (–5/–9/–4 %-Pkt.) und der Schnittstellenüberwachung (–3/–9/–6 %-Pkt.). Außer bei den Inhaltsfiltern sind hier jedoch noch bei einer großen Zal der Teilnehmer Implementierungen in Planung.

Erhebliches Potenzial besteht zudem noch beim weiteren Ausbau von Netzwerkzugangskontrollen, Identity- und Access- (IAM) sowie zentralisiertem Schwachstel-

Tabelle 13: Qualität von Hersteller-Infodiensten

	sehr gut	gut	befriedigend	ausreichend	nicht ausreichend	Note
Umfang/Vollständigkeit	3%	57%	34%	4%	2%	2,46
Verständlichkeit	2%	44%	45%	8%	1%	2,62
Geschwindigkeit	0%	42%	42%	12%	4%	2,80

Basis: Ø 113 Antworten

	Server / Zentrale			Clients / Endstellen			mobile Endgeräte		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
Firewalls	98%	2%	0%	77%	3%	21%	65%	10%	25%
Intrusion-Detection-/ Prevention-Systems (IDS/IPS)	55%	14%	31%	24%	13%	63%	20%	11%	70%
Netzwerkzugangskontrolle (EAP, NAC, NAP, ...)	56%	13%	31%	43%	21%	36%	39%	19%	42%
Schnittstellenüberwachung/-schutz (USB, ser., par., Bluetooth, ...)	35%	16%	48%	43%	23%	34%	31%	19%	50%
Identity- und Access-Management (IAM)	37%	18%	44%	37%	17%	46%	29%	21%	50%
Authentifizierung									
... Hardware-Token	27%	4%	70%	28%	5%	68%	31%	4%	65%
... Passwort	96%	1%	3%	98%	0%	2%	97%	1%	2%
... Chipkarte / Smartcard	16%	4%	80%	16%	6%	79%	11%	3%	86%
... biometrische Verfahren	5%	5%	89%	7%	6%	87%	8%	2%	90%
... SSL-/TLS-/X.509-Zertifikate	56%	9%	35%	45%	8%	48%	40%	10%	50%
Security-Information- und -Event-Management (SIEM)	23%	26%	51%	13%	17%	70%	12%	15%	74%
Application-Management (Schutz vor Installation/Nutzung unerw. App.)	44%	13%	43%	44%	18%	38%	38%	19%	43%
zentralisiertes Schwachstellen-Management (Vulnerability-Mgmt.)	35%	20%	45%	22%	21%	58%	17%	16%	67%
zentralisiertes System-/Patch-Management	78%	10%	12%	78%	7%	15%	55%	14%	30%
Virtualisierung	86%	7%	7%	44%	6%	51%	14%	2%	84%
Malware-/Spyware-Abwehr	95%	3%	2%	94%	2%	4%	78%	6%	16%
Spam-Abwehr	90%	3%	7%	81%	3%	16%	70%	2%	28%
Content Inspection/Filtering (Adress-/Inhaltsfilter eingehend)	64%	9%	27%	45%	8%	47%	33%	7%	60%
Data-Leakage-/Loss-Prevention (DLP, Inhaltskontrolle abgehend)	20%	17%	63%	14%	13%	73%	11%	12%	77%
Digital-/Enterprise-Rights-Management (DRM/ERM)	15%	13%	73%	14%	12%	75%	11%	7%	82%
Public-Key-Infrastructure (PKI)	46%	20%	34%	29%	18%	52%	26%	15%	59%
Verschlüsselung									
... sensitive Daten	65%	13%	22%	61%	11%	28%	61%	10%	29%
... Festplatten/eingebaute Speicher ... (komplett/partitionsweise)	42%	9%	50%	46%	15%	39%	59%	13%	27%
... mobile Speichermedien (USB, SDcard, ...)	39%	9%	52%	42%	20%	38%	37%	15%	48%
... Archivdatenträger/Backups	51%	8%	41%	24%	7%	69%	19%	7%	74%
... LAN/Intranet-Verbindungen (VPN)	52%	8%	41%	46%	7%	47%	41%	7%	52%
... WLAN-Verbindungen (WPA, VPN, ...)	70%	5%	25%	76%	6%	18%	72%	8%	20%
... WAN/Internet-Verbindungen (VPN)	77%	6%	17%	73%	5%	22%	71%	6%	24%
... mobile Verbindungen (VPN via UMTS, Hotspots, ...)	53%	4%	43%	54%	7%	39%	69%	6%	26%
... Telefon / Fax (Festnetz/GSM)	12%	5%	83%	11%	7%	81%	17%	6%	77%
... Voice over IP (VoIP)	23%	11%	66%	23%	12%	65%	21%	9%	69%
... E-Mail	55%	19%	27%	53%	20%	27%	48%	17%	35%
Datensicherung (Backup)	82%	7%	12%	49%	6%	45%	33%	9%	58%
Langzeit-Archivierung	61%	13%	26%	25%	6%	69%	13%	6%	81%
physische Sicherheit									
... Zutrittskontrolle, biometrisch	8%	7%	85%	1%	3%	96%	–	–	–
... Zutrittskontrolle, sonstige	93%	4%	3%	73%	4%	23%	–	–	–
... Bewachung	53%	6%	42%	39%	2%	59%	–	–	–
... Video-Überwachung	56%	10%	35%	32%	6%	62%	–	–	–
... Einbruchmeldesysteme	75%	6%	20%	50%	4%	46%	–	–	–
... Sicherheitstüren	80%	4%	16%	48%	4%	49%	–	–	–
... Brandmeldesysteme	87%	7%	6%	65%	3%	33%	–	–	–
... Löschanlagen	68%	4%	28%	31%	5%	65%	–	–	–
... andere Meldesysteme (Gas, Staub, Wasser, ...)	61%	6%	33%	19%	3%	78%	–	–	–
... Datensicherungsschränke/-räume	81%	5%	14%	30%	2%	68%	–	–	–
... Schutz gegen kompromittierende Abstrahlung (Tempest)	18%	3%	78%	5%	0%	95%	3%	1%	96%
... sonstige Maßnahmen gegen Hardware-Diebstahl	48%	4%	48%	34%	8%	58%	43%	6%	51%
physikalisches Löschen von Datenträgern	78%	3%	19%	66%	5%	30%	52%	4%	44%
unterbrechungsfreie Stromversorgung (USV)	95%	2%	3%	21%	6%	73%	12%	1%	87%
Überspannungsschutz für Stromleitungen	91%	2%	8%	52%	2%	46%	21%	0%	79%
Überspannungsschutz für Daten-/IT-Leitungen	69%	8%	23%	41%	4%	55%	16%	1%	82%
Reserve-Netzzugang (IT/TK) zur Ausfallüberbrückung	68%	7%	26%	35%	3%	62%	18%	0%	82%

Basis: Ø 116 Antworten (Server), Ø 106 (Clients), Ø 105 (mob. Systeme)

Tabelle 14: Realisierte und geplante Sicherheitsmaßnahmen

	realisiert	geplant	nicht vorgesehen
zentrales Speichern aller Log-Informationen	46%	25%	29%
zentrales, regelmäßiges Auswerten aller Log-Informationen	31%	37%	32%
zentrales Echtzeit-Monitoring der Logs	22%	27%	52%
zentrales Korrelieren der Logs	11%	30%	59%
Integration von Helpdesk-Information in das zentrale Logging	9%	21%	70%
zentrales Compliance-Reporting	17%	33%	50%
firmenweites Security-Dashboard	13%	28%	60%
Nutzung externer Dienste zur Früherkennung neuer Bedrohungen	31%	20%	50%
Melden eigener Informationen an solche Dienste oder an Behörden	17%	16%	67%

Tabelle 15: Maßnahmen zu Lagebild und „situational Awareness"

Basis: Ø 122 Antworten

len-Management, aber auch bei Public-Key-Infrastructures (PKI). Sehr viele Pläne gibt es zudem für Security-Information- und -Event-Management (SIEM), das wir erstmalig mit diesem Begriff abgefragt haben – zuvor enthielt der Fragebogen die allgemeinere Formulierung „Security-Event-Management (Protokollierung/Auswertung)", weswegen auch kein Vergleich zu früheren Zahlen möglich ist.

Die „Hitliste wenig erwünschter Sicherheitsmaßnahmen" führen weiterhin der sehr spezielle Schutz vor kompromittierender Abstrahlung (Tempest) sowie biometrische Zutrittskontroll- und Authentifizierungs-Verfahren an. Es folgen Chipkarten für die Authentifizierung, TK-Verschlüsselung und Digital-/Enterprise-Rights-Management (DRM/ERM), die weiterhin noch jeweils rund drei Viertel oder mehr der Befragten in keinem Bereich implementieren wollen.

Und auch Data-Leakage-/Loss-Prevention (DLP) bleibt weiterhin unbeliebt: Auf Servern beziehungsweise zentraler IT sagen noch immer 63 % „Nein, danke!", bei Clients 73 % und für mobile Systeme 77 % – das entspricht in etwa den Ergebnissen von 2012. Rund 60 % der Teilnehmer, die zu DLP mindestens auf eine Frage antworteten, haben für *keine* der drei Ebenen DLP-Mechanismen realisiert oder geplant.

Vertraulichkeit und Netznutzung

81 % der Befragten gaben an, Daten bezüglich ihrer Sensitivität (z. B. als geschäftskritisch, vertraulich, Verschlusssache usw.) zu klassifizieren – beim größten Teil geschieht das weiterhin manuell (76 %), nur 5 % können auf automatisierte Verfahren zurückgreifen. Spezielle Bereiche, die als besonders risikobehaftet oder gefährdet eingestuft sind, existieren bei 70 % der Teilnehmer.

Zur Abschottung klassifizierter beziehungsweise gefährdeter Systeme und Daten innerhalb des eigenen Hauses kommen weiterhin vorwiegend allgemeine Sicherheitssysteme zum Einsatz (62 %), gefolgt von Netzwerkmechanismen wie VLANs, NAC oder Ähnlichem (56 %). Spezielle Systeme für eingestufte Daten nutzen 33 % der Teilnehmer – bei 31 % gibt es eine vollständige physische Trennung vom allgemeinen Hausnetz (Mehrfachnennungen möglich). Nicht ganz ein Fünftel *verzichtet* jedoch auf jegliche Sicherung gegenüber dem Hausnetz (19 %), obwohl es klassifizierte Daten oder Bereiche gibt.

Der Zugang zu WWW und E-Mail ist in den meisten Organisationen für geschäftliche Zwecke allen Mitarbeitern gestattet (Abb. 14) – in Sachen Multimedia und „Web 2.0" sind Restriktionen zwar etwas häufiger als in der vorigen Stichprobe (+4 %-Pkt. generelles Verbot, +3 %-Pkt. mit Einschränkungen), aber auch weiterhin erlaubt mehr als die Hälfte der Teilnehmer dies ebenfalls der gesamten Mitarbeiterschaft. Ein Berechtigungskonzept für die Nutzung aktiver Inhalte im Web-Browser existiert bei 59 %. 65 % gaben an, derartige Berechtigungen zentral (etwa per Gruppenrichtlinie) zu steuern.

Die Nutzung des Internets zu privaten Zwecken ist in mehr als zwei Dritteln der Häuser freigegeben – nur 18 % verbieten das generell, was in etwa dem Mittel der letzten Studien entspricht (2012: 28 %, 2010: 16 %, 2008: 21 %, 2006: 23 %, 2004: 13 %).

Privat beschaffte oder administrierte Systeme mit Unterneh-

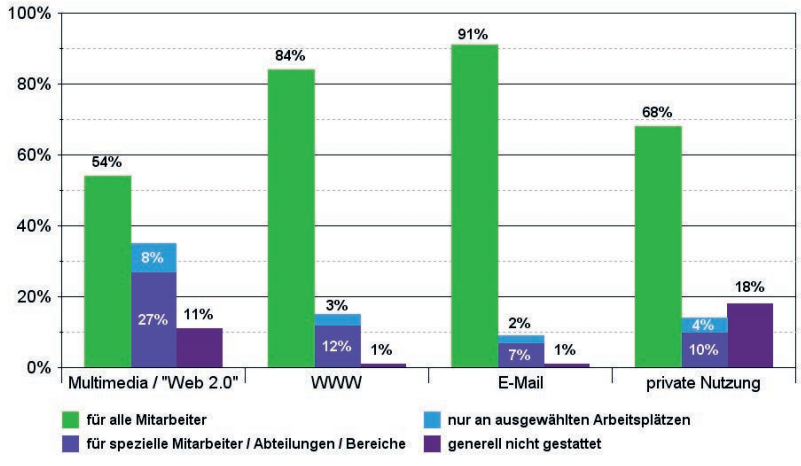


Abbildung 14: Beschränkungen geschäftlicher und privater Internetnutzung

Basis: Ø 117 Antworten

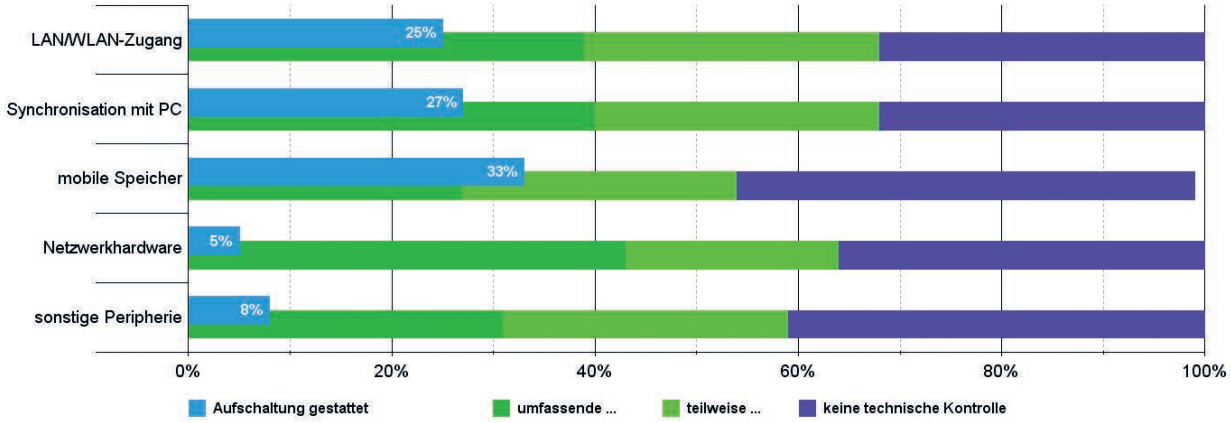


Abbildung 15: Zulässigkeit und Kontrolle privater Systeme

Basis: Ø 125 Antworten (Aufschaltung), Ø 115 (Kontrolle)

menshardware oder -netzen zu verbinden, ist hingegen weiterhin häufig verboten und dementsprechend verbreitet technischen Kontrollen unterworfen (Abb. 15). Lediglich bei mobilen Speichern sind die Befragten der aktuellen Studie wieder etwas „gnädiger" (Zulässigkeit 2014: 33 %, 2012: 26 %, 2010: 39 %), bei sonstiger Peripherie noch deutlich „schärfer" (–7 %-Pkt.) als die Stichprobe von 2012.

Keine großen Änderungen ergab unsere Frage nach der „Readiness" von Netzwerk- und Sicherheitssystemen bezüglich DNSSEC (46 %) und IPv6 (59 %). Dabei ist die Verbreitung des „neuen" Internetprotokolls durchaus gestiegen: Nunmehr 34 % nutzen IPv6 (+11 %-Pkt.) in der einen oder anderen Form – bei 20 % der Teilnehmer läuft ein Pilotbetrieb (+6 %-Pkt.), 17 % meldeten interne Nutzung (+6 %-Pkt.). 3 % Befragte, bei denen IPv6 auch für externe Verbindungen sorgt, sind hingegen in etwa derselbe Wert wie vor zwei Jahren (2012: 4 % – Mehrfachnennungen).

Angriffs- und Bedrohungs-Management

Neu in der Studie sind umfassende Fragen zu realisierten oder geplanten Mechanismen, die der Angriffserkennung oder dem Erstellen eines Lagebilds dienen – die Antworten enthält Tabelle 15. Ein beträchtlicher Teil der Befragten hat bereits zentrale Systeme zur Speicherung und Auswertung von Log-Informationen im Einsatz – gut ein Fünftel (22 %) überwacht Protokolldateien in Echtzeit. Log-Files von *Endgeräten* analysiert immerhin ebenfalls fast ein Fünftel (19 %) regelmäßig – jeweils etwa ein Drittel davon täglich, wöchentlich oder in längeren Intervallen bis zu 30 Tagen. Nur 8 % werten solche Logfiles überhaupt nicht aus, 73 % tun dies anlassbezogen.

Auch wenn die aktuelle Stichprobe dem Unified-Threat-Management (UTM) im Detail wieder etwas kritischer gegenübersteht als diejenige von 2012, bleiben diese Systeme dennoch fast durchgängig „im Plus" gegenüber Einzellösungen oder „Best-of-Breed"-Ansätzen (Abb. 16): Nur in Sachen „Anpassbarkeit an veränderte Anforderungen" bewerten die Teilnehmer UTM ein wenig schlechter. Die Rangfolge der UTM-Vorzüge (in der Abb. von oben nach unten) bleibt im Übrigen dieselbe wie in der vorigen Studie. Und erneut hält nur etwa jeder Fünfte Teilnehmer (20 % / +1 %-Pkt. vs. 2012) die Sicherheit von UTM für schlechter als diejenige von Einzellösungen.

Systeme verschiedener Anbieter sind hingegen bei der Mal-

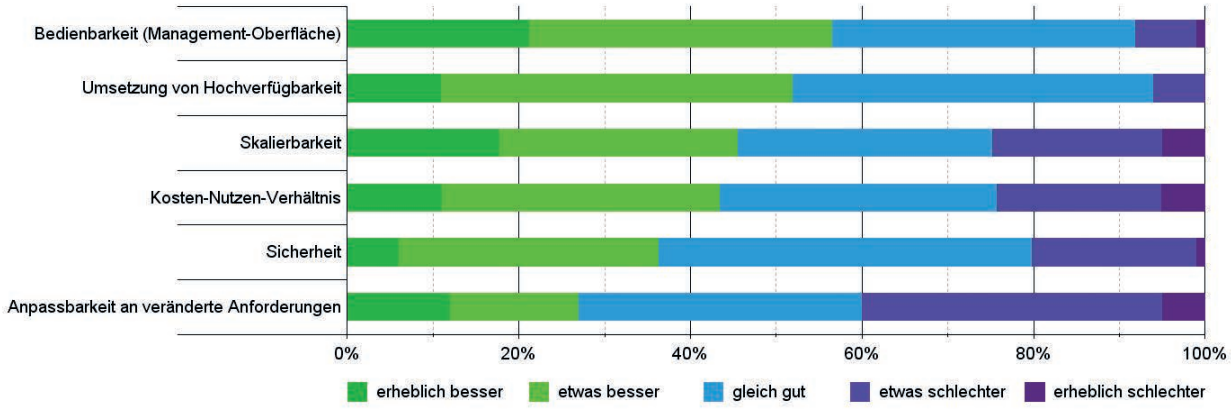


Abbildung 16: Unified-Threat-Management-(UTM)-Systeme im Vergleich zu Einzellösungen/ „Best-of-Breed"-Ansätzen

Basis: Ø 79 Antworten

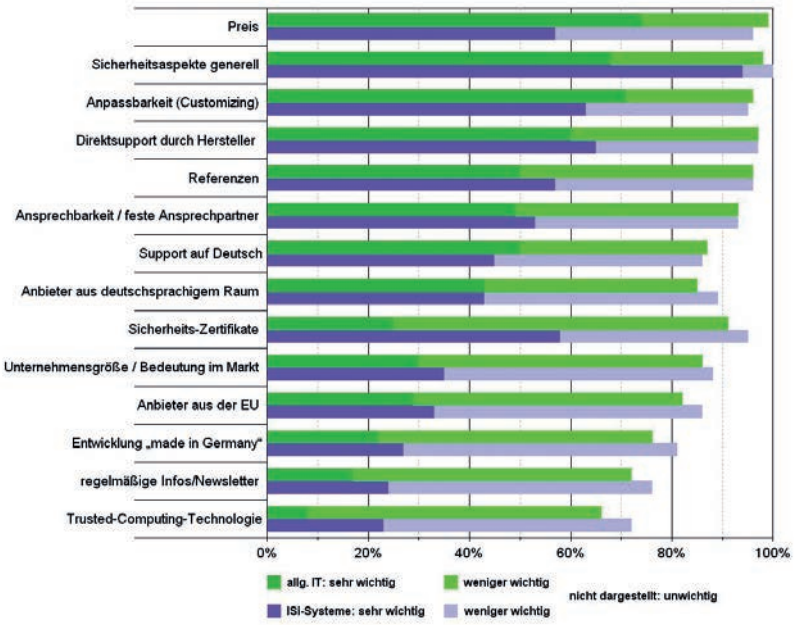


Abbildung 17: Kriterien zur Auswahl von IT-Systemen und -Lösungen (sortiert nach Wichtigkeit für allg. IT)

Basis: Ø 126 Antworten (allg. IT), Ø 121 (ISi-Systeme)

ware-Abwehr weiterhin hoch im Kurs: Erneut setzen 60 % hier aus Sicherheitsgründen auf eine „Multi-Vendor"-Strategie (Tab. 16). Deutlich häufiger als in der vorigen Studie werden jetzt auch heterogene Web-Server eingesetzt (+9 %-Pkt.), deutlich mehr *Homo*genität als 2012 zeigt sich bei Firewalls (+11 %-Pkt.) und Server-Betriebssystemen (+7 %-Pkt.). Ein zentrales Management-Tool zur Verwaltung von heterogenen Sicherheitssystemen ist bei 12 % der Befragten im Einsatz, bei weiteren 26 % in Planung.

Systemauswahl und -sicherheit

Den Abschnitt zur Bedeutung verschiedener Eigenschaften für die Auswahl von IT-Systemen und -Lösungen haben wir in diesem Jahr um weitere Kriterien ergänzt und zudem für allgemeine IT sowie ISi-Systeme getrennt erfragt – die Ergebnisse zeigt Abbildung 17. Bei *allgemeiner IT* steht der Preis an erster Stelle (74 % „sehr wichtig" / 25 % „wichtig"), gefolgt von Sicherheitsaspekten (68 % / 30 %), Anpassbarkeit (71 % / 25 %), Herstellersupport (60 % / 37 %) und Referenzen (50 % / 46 %).

Die Top-5-Kriterien für *Informations-Sicherheits-(ISi)-Systeme* sind dieselben, jedoch in deutlich veränderter Reihenfolge: Mit Abstand vorne liegen hier die Sicherheitsaspekte (94 % / 6 %) – die „Verfolgergruppe" bilden Herstellersupport (65 % / 32 %), Anpassbarkeit (63 % / 32 %) sowie Referenzen und Preis (jeweils 57 % / 39 %). Auf fast demselben Level folgen dann schon die bei allgemeiner IT deutlich weniger wertgeschätzten Sicherheits-Zertifikate (58 % / 37 %).

Dass der jeweilige Anbieter seinen Hauptsitz im deutschsprachigen Raum hat, findet indessen generell weniger als die Hälfte der Befragten „sehr wichtig" – eine Entwicklung „made in Germany" sogar nur rund ein Viertel, was schon fast so unbedeutend ist wie der regelmäßige Versand von Informationen oder Newsletters. Weniger bedeutsam ist in den Augen der Teilnehmer nur noch die Nutzung von Trusted-Computing (TPMs usw.).

In einer anderen Frage haben zwar 34 % bejaht, dass „made in Germany" höhere Preise rechtfertigt – der große Abstand in der Wichtigkeit von Kosten und Herkunft legt jedoch den Verdacht nahe, dass man im Einzelfall nicht bereit ist, die höheren Preise auch zu bezahlen. Ähnliches gilt wohl für evaluierte Systeme in der allgemeinen IT, obwohl für Produkte und Lösungen mit Sicherheitszertifikaten sogar 59 % höhere Preise als gerechtfertigt ansehen. Anders könnte dies allerdings bei ISi-Systemen sein, wo Kosten und Zertifikaten quasi derselbe Stellenwert zugemessen wurde.

Eine Verifizierung von ISi-Anforderungen gaben dieses Mal 51 % der Teilnehmer als Voraussetzung für die Inbetriebnahme von Systemen an. Bei den großen Organisationen ist der Anteil mit

Tabelle 16: Heterogenität aus Sicherheitsgründen (Multi-Vendor-Strategie)

Im Einsatz sind Lösungen von ...	einem Anbieter	zwei Anbietern	drei oder mehr Anbietern	Mittelwert Lösungen
Anti-Virus-Software	40%	40%	20%	1,81
Server-Betriebssysteme	51%	29%	20%	1,68
Applikations-Server	57%	19%	23%	1,66
Web-Server	50%	38%	12%	1,62
Router/Netzwerkhardware	58%	27%	15%	1,57
Firewalls	61%	34%	5%	1,44

Basis: Ø 113 Antworten

Tabelle 17: Sicherheitsaspekte bei Smartphones/Tablets von Mitarbeitern oder Partnern

	realisiert	geplant	nicht vorgesehen
Verschlüsselung gespeicherter Daten	47%	18%	34%
zentrales Management (Apps, Patches, ...)	40%	25%	35%
Security-Suite (Virenschutz, Personal-Firewall, ...)	34%	28%	38%
Online-Zugriff auf schutzwürdige Unternehmensdaten	46%	12%	42%
Speicherung schutzwürdiger Daten auf dem Gerät	35%	6%	59%
Verschlüsselung von Sprachkommunikation	6%	10%	85%

Basis: Ø 125 Antworten

61 % erneut höher als bei kleineren Häusern – und erneut gestiegen (2012: 58 %, 2010: 53 %). Doch auch 43 % der KMU dieser Stichprobe sind Sicherheitsanforderungen entsprechend wichtig – nach nur 21 % vor zwei Jahren und 33 % im Jahr 2010 ein erfreulich hoher Wert.

Die Bedeutung von Server-based Computing ist hingegen nur wenig gewachsen: Zwar gaben mit 70 % der Teilnehmer +3 %-Punkte mehr an, Terminalserver zu nutzen, aber nur weitere 8 % planen dies noch für die Zukunft (2012: 12 %). Immerhin 6 % (+1 %-Pkt.) nutzen ausschließlich Thin Clients, 16 % bevorzugt (–2 %-Pkt.), 10 % „gleichrangig" (+3 %-Pkt.). Bei einem Drittel der Befragten (2012: 47 %) sind derart „leichtgewichtige" Endgeräte überhaupt nicht im Einsatz.

Wieder etwas kritischer zeigen sich die Einschätzungen zur Sicherheit von Open-Source-Software (OSS) im Vergleich zu Produkten mit nicht-offengelegtem Quelltext: Nur noch 46 % der Befragten sehen OSS hier im Plus (2012: 52 %, 2010: 43 %, 2008: 46 %), immerhin 17 % halten offene Systeme sogar für unsicherer (2012: 13 %, 2010: 14 %. 2008: 8 %). Details zeigt Abbildung 18.

Die generelle Nutzung von OSS bleibt bei 80 % der Befragten (29 % „häufig", 51 % „selten") auf dem Niveau der vorigen Studie. Kosten (bei 60 %) und bessere Funktionalität (bei 54 %) sind erneut mit Abstand die meistgenannten Gründe für den OSS-Einsatz – die Sicherheit ist mit 21 % wieder bei weniger Teilnehmern ein Anlass hierfür als bessere Interoperabilität (26 %) oder „Sonstiges" (29 % – Mehrfachnennungen).

Dem entsprechend stehen auch Prüfungen hinsichtlich funktionaler Aspekte bei der Arbeit mit Open-Source-Code weiterhin im Vordergrund: 21 % der teilnehmenden Organisationen rücken dem offenen Quellcode deswegen „häufig" zu Leibe, weitere 27 % „gelegentlich". Modifikation und lokale Anpassungen (11 % / 32 %) rangieren in der Bedeutung erneut vor Sicherheitsprüfungen (5 % / 32 %).

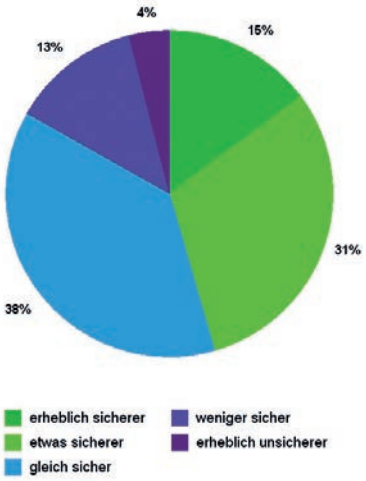
Smartphones/Tablets

Risikoprofile und Sicherheitsmechanismen für Smartphones und Tablets von Mitarbeitern oder Partnern der Befragten zeigt Tabelle 17. Im Vergleich zur vorigen Stichprobe haben die Verarbeitung und Speicherung schutzwürdiger Daten mit den mobilen Systemen um jeweils rund ein Drittel zugenommen. Erfreulicherweise hat auch der Einsatz von Verschlüsselung (+16 %-Pkt.) und zentralem Management (+9 %-Pkt.) deutlich zugelegt – Security-Suiten verharren indessen auf etwa demselben Wert (+1 %-Pkt.) und sind weiterhin nur auf rund einem Drittel aller Systeme vorhanden. Auch dort, wo entweder ein Online-Zugriff auf schutzwürdige Daten oder deren Speicherung auf den Mobilgeräten bereits Realtität sind, haben erst 42 % eine Security-Suite schon eingerichtet und selbst dort sagen noch 29 %, dies sei auch zukünftig „nicht vorgesehen".

In Sachen Verbreitung hat iOS mit 71 % (+17 %-Pkt.) seinen Spitzenplatz im Vergleich zu 2012 deutlich ausgebaut. Bei jeweils 42 % der Befragten waren Android (–3 %-Pkt.) und Blackberry (–9 %-Pkt.) im Einsatz, es folgen Windows Phone (23 % / +9 %-Pkt.), Windows Mobile (15 % / –15 %-Pkt.) und Symbian (7 % / –9 %-Pkt.) vor Sonstigen (1 % / –3 %-Pkt.).

Content- und E-Mail-Security

Tabelle 18 zeigt den gewünschten Funktionsumfang von Content-Security-Lösungen: An erster Stelle stehen wie immer Viren- und Spyware-Schutz. Die größten Veränderungen in der „Wunschliste" waren +19 %-Punkte für Intrusion-Detection/-Prevention, das damit um sechs Ränge in die erste Tabellenhälfte aufsteigt. Auch Inhaltsfilter steigen um zwei Ränge in der Beachtung (+12 %-Pkt.). Die Prüfung von SSL-Übertragungen (+11 %-Pkt.) sowie DLP (+7 %-Pkt.) sind zwar ebenfalls gefragter, rangieren aber weiterhin am unteren Ende der Liste.



Basis: 124 Antworten

Abbildung 18: Einschätzung der Sicherheit von Open-Source-Software (OSS) gegenüber Programmen mit nicht-offengelegtem Quelltext

Dass eine Malware-Prävention ohne Patternupdates auskommt, halten 45 % der Befragten für „sehr wichtig", weitere 50 % für „wichtig". 32 % haben eine solche Lösung bereits realisiert (2012: 46 %, 2010: 38 %, 2008: 28 %), weitere 31 % planen dies für die Zukunft. 75 % der teilnehmenden Organisationen setzen auf eine stetige Schreib-/Leseprüfung (Virenwächter) für PCs/Notebooks/Tablets (2012: 82 %, 2010: 83 %, 2008: 61 %), 46 % stel-

Gewünschter Funktionsumfang	
Virenschutz	98%
Spyware-Schutz	83%
Phishing-Abwehr	77%
zentrale Administration	72%
Spam-Abwehr	70%
Monitoring/Alerting	67%
Intrusion-Detection/-Prevention	62%
Desktop/Client-Firewall	61%
Reporting-Tools	61%
Inhaltsfilter	55%
Device-/Schnittstellenkontrolle	53%
Verschlüsselung	50%
Prüfung von SSL-Übertragungen	49%
Data-Leak-/Loss-Prevention	44%
Applikationskontrolle	43%

Basis: 126 Antworten

Tabelle 18: Anforderungen an Content-Security-Lösungen

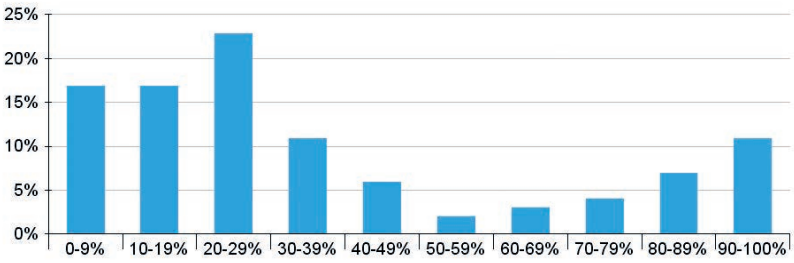


Abbildung 19: Spam-Anteil an eingehenden E-Mails

Basis: 101 Antworten

	realisiert	geplant	nicht vorgesehen
nur Software	57%	15%	28%
Hardwaremodule (HSM)	12%	6%	81%
Hardware-Token	26%	5%	70%
Chipkarten	23%	9%	68%
elektronischer Personalausweis	4%	7%	90%
fortgeschrittene Signatur	16%	10%	74%
qualifizierte Signatur	26%	15%	59%
qualifizierte Signatur mit Anbieterakkreditierung	22%	7%	71%

Tabelle 19: Infrastruktur für elektronische Signaturen

Basis: Ø 103 Antworten

len eine isolierte Testumgebung für Malware bereit (2012: 53 %, 2010: 45 %, 2008: 46 %).

Die durchschnittlichen Update-Zyklen für die Malware-Abwehr waren in dieser Erhebung auf Gateway-Systemen mit 6,3 Std. sowie auf Servern mit 7,4 Std. jeweils um fast anderthalb Stunden kürzer als 2012; auch auf PCs/Workstations war mit 11,2 Std. immerhin noch ein Plus von einer halben Stunde zu verzeichnen. Scanner auf mobilen Endgeräten weisen in Sachen Update-Frequenz weiterhin eine deutlich höhere Streuung auf und landen dieses Mal im Mittel bei knapp 16 Std., was sich in die Werteskala der vorigen Studien einreiht (2012: 19 Std., 2010: 12 Std., 2008: 16 Std.).

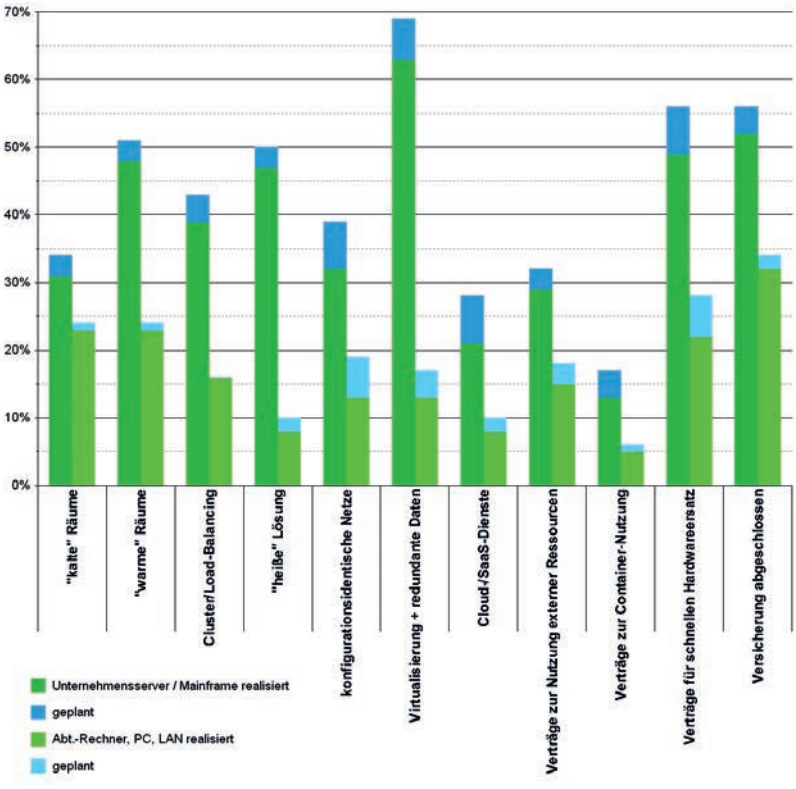


Abbildung 20: Bereitstellungen für längere Ausfälle

Basis: Ø 112 Antworten (Unternehmensserver/Mainframes), Ø 109 (Abt.-Systeme/PCs)

Eine weitere leichte Entspannung zeigt sich in Sachen Spam (Abb. 19): Im Mittel haben die Befragten 34 % unerwünschte E-Mails erhalten (2012: 38 %, 2010/2008: 53 %, 2006: 33 %, 2004: 24 %) – und „nur" noch ein starkes Viertel erhält mehr Spam als erwünschte Nachrichten (2012: 36 %, 2010/2008: 56 %, 2006: 27 %, 2004: 15 %). Allerdings beruhen diese Zahlen auch weiterhin zum größten Teil auf Schätzungen (86 %).

Die Bereitschaft, E-Mails zu chiffrieren, sofern die notwendigen Kryptoschlüssel beim Kommunikationspartner vorliegen, übertrifft das bereits vergleichsweise hohe Niveau der vorigen Studie: 69 % der Befragten würden dann zumindest sensitive Nachrichten verschlüsseln (2012: 61 %, 2010: 52 %, 2008: 48 %, 2006: 47 %), 23 % alle externen, 19 % *alle* Nachrichten (Mehrfachnennungen). Der Anteil der „Verweigerer", die trotz bestehender Möglichkeit „nie" verschlüsseln, sank erneut deutlich auf 23 % (2012: 32 %, 2010: 38 %, 2008: 44 %, 2006: 42 %).

Signaturen sind – auch bei vorliegenden Schlüsseln – jedoch weiterhin weniger beliebt und würden nun von 43 % der Befragten für sensitive E-Mails (–2 %-Pkt.), 21 % für externe Nachrichten (–10 %-Pkt.) und von 19 % für alle Nachrichten (–5 %-Pkt.) verwendet. 42 % „Signaturmuffel", die trotz entsprechender Vorbedingungen „nie" signieren, entspricht in etwa dem Wert von 2012 (43 %).

Bei den eingesetzten Standards positioniert sich S/MIME mit 67 % Nutzung erstmals klar vor (Open)PGP mit 47 % (Mehrfachnennungen) – 18 % der Teilnehmer verwenden (zumindest auch) sonstige Verfahren. Eine virtuelle Poststelle zur zentralisierten Ver-/Entschlüs-

selung und Signaturerstellung/-prüfung haben 23 % der Befragten realisiert (2012: 25 %, 2010: 17 %, 2008: 10 %), weitere 20 % in Planung.

In Sachen Infrastruktur für elektronische Signaturen (Tab. 19) legt die aktuelle Stichprobe wieder eine stärkere Betonung auf Software-Lösungen (+9 %-Pkt. „realisiert"), statt Hardware-Token (–10 %-Pkt.) oder Chipkarten (–19 %-Pkt.) einzusetzen. Besonders der elektronische Personalausweis ist unbeliebt wie nie: Für 90 % kommt eine Nutzung für Signaturen überhaupt nicht infrage – der geplante Einsatz für Geschäftsprozesse verharrt bei 12 %. Jeder Fünfte bezeichnete seine Kenntnisse über die Möglichkeiten des „neuen" Personalausweises (nPA) als „gering" (+7 %-Pkt.) – nur noch 23 % sahen sich hier „umfassend" informiert (–5 %-Pkt.). Immerhin noch 35 % glauben aber dennoch, dass der elektronische Geschäftsverkehr durch den nPA für Bürger und Unternehmen interessanter wird (–11 %-Pkt.).

Notfallvorsorge

Angaben zu Existenz und Besonderheiten von IT-Notfall- und -Wiederanlauf-Konzepten beschreibt Tabelle 20 – der Anteil der Teilnehmer mit einem entsprechend ausgearbeiteten Konzept reiht sich mit 80 % am oberen Ende der Bandbreite der vorausgegangenen Studien ein (2004–2012: 69–82 %).

Einige klare Veränderungen gegenüber 2012 zeigen die Bereitstellungen für längere Ausfälle (Abb. 20): Einerseits haben Cloud- und Software-as-a-Service-(SaaS)-Dienste als „Reserve" für zentrale IT erneut deutlich zugelegt (+12 %-Pkt. „realisiert" oder „geplant"), zum anderen ist die Bedeutung von Verträgen zur Container-Nutzung in dieser Studie erheblich gesunken (–10 %-Pkt. bei zentralen Servern/Mainframes, –7 %-Pkt. bei Abt.-Systemen/PCs). Ferner zeigt sich eine geringere Affinität zu Verträgen über die schnelle Lieferung von Hardware auf Abteilungsebene (–12 %-Pkt.). Von 67 Befragten, die einen Recovery-Vertrag abgeschlossen haben, mussten 12 diesen in den vorausgegangenen zwei Jahren in Anspruch nehmen – 7 sogar mehrmals.

Für die Notfalldokumentation nutzen 69 % der Befragten derzeit ein manuelles und 54 % ein onlinegestütztes Handbuch – eine Online-Anwendung ist bereits bei 16 % im Einsatz. Ein gutes Fünftel (21 %) aktualisiert seine Dokumentation regelmäßig (+2 %-Pkt.), wenngleich im Mittel etwas seltener als in vorigen Studien, nämlich durchschnittlich alle 274 Tage (2006–2012: 154–231 Tg.). 70 % aktualisieren anlassbezogen (–2 %-Pkt.), erneut 9 % „nie".

Datenverluste und Forensik

Erheblich weniger Teilnehmer als in der vorigen Studie hatten in den vorausgegangenen zwei Jahren nennenswerte Probleme mit (zumindest zeitweise) unverfügbaren oder verlorenen Daten: Dies war bei 22 % (–15 %-Pkt.) der Fall. Die Gründe für die Ausfälle zeigt Abbildung 21. Die große Mehrheit davon (85 %) konnte jedoch alle betroffenen Daten wiederherstellen: 67 % griffen auf ein Backup zurück, 30 % auf manuelle Neuerfassung, 26 % auf Selbsthilfe per Datenrettungs-Tool, 7 % auf externe Datenrettung und 7 % auf Sonstiges (Mehrfachnennungen).

Die geschätzten Verluste bei einer Vernichtung aller elektronisch gespeicherten Daten zeigt Tabelle 21 – im Durchschnitt ergaben sich rund 350 Mio. € (KMU 128 Mio. € / Große 540 Mio. €). Acht weitere Teilnehmer gaben sinngemäß an, ein entsprechender Verlust wäre für ihre Organisation existenzgefährdend oder ruinös.

Bei einem Fünftel der Teilnehmer wurde 2012/2013 mindestens ein Sicherheitsvorfall rechtlich verfolgt. Wo das nicht der Fall war, gab es bei 76 % tatsächlich keinen Vorfall zu beklagen, bei 18 % fehlte es an Verfolgungsinteresse und bei 6 % an Wissen um Ermittlungsmöglichkeiten.

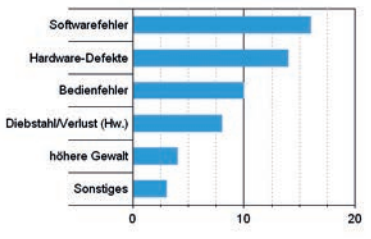
IT-Notfall-/Wiederanlaufkonzept	
… existiert	80%
… ist schriftlich fixiert	90%
berücksichtigt explizit spezielle Anforderungen für/bei…	
… Hardware-Ausfall/ -Wiederbeschaffung	93%
… physische Einwirkungen	92%
… Software-Sicherheitsvorfälle	74%
… Hochverfügbarkeit des E-Business	72%
… Malware-/Exploit-Epidemien	72%
… Zusammenbruch externer Infrastrukturen	70%
… Denial-of-Service-Attacken	56%
… gezielte Angriffe durch Einzeltäter	53%
Unternehmswichtige Daten liegen räumlich getrennt vor	87%

Basis: Ø 100 Antworten

Tabelle 20: Existenz und Besonderheiten von IT-Notfall-/Wiederanlaufkonzepten

Dienstleistungen

Ein eigenes Computer-Emergency-Response-Team (CERT) betreibt ein Viertel der Befragten – knapp zwei Fünftel nutzen Dienste eines externen Teams (26 % nur kostenlos, 13 % auch kostenpflichtig). Generell nutzen 61 % Outsourcing in der einen oder anderen Form



Basis: Ø 27 Antworten

Abbildung 21: Ursachen für Verluste oder (zumindest zeitweilige) Nichtverfügbarkeit von Daten

Datenwert / Verlust	Nennungen
unter 10 Tsd. €	2
unter 100 Tsd. €	6
unter 1 Mio. €	15
unter 100 Mio. €	18
unter 500 Mio. €	6
unter 1 Mrd. €	1
ab 1 Mrd. €	8

Basis: 56 Antworten

Tabelle 21: Geschätzter Verlust bei Vernichtung aller elektronisch gespeicherten Daten

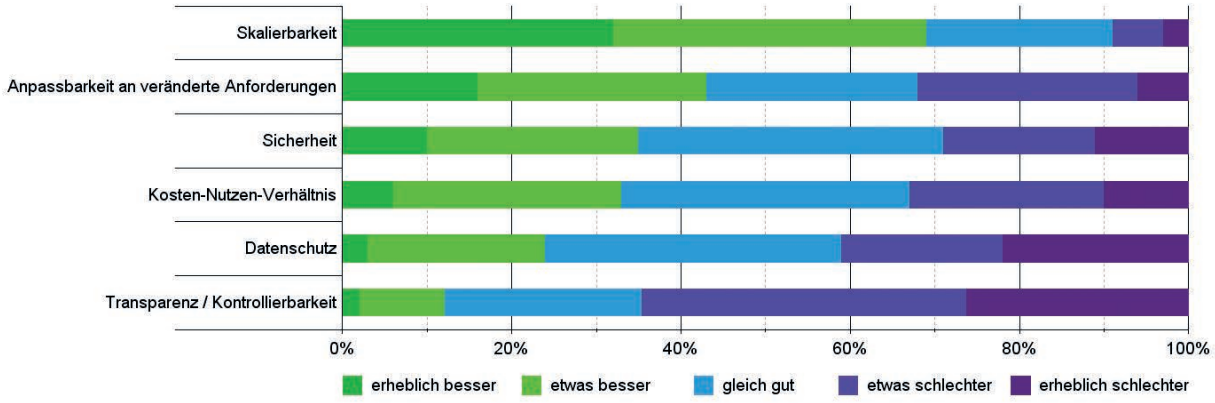


Abbildung 22: Externe Dienste (Outsourcing/ MSS/Cloud) im Vergleich zu In-house-Lösungen

Basis: Ø 106 Antworten

(KMU 53 % / Große 68 %) – Tabelle 22 zeigt, wofür. Mit diesen Leistungen sind die Teilnehmer weiterhin zufrieden und vergeben im Mittel erneut eine knappe „Zwei“: 77 % befanden Outsourcingdienste als „sehr gut“ oder „gut“ – nur jeder Zehnte sah sie als gerade einmal oder nicht mehr ausreichend an.

genutzte Outsourcing-Dienstleistungen	
Vernichtung von Datenträgern (Papier, IT)	75%
Wachschutz / Bewachung	55%
gesamte(s) Rechenzentrum/IT	39%
Netzwerk-Management	36%
Spamabwehr	35%
E-Mail-Betrieb	35%
Anwendungssysteme	35%
Managed Firewall/IDS/IPS	32%
Archivierung, Dokumentation	29%
Betriebssystempflege/Administration	29%
Datensicherung, Backup-Lösungen	27%
Content-Security/Virenabwehr	19%
Datenbank-Systeme/-Werkzeuge	18%
Datenschutz	18%
Haustechnik	14%
Personaleinsatz/-entwicklung, Mitarbeiterweiterbildung	8%
Notfallvorsorge/Business-Continuity	8%
externer ISi-Beauftragter	6%

Tabelle 22: Outsourcing

Basis: 77 Antworten

genutzte Consulting-Dienstleistungen	
Penetrationstests	67%
Risikoanalysen und Konzeptentwicklung	54%
Schwachstellenanalysen	49%
Kontrolle vorhandener Konzepte	42%
Strategie- und Managementberatung	41%
Umsetzung von Konzepten und Maßnahmen	41%
Produktberatung und Kaufunterstützung	29%
Durchführung von Inhouse-Schulungen	26%
Prozess-Entwicklung und -Optimierung	25%

Tabelle 23: ISi-Beratung

Basis: 76 Antworten

Dabei erweist sich die aktuelle Stichprobe als sehr regelungs- und auditfreudig: Service-Level-Agreements (SLAs) oder vergleichbare Vereinbarungen existieren bei 95 % (+14 %-Pkt. gegenüber einem bereits „strengen“ Ergebnis von 2012). Explizite Anforderungen an den Datenschutz stellen dabei 80 % (–2 %-Pkt.), Regelungen zu Haftungsübernahme oder Schadenersatz haben 74 % vereinbart (+13 %-Pkt.) Und in Sachen ISi sind jetzt bei immerhin 67 % explizite Anforderungen festgehalten (+13 %-Pkt.). Auch Prüfungen erfolgen nunmehr in allen Bereichen bei rund der Hälfte „regelmäßig“ (je +12 %-Pkt.) und nur noch eher selten „nie“ (bei 4 % bzgl. ISi und je 8 % bzgl. Datenschutz und allg. SLAs).

Vorzüge von Outsourcing (inkl. MSS und Cloud-Diensten) gegenüber Inhouse-Lösungen sehen die Befragten vor allem in Sachen Skalierbarkeit und Anpassbarkeit an veränderte Anforderungen. Sicherheit sowie Kosten-Nutzen-Verhältnis erhalten eine in etwa ausgeglichene Bewertung – Datenschutz sowie Transparenz und Kontrollierbarkeit werden überwiegend schlechter bewertet. Details zeigt Abbildung 22.

Keine allzu großen Transparenzprobleme beobachten die Teilnehmer hingegen erneut bei Applikationen oder Sicherheitssystemen, die auf Cloud- oder Web-Services zurückgreifen: 50 % waren sich sicher, dass es so etwas in ihrem Haus nicht gibt (2012: 54 %, 2010: 57 %) – weitere 20 % sagten „vermutlich nicht“ (2012: 16 %, 2010: 23 %). Ein klares „Ja“ gab es hingegen von 23 % (2012: 22 %, 2010: 14 %), „vermutlich ja“ gaben 6 % an (2012: 8 %, 2010: 6 %). Gut zwei Drittel der Nutzer solcher Systeme sahen dabei deren Kommunikation sowie die Weitergabe von Daten an den Dienstleister als hinreichend nachvollziehbar an.

ISi-Beratung wird von der jetzigen Stichprobe ein wenig häufiger nachgefragt als in der vorigen Studie: Über das gesamte Teilnehmerfeld nutzen 13 % „häufig“ und 50 % „gelegentlich“ Consulting-dienstleistungen (jeweils +3 %-Pkt.); weiterhin liegen die großen Unternehmen hier vorn (19 % / 60 % vs. 5 % / 39 % bei KMUs). Genutzte Dienste (siehe Tab. 23) bewerteten 80 % der Teilnehmer als „sehr gut“ oder „gut“, nur 4 % sahen sie als gerade einmal oder nicht ausreichend an – im Mittel fast eine glatte „Zwei“.

77 % gaben für die Auswahl eines Consulting-Partners dessen Reputation und Leistungsspektrum als besonders wichtiges Kriterium an. 54 % konzentrieren sich vorzugsweise auf die Zusammenarbeit mit einem einzelnen Berater. Kurzfristige Partnerschaften zugunsten eines „Best-Price“-Prinzips (20 %)

oder ein häufiger Wechsel zugunsten der Meinungsvielfalt in Sachen Beratung (11 %) waren hingegen eher unbeliebt.

Teilnehmer

Die eingegangenen Fragebögen wurden zu 65 % von Teilnehmern ausgefüllt, die unmittelbar für die Informations-Sicherheit verantwortlich sind oder anderweitig leitende Positionen innehaben. Auch in diesem Jahr ist der Anteil der CISOs und expliziten IT-Sicherheits-Verantwortlichen noch einmal deutlich gestiegen und lag nunmehr bei 38 % (Tab. 24). In den großen Unternehmen kamen mit 53 % wieder über die Hälfte aller eingesandten Fragebögen vom CISO/IT-Sicherheitsverantwortlichen. Bei den KMU waren es immerhin noch 19 % – weitere große Ausfüller-Gruppen aus den Häusern unter 500 Mitarbeitern waren Geschäftsführer (21 %) und RZ-/IT-Leiter (17 %).

Auch bei der Frage nach den vorhandenen Funktionsträgern in den teilnehmenden Unternehmen und Behörden (Tab. 25) zeigte sich eine weiter gestärkte Sicherheitsorganisation: IT-Sicherheitsverantwortliche und CISOs legten im Vergleich zu 2012 noch einmal um +5 %-Punkte zu und waren nun in 62 % aller teilnehmenden Organisationen vorhanden; ISi-Ausschüsse oder ähnliche Gremien legten insgesamt sogar um +8 %-Punkte zu (KMU +3 %-Pkt. / Große +5 %-Pkt.). Auch Datenschutzbeauftragte hatte die aktuelle Stichprobe wieder häufiger vorzuweisen (+5 %-Pkt.) und erreicht damit nach einer schwächeren Repräsentanz in 2012 nun wieder fast die intensive Durchdringung der vorletzten Studie.

Die Nationalität des Hauptsitzes der Studienteilnehmer zeigt Abbildung 23, ihre Branchenzugehörigkeit ist in Tabelle 26 zu finden. Das „durchschnittliche Unternehmen“ dieser Studie (unter Auslassung eines einzelnen Großbetriebs mit enormer IT-/ISi-Abteilung) beschäftigt insgesamt 3381 Mitarbeiter, davon 116 in der IT mit vier ausgewiesenen ISi-Spezialisten. Den befragten KMU standen im Mittel 136 Mitarbeiter mit 16 ITlern inklusive zwei Sicherheitsexperten zur Verfügung – den „Großen“ (exkl. des genannten Ausreißers) 6330 Mitarbeiter, davon eine 206-köpfige IT-Abteilung mit sechs ISi-Spezialisten. Eine Staffelung der teilnehmenden Organisationsgrößen zeigt Abbildung 24.

Infrastruktur

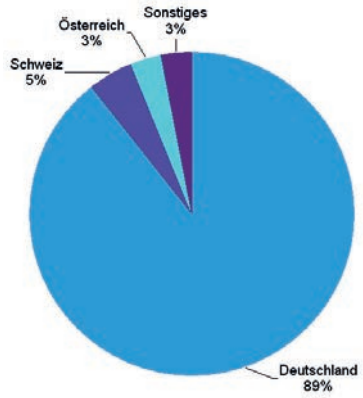
Die gemittelte IT-Landschaft des „Durchschnittsunternehmens“ dieser Studie umfasst 3 Mainframes (KMU 1 / Große 5), 358 Server (51 / 685), 1918 Clients/PCs (147/3742) sowie 67 Heim-/Telearbeitsplätze (10 / 125). Hinzu kommen noch 703 Note-/Netbooks (39 / 1423), 308 Smartphones und Tablets (30 / 600) sowie 757 Voice-over-IP-(VoIP)-Systeme (96 / 1505). Für „gute Verbindungen“ sorgen durchschnittlich 32 Weitverkehrsnetze (5 / 59 – jeweils inkl. VPN und Mietnetzen), 49 LAN-/PC-Netze (4 / 97) sowie 22 Wireless LANs (2 / 43).

Betrachtet man die Zahl der Endgeräte (ohne VoIP-Systeme) für jede einzelne Organisation, die an der Studie teilgenommen hat, so liegt der Durchschnitt bei 2962 (KMU 225 / Große 5782). Der Anteil der mobil betriebenen Systeme ist über die gesamte Stichprobe von rund einem Drittel in den vorausgegangenen beiden Studien auf jetzt 40 % gestiegen. Die KMU haben sogar um +9 %-Punkte auf 47 % Mobilanteil zugelegt – die großen Unternehmen sind hier weiterhin etwas zurückhal-

IT-Sicherheitsverantwortlicher/CISO	38%
RZ-/IT-Leiter	12%
Geschäftsführer	10%
Administrator/Systemtechniker	8%
Datenschutzbeauftragter	7%
IT-Mitarbeiter	6%
Sonstiges	6%
IT-Sicherheitsadministrator	5%
Orga-Leiter	4%
Revisor	3%
CIO	1%

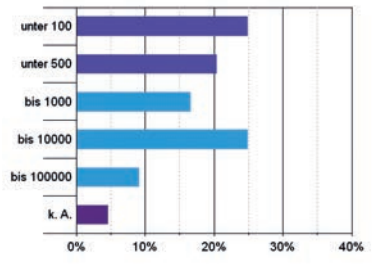
Basis: 126 Antworten

Tabelle 24: Funktionsbezeichnung der Fragebogenausfüller



Basis: 131 Antworten

Abbildung 23: Hauptsitz der teilnehmenden Unternehmen und Behörden



Basis: 133 Antworten

Abbildung 24: Größe der teilnehmenden Organisationen

Im Unternehmen gibt es …	alle	KMU	Große
ISi-Beauftragter/C(I)SO	62%	42%	78%
ISi-Ausschuss (o.Ä.)	34%	21%	43%
Datenschutzbeauftragter	84%	72%	93%
Leiter IT/DV/RZ	83%	72%	91%
IT-/DV-Revision	33%	18%	46%
Leiter Organisation	46%	42%	49%
Leiter Sicherheit/Werkschutz	33%	11%	49%
IT-Administratoren	83%	82%	82%
DV-orientierter Jurist	21%	9%	31%

Basis: 128 Antworten (KMU: 57, Große 67)

Tabelle 25: Vorhandene Funktionsträger in den befragten Organisationen

Behörden/öffentliche Hand	17%
Kreditwirtschaft	17%
Berater	15%
übrige Industrie (ohne chem. Industrie)	12%
Gesundheitswesen	5%
Telekommunikationsdienstleister/ Provider	5%
Handel	4%
Wissenschaft/Forschung/Schulen	4%
Energieversorgung	3%
Versicherungen	3%
chemische Industrie	2%
Outsourcing-Dienstleister	2%
Transport/Verkehr	2%
Verlage/Medien	2%
Sonstiges	6%

Tabelle 26: Branchenzugehörigkeit der Studien-Teilnehmer

Basis: 130 Antworten

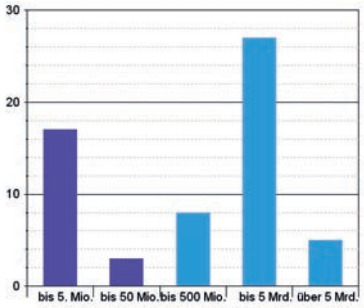


Abbildung 25: Geschäftszahlen (Umsatz bzw. Bilanzsumme) der Studienteilnehmer [Nennungen]

Basis: 60 Antworten

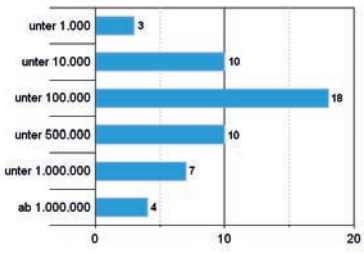


Abbildung 28: Budget für Informations-Sicherheit [Anzahl der errechneten Werte]

Basis: 52 Antworten

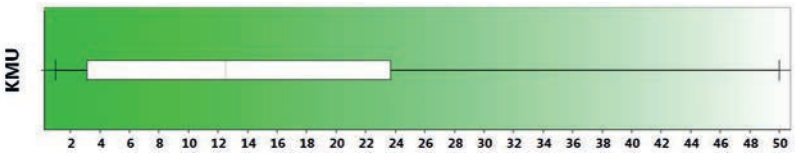


Abbildung 26: Anteil der ISi am IT-Budget bei teilnehmenden KMU (ohne Extremwert)

Basis: 25 Antworten

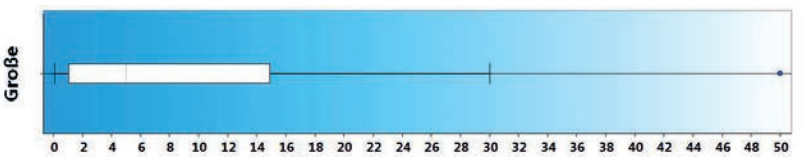


Abbildung 27: Anteil der ISi am IT-Budget bei teilnehmenden großen Organisationen (ohne Extremwerte)

Basis: 31 Antworten

tender, steigerten sich aber ebenfalls erheblich um +6 %-Punkte auf nunmehr 33 %.

Budgets

Konkrete Zahlen zu Umsatz oder Bilanzsumme ihres Hauses haben 60 Befragte mitgeteilt – 42 weitere gaben an, dass solche Zahlen in ihrer Organisation nicht relevant seien, da es sich um eine Behörde oder Ähnliches handelt.

Der hierbei duchschnittlich angegebene Umsatz betrug circa 1,2 Mrd. € (KMU 102 Mio. € / große Unternehmen 2,3 Mrd. €) – die mittlere genannte Bilanzsumme belief sich auf gut 8 Mrd. € (1,4 Mrd. € / 20,5 Mrd. €). Eine gestaffelte Darstellung der entsprechenden Nennungen dieser Geschäftszahlen zeigt Abbildung 25.

Zu verfügbaren Mitteln für die IT und die Informations-Sicherheit (ISi) haben wir Angaben von 66 beziehungsweise 61 Teilnehmern erhalten. Bei diesen Zahlen waren wieder einmal fast alle Befragten auf Schätzungen angewiesen: Nur fünf Teilnehmer aus großen Unternehmen konnten auf ermittelte Werte für das IT-Budget zurückgreifen, beim Anteil für die ISi war das sogar nur einem möglich.

Auf Basis dieser Angaben verfügte das „durchschnittliche Unternehmen“ in dieser Studie für das Jahr 2013 über ein IT-Budget (inkl. Personalkosten) von gut 10 Mio. € (KMU 530 Tsd. € / Große 19 Mio. €).

Die Antworten zum Anteil für die Informations-Sicherheit waren erneut sehr stark gestreut – das rechnerische Mittel über alle Angaben betrug rund 11,5 % (8 % unter Ausschluss von Extremwerten), der Median lag bei 5 %. Abbildung 26 zeigt einen Boxplot der ISi-Anteile für KMU (unter Auslassung eines Extremwerts von 100 %), Abbildung 27 liefert die Verteilung der Werte für große Unternehmen (unter Auslassung zweier Nullangaben und eines Extremwerts von 80 %).

Absolute ISi-Budgets konnten wir aus 52 Fragebögen errechnen, in denen sowohl Angaben zu IT-Budgets als auch zum Anteil der Informations-Sicherheit enthalten waren. Hieraus ergeben sich durchschnittliche finanzielle Mittel für die ISi von gut 266 Tsd. €, beziehungsweise rund 29 Tsd. € in der Teilmenge aus den KMU und 469 Tsd. € bei großen Unternehmen. Eine gestaffelte Auswertung dieser errechneten Zahlen zeigt Abbildung 28. ■

Impressum

Sonderdruck aus <kes> – Die Zeitschrift für Informations-Sicherheit
Nr. 2014#4, 2014#5 und 2014#6
für Applied Security GmbH
Einsteinstr. 2a
63868 Großwallstadt

Lise-Meitner-Straße 4
55435 Gau-Algesheim
Telefon +49 6725 9304-0
E-Mail: info@secumedia.de
Web: www.kes.info

Verantwortlich i.S.d.P.:
Norbert Luckhardt

Satz und Layout:
Black Art Werbestudio
Schnaas und Schweitzer
55413 Weiler

Druck: PRINTEC OFFSET
Ochshäuser Straße 45
34123 Kassel

Sind Sie verantwortlich für die IT-Sicherheit?
Dann lernen Sie <kes> jetzt noch besser kennen!

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

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit, Zutrittskontrolle, Virenabwehr, Verschlüsselung, Risikomanagement, Abhör- und Manipulationsschutz, Sicherheitsplanung, Elektronische Signatur und PKI, IT-Recht, BSI-Forum

<kes> ist *die* Fachzeitschrift zum Thema Informations-Sicherheit – eine Garantie für Zuverlässigkeit.

Neben den regulären Ausgaben können Sie von den <kes> Specials profitieren, die zu Messen oder besonderen Themen erscheinen.

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 Kurzmeldungen, Links zu relevanten Veranstaltungen sowie aktuelle Artikel zum Probelesen.

www.kes.info

PROBEHEFT-ANFORDERUNG

ja, bitte schicken Sie mir gratis und unverbindlich

- ☐ ein Exemplar **<kes>** – **Die Zeitschrift für Informations-Sicherheit**
- ☐ ein Exemplar **<kes> Special** „Mobile Security"
- ☐ ein Exemplar **<kes> Special** „Wirtschaftsspionage"
- ☐ ein Exemplar **<kes> Special** „E-Health"

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Datum | Zeichen | Unterschrift

FAX an +49 6725 5994

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

Lieferung bitte an

Telefon Durchwahl

IT-Sicherheit einfach effizient

Auf Kurs in ruhige Gewässer

www.apsec.de

Verschlüsselung für alle!

Und das für jeden Geldbeutel – sogar für den leeren!

fide*AS*® file private:

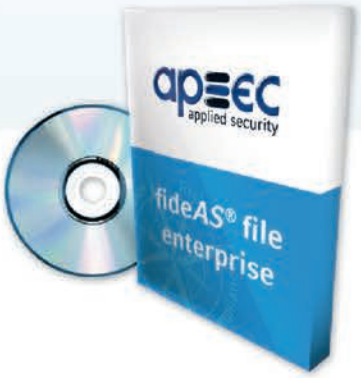
Die besten Dinge im Leben sind kostenlos.

Sichern Sie Ihre Privatsphäre mit Profi-Software. **fide*AS*® file private** verschlüsselt alle sensiblen Dateien auf Ihrem PC, Laptop oder USB-Stick und schützt sie so vor unbefugtem Zugriff.
Einfach, effizient und sicher.

fide*AS*® file workgroup:

Für kleine Unternehmen mit großen Ansprüchen.

Für kleine Unternehmen mit maximal 5 bzw. 25 Arbeitsplätzen gibt es **fide*AS*® file workgroup**. Der netzwerk- und gruppenfähige Bruder von **fide*AS*® file private** sichert Daten auch im Geschäftsumfeld.



fide*AS*® file enterprise:

Das Flaggschiff mit maximalem Komfort.

Die File-Folder-Verschlüsselung bietet optimalen Schutz. Verschlüsselt werden können Dateien auf Fileservern, PCs oder Notebooks, mobilen Datenträgern wie USB-Sticks oder Dateiablagen in der Cloud.

Mehr Infos gibt es auf www.daten-verschluesselung.de

Applied Security GmbH · Einsteinstraße 2a · 63868 Großwallstadt
Telefon: +49 (0) 60 22 / 263 38-0 · info@apsec.de · www.apsec.de

IT-Sicherheit – Made in Germany seit 1998.

apsec applied security