<kes>
Die Zeitschrift für Informations-Sicherheit

special

Auszüge aus <kes> 2018#4/6

Sonderdruck für UIMC®

IT-Landschaften 2018: Lagebericht zur Sicherheit

DATAKONTEXT

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

seit über 30 Jahren stellt die <kes>/Microsoft-Sicherheitsstudie Zahlen und Fakten zur Verfügung, die in ihrer Gesamtheit ein hervorragendes Lagebild zur Informationssicherheit (ISi) liefern. Die Studie bietet neben Sicherheitsverantwortlichen auch Datenschutzbeauftragten eine gute Übersicht zu relevanten Themen und eröffnet den Blick auf Synergieeffekte zwischen beiden Bereichen.

Gerade in den Zeiten von WannaCry und der erst kürzlich bekanntgewordenen Datenpanne bei Google+ gewinnt die Kombination der Themen Informationssicherheit und Datenschutz merklich an Bedeutung. Eine getrennte Betrachtung der beiden Themenbereiche ist für ein Unternehmen kaum mehr möglich und noch weniger sinnvoll.

Dies liegt primär an der generell gestiegenen Bedeutung des Datenschutzes im Zusammenhang mit der Datenschutz-Grundverordnung (DSGVO). Einen eindeutigen Beleg hierfür liefert die Umfrage: Die DSGVO erreichte eine Relevanz von 99 Prozent unter den befragten Unternehmen; sicherlich begünstigt durch eine fortgesetzte mediale Berichterstattung zur Datenschutz-Novelle.

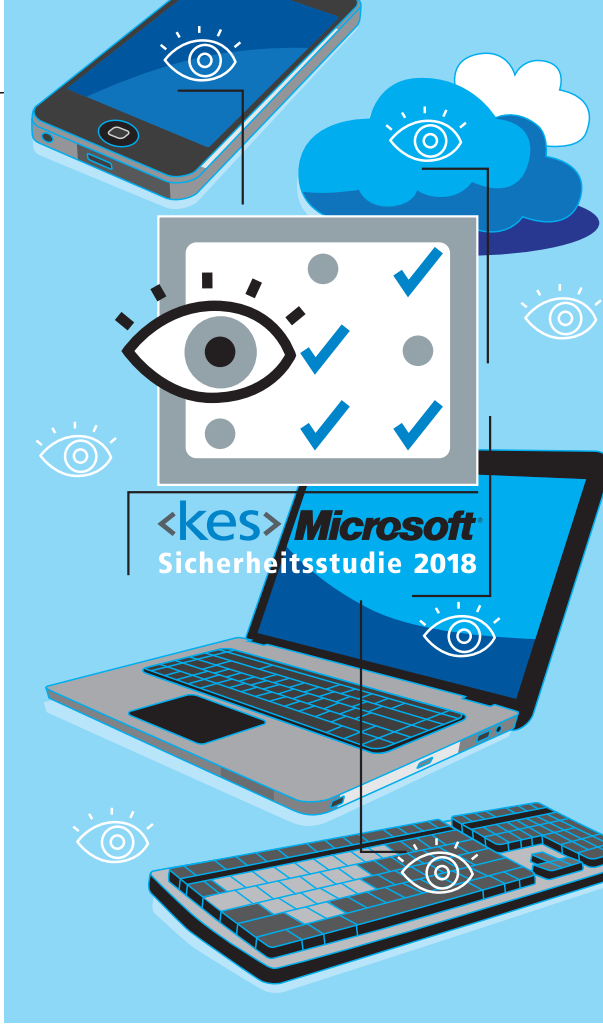
Neben den Veränderungen durch die DSGVO im Feld des Datenschutzes sind die Auswirkungen im Bereich der ISi keineswegs unbedeutender. Der Fall liegt klar: die DSGVO führt im Rahmen der technischen und organisatorischen Maßnahmen zu einer Neuausrichtung. So fordert die DSGVO nicht nur die Erfüllung der klassischen Ziele der ISi, sondern stellt auch Forderungen nach erhöhter Transparenz und regelmäßiger Revision der implementierten Maßnahmen, die stark an ein Informationssicherheits-Managementsystem (ISMS) erinnern. Hieraus ergibt sich der Aufbau eines Datenschutz-Managementsystems im Sinne eines ISMS für personenbezogene Daten. Eine getrennte Betrachtung ist demnach wenig sinnvoll, um keine Synergien durch zwei parallele Systeme zu verlieren.

Vor diesem Hintergrund haben drei Fragestellungen im Rahmen der Studie eine besondere Aufmerksamkeit verdient: 1. 56 Prozent der Befragten sagen, dass die DSGVO keine Auswirkung auf das eigene Management-System hat. 2. Bei 29 Prozent gibt es kein Datenschutzmanagement-System. 3. Trotzdem nehmen aber 52 Prozent der Befragten an, dass ihr Unternehmen bis zum Stichtag „compliant" im Sinne der DSGVO gewesen sein sollte. Diese Zahlen lösen Stirnrunzeln aus. Besonders vor dem Hintergrund der Tatsache, dass die geforderten Maßnahmen im Rahmen der DSGVO fast zwangsläufig Veränderungen des ISMS zur Folge haben müssten.

Denn gerade aus dem Datenschutz, in seiner originären Bedeutung, ergeben sich viele Chancen für die ISi und vice versa. So können Informationssicherheits- und Datenschutzprojekte zusammenhängend und effektiv gesteuert und gemanagt werden. Folge: der zusätzliche Mehraufwand bleibt überschaubar und eine vollständige „Compliance" kann sichergestellt werden.

Die Studie stellt einen wichtigen Impuls für eine Sensibilisierung bei der Verschränkung von Datenschutz und Informationssicherheit dar. In diesem Sinne wünsche ich Ihnen viel Spaß bei der Lektüre und viel Erfolg beim Aufspüren neuer Erkenntnisse.

Ihr
Dr. Jörn Voßbein



IT-Landschaften 2018:
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.

Für die diesjährige <kes>/Microsoft-Studie haben wir 99 verwertbare Fragebögen erhalten – damit bleibt die Teilnehmerzahl deutlich unter den vorigen Erhebungen zurück (s. a. Schlussbemerkung auf S. 25). Umso mehr bedanken wir uns für die umfassenden und vertrauensvollen Angaben der Studienteilnehmer sowie die Unterstützung durch Sponsoren und Partner!

Einige Kernaussagen lauten zusammengefasst:

_____ Malware schafft den „Hattrick“: Erstmals landen Viren, Würmer und Trojanische Pferde zum dritten Mal in Folge auf dem ersten Rang der bedeutendsten Gefährdungen – „Irrtum und Nachlässigkeit eigener Mitarbeiter“ holt wieder etwas auf, Hacking normalisiert sich.

_____ Die Malware-Abwehr hat weiterhin einen schweren Stand – die aktuelle Stichprobe zeigte zwar etwas weniger dramatische Indikatoren als diejenige von 2016, belastbare Anzeichen für eine Entwarnung sind jedoch nicht zu erkennen.

_____ Vertraulichkeitsbrüche sind wieder bei mehr als der Hälfte der Befragten zu beobachten gewesen. Hinsichtlich der Ursachen bleibt Social-Engineering an erster Stelle – Datenlecks und Probleme bei Partnern sowie Verlust und Diebstahl von Systmen und Datenträgern waren seltener anzutreffen.

_____ Probleme mit mangelndem Sicherheitsbewusstsein der Mitarbeiter bleiben als Hindernis für eine Verbesserung der Informations-Sicherheit auf Rekordniveau – Bewusstsein und Unterstützung durch das Top-Management erhält historisch schlechte Bewertung.

_____ Die EU-Datenschutzgrundverordnung (DSGVO) erhält höchste Aufmerksamkeit und wird von nahezu allen Studienteilnehmern gekannt und als relevant für die eigene Arbeit angesehen – aber nur gut die Hälfte hat erwartet, dass Systeme und Prozesse ihres Hauses bereits zum Stichtag „compliant“ sein würden.

Risikosituation

Als Top-Gefährdung, der man die höchste Aufmerksamkeit schenken muss, gilt den Teilnehmern der diesjährigen Studie erneut die Malware (vgl. Tab. 1 – „Bedeutung heute“). Damit bleibt diese Kategorie erstmals in der Geschichte der <kes>-Studien dreimal hintereinander auf Rang eins vor dem „Dauerbrenner“ „Irrtum und Nachlässigkeit eigener Mitarbeiter“, auch wenn der historische Vorsprung aus der vorigen Erhebung (2016: +0,48 Prio-Pkt.) wieder deutlich schrumpft und sich dem Abstand von vor vier Jahren annähert (2018: +0,26, 2014: +0,22).

Hintergrund der in der Tabelle genannten Prioritäten ist die Annahme, dass man bei begrenzten Ressourcen für die Informations-Sicherheit (ISi) 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 vergeben die Teilnehmer unserer Studien auf diese Weise zwischen 8 und 9 Punkten, die anschließend für jeden Fragebogen individuell auf sechs Punkte normiert und für die Auswertung gemittelt werden.

Auf den Rängen drei bis sechs rangiert dabei die typische „Verfolgergruppe“ der letzten Dekade, die nun wieder enger zusammenrückt. Vor vier Jahren hatte sich das Hacking etwas nach vorne abgesetzt und einen kleinen Vorsprung auch

2016 verteidigt. Nun fiel es wieder in der Beachtung – um –0,11 Prioritätspunkte (Diff. ungerundeter Werte) und damit sogar knapp hinter die Dokumentationsmängel, die ein kleines Plus (+0,05 Prio-Pkt.) verzeichneten. Insgesamt liegt das Hacking damit nahe am Mittelwert der Studien von 2008 bis 2016 (0,60 Prio-Pkt.).

In der zweiten Tabellenhälfte verliert „Sabotage“ zwar zwei Plätze (–0,04 Prio-Pkt.), bleibt aber den jetzt minimal höher eingeordneten Hardwaremängeln sowie „unbeabsichtigten Fehlern von Externen“ dicht auf den Fersen. „Manipulation zum Zweck der Bereicherung“ schließt zu dieser Gruppe auf (+0,09 Prio-Pkt.), bleibt aber auf dem 10. Platz.

Schäden

Bei der Frage, ob die jeweiligen Gefährdungen in den vorausgegangenen zwei Jahren auch „tatsächlich zu mittleren bis größeren Beeinträchtigungen“ geführt haben („Schäden“ in Tab. 1), korrespondieren die drei größten Veränderungen mit den Prioritätsanpassungen der aktuellen Stichprobe.

Die Zahl der Opfer erheblicher Malwareschäden ist um –11 Prozentpunkte zurückgegangen und fast wieder auf den Wert von 2014 gesunken (32 %, 2016: 43 %, 2014: 31 %, 2012: 28 %, 2010: 27 %).

Wir danken den Sponsoren unserer Studie

Weiterhin gilt unser Dank den Organisationen, 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).

	Vorhersage 2016		Bedeutung heute		akt. Prognose		Schäden	
	Rang	Priorität	*Rang*	*Priorität*	Rang	Priorität	Rang	ja, bei
Malware (Viren, Würmer, Troj. Pferde, ...)	1	1,43	1	1,19	1	1,18	2	32%
Irrtum und Nachlässigkeit eigener Mitarbeiter	3	0,70	2	0,93	2	0,71	1	34%
Mängel der Dokumentation	5	0,53	3	0,58	7	0,46	5	19%
Hacking (Vandalismus, Probing, Missbrauch, ...)	2	0,78	4	0,56	4	0,67	11	5%
Software-Mängel/-Defekte	7	0,48	5	0,55	5	0,63	3	27%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	4	0,63	6	0,53	3	0,69	7	9%
Hardware-Mängel/-Defekte	10	0,24	7	0,38	8	0,36	4	25%
unbeabsichtigte Fehler von Externen	8	0,30	8	0,37	10	0,35	6	13%
Sabotage (inkl. DoS)	6	0,49	9	0,35	6	0,47	8	8%
Manipulation zum Zweck der Bereicherung	9	0,28	10	0,34	9	0,35	9	8%
höhere Gewalt (Feuer, Wasser, ...)	11	0,09	11	0,16	11	0,12	10	7%
Sonstiges	12	0,05	12	0,04	12	0,01	12	0%

Basis: 98 Antworten (Bedeutung), Ø 95 (Prognose), Ø 90 (Schäden), Ø 262 (Vorhersage 2016)

Tabelle 1: Bedeutung der verschiedenen Gefahrenbereiche

Somit landet die Malware im Schadensrang wieder auf Platz 2 hinter „Irrtum und Nachlässigkeit eigener Mitarbeiter".

Der zweitgrößte Rückgang im Vergleich zur vorigen Studie ist beim Hacking zu beobachten (–6 %-Pkt., –4 Ränge). Einen Zuwachs gab es in der aktuellen Stichprobe (+3 %-Pkt.) bei „Manipulation zum Zweck der Bereicherung" (+2 Ränge). Ansonsten entspricht die Rangfolge der Studie von 2016.

Vergleicht man Schadensränge mit der eingeräumten Priorität, zeigt sich das gewohnte Bild, dass „Unfälle" im Sinne von Mängeln und Defekten von Soft- und Hardware sowie unbeabsichtigten Fehlern von Externen weniger Beachtung finden als Angriffe, die letztlich zu weniger erheblichen Schäden in der Stichprobe geführt haben. Ebenfalls wie üblich sei hier aber auch darauf hingewiesen, dass naturgemäß eine erhöhte Aufmerksamkeit das Auftreten tatsächlicher Schäden durch Angriffe begrenzt haben könnte, sodass nicht automatisch eine Überbewertung zu unterstellen ist.

Der Anteil der Teilnehmer, deren Organisation mindestens einmal von erheblichen Schäden durch menschliches oder technisches Versagen betroffen war („Unfälle" in Tab. 2) ging erneut leicht zurück (55 %, 2016: 59 %, 2014: 73 %, 2008: 64 %). Die aufsummierte Priorität hat sich nunmehr wieder deutlich angeglichen, betont aber weiterhin die Angriffe, wie das auch in den früheren Jahren mit Malware-Dominanz der Fall war (2,82/2,98 vs. 2016: 2,59/3,21, 2014: 2,54/3,10, 2012: 3,11/2,63, 2010: 2,79/2,78, 2008: 2,68/2,94).

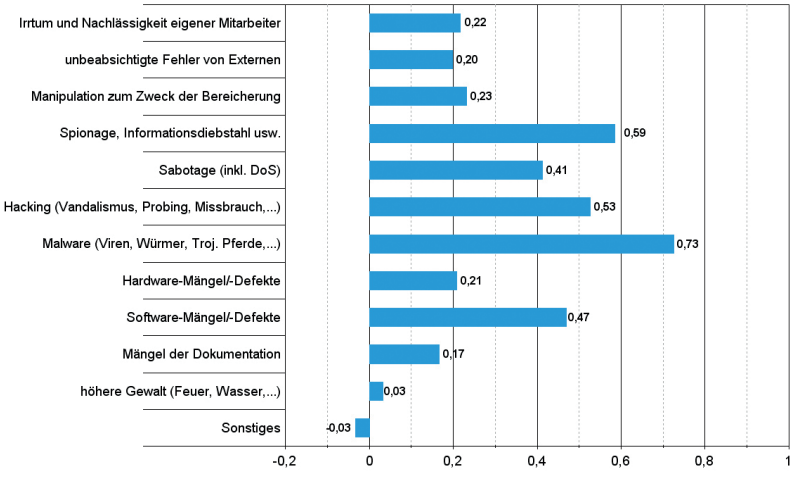
Prognosen damals und heute

Abgesehen von der Malware, die ihre Führung halten, wenn auch nicht ausbauen konnte, und den „unbeabsichtigten Fehlern von Externen", die tatsächlich einen Rang gutgemacht haben (sowie mit Ausnahme der ewigen letzten Plätze höhere Gewalt und Sonstiges), lagen alle Prognosen von 2016 (vgl. Tab. 1

	Priorität		Schäden	
	heute	Prognose	min. 1 bei	Nennungen
Unfälle	**2,82**	**2,51**	**55%**	**108**
... Mensch	1,30	1,06	41%	44
... Technik	1,51	1,45	43%	64
Angriffe	**2,98**	**3,36**	**42%**	**55**
... durch Malware	1,19	1,18	32%	29
... direkt	1,79	2,18	23%	26

Basis: siehe Tab. 1

Tabelle 2: Zusammenfassung der Gefahrenbereiche



Basis: Ø 95 Antworten, 62 (Sonstiges)

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

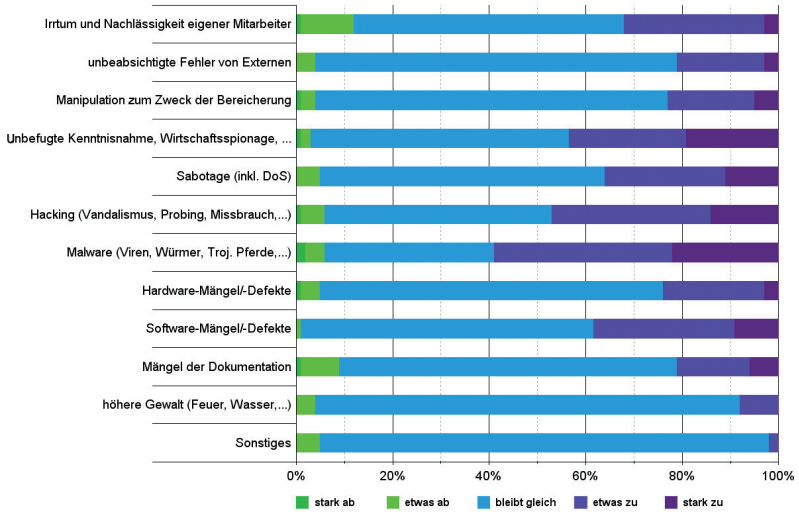


Abbildung 2: Prognostizierte Veränderung der Bedeutung der Gefahrenbereiche (Details)

Basis: Ø 95 Antworten, 62 (Sonstiges)

– „Vorhersage 2016“) bezogen auf die Priorisierung der aktuellen Stichprobe im vielfach beobachteten Sinne falsch: Alle „Unfälle“ wurden nun doch (wieder) höher priorisiert als vorhergesagt, alle „Angriffe“ niedriger. Besonders deutlich war das bei der Sabotage (–3 Ränge unter Prognose) und den Hardware-Mängeln und -Defekten (+3 Ränge) der Fall.

Die aktuell prognostizierten Veränderungen der Gefährdungen (Abb. 1) zeigen das bekannte Grundmuster einer erwarteten Verschärfung besonders von Angriffen – allem voran durch Malware sowie „unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage“ (kurz „Spionage“). Dabei bleiben sie zwar hinter den drastischen Befürchtungen der vorigen Studie zurück, aber dennoch pessimistischer als früher: So landet der Veränderungsindex für Malware noch immer bei +0,73 (2016: +1,02, 2014: +0,37, 2012: +0,56, 2010: +0,53) – der ebenfalls „klassische Angstwert“ zur Spionage liegt aktuell sehr hoch bei +0,59 (2016: +0,49, 2014: +0,28, 2012: +0,34, 2010: +0,46).

Eher ungewöhnlich sind der Peak bei der erwarteten Zunahme von Softwareproblemen (+0,47, 2016: +0,30, 2014: +0,15, 2012/2010: +0,20) sowie das geringe Vertrauen in die zukünftige Fehlersicherheit von Hardware (+0,21, 2016: +0,03, 2014: +0,13, 2012/2010: +0,02).

Der Veränderungs-Index berechnet sich aus den Einzelangaben zu einer erwarteten „sehr starken“ (+/–2) oder starken (+/–1) Zu- beziehungsweise Abnahme (vgl. Abb. 2). Positive Prognosen waren dabei dieses Mal besonders selten und am ehesten noch bei „Irrtum und Nachlässigkeit eigener Mitarbeiter“ zu sehen, wo 12 % ein mehr oder weniger starkes Nachlassen der Bedeutung dieser Gefährdung erwarten. Auch bei den heuer hoch priorisierten Dokumentationsmängeln haben immerhin noch 9 % einen Rückgang prognostiziert.

Kosten und Aufwand von Vorfällen

Die Schätzungen zur Häufigkeit verschiedener Sicherheitsvorfälle oder Fehlalarme sowie zu den damit verbundenen Kosten und Ausfallzeiten variieren regelmäßig sehr stark. In allen Kategorien gibt es mehr oder minder viele „Null“-Schätzungen und die Maximalwerte schnellen teils in enorme Höhen (vgl. Tab. 3). Daher geben wir in dieser Auswertung seit einiger Zeit für die Fallzahlen eine Alternativrechnung an, die sowohl die „Optimisten“ (Nullwerte) als auch die „Pessimisten“ (2–3 schlimmste Einzelangaben) außer Acht lässt. Um angesichts der geringen Teilnehmerzahl dieses Jahres einen Durchschnitt zu erhalten, der weniger durch die Ausreißer beeinflusst wird, wurden bei der Berechnung der mittleren Kosten in Tabelle 3 ebenfalls Null- und Maximalwerte ausgelassen.

Als „bereinigte alternative“ Fallzahlschätzungen ergab die aktuelle Erhebung ein mittleres jährliches Auftreten von 62 Virus-/Wurm-/Trojaner-Infektionen (2016: 59, 2014: 41, 2012: 16, 2010: 40, 2008: 70), 53 Malware-Fehlalarmen (2016: 50, 2014: 22, 2012: 20, 2010: 24, 2008: 40), 22 unbegründeten Warnungen (Hoaxes – 2016: 19, 2014: 14, 2012: 9, 2010: 20, 2008: 20) sowie 19 gezielten Angriffen (2016: 17, 2014: 10, 2012: 13, 2010: 4, 2008: 3).

Tabelle 3: Geschätzter Aufwand durch Sicherheitsvorfälle

	Häufigkeit		Ausfallzeit		Kosten	
	Durchschnitt	max. Wert	Durchschnitt	max. Wert	Durchschnitt*	max. Wert
Virus-/Wurm-Infektion	238 p.a.	13.000 p.a.	96 Std.	4.000 Std.	9.496 €	1.000.000 €
Malware-Fehlalarm	183 p.a.	10.000 p.a.	18 Std.	1.000 Std.	679 €	20.000 €
unbegründete Warnung (Hoax)	81 p.a.	5.000 p.a.	5 Std.	100 Std.	379 €	125.000 €
gezielter Angriff auf / über / mit IT	75 p.a.	5.000 p.a.	163 Std.	10.000 Std.	44.600 €	10.000.000 €

Basis: Ø 82 Antworten (Häufigkeit), Ø 74 (Ausfallzeit), Ø 66 (Kosten)

* unter Auslassung von Null- und Maximalwerten

Bei dieser Frage zeigen sich zudem natürlich deutliche Unterschiede zwischen KMU und großen Unternehmen. Rechnet ein KMU etwa für einen Malware-Angriff im Mittel mit 728 € direkten Kosten, so schlägt dieser bei den „Großen" mit durchschnittlich knapp 14 Tsd. € zu Buche (bei Auslassung eines Ausreißerwerts). Die Kosten eines Fehlalarms schätzten die KMU der Stichprobe auf durchschnittlich 154 € (Große 1376 €), für einen Hoax kamen sie auf 140 € (Große ca. 5 Tsd. €). Und für einen gezielten Angriff rechneten die KMU im Mittel mit Kosten von 415 € (bei Auslassung eines Ausreißerwerts), die großen Organisationen mit knapp 30 Tsd. €.

Größtes Schadensereignis

Über das größte Schadensereignis der vorausgegangenen zwei Jahre haben 73 Teilnehmer berichtet – 9 davon gaben explizit an, dass es keinen oder keinen nennenswerten Vorfall gegeben habe. Der Löwenanteil der schlimmsten Vorkommnisse ging erneut auf Malware zurück (42 % – nachträglich aus Freitextangaben kategorisiert). Auch dieses Jahr folgen verschiedene Attacken auf Platz zwei (19 %).

13 % gingen auf defekte oder ausgefallene Hardware zurück, 6 % wurden durch Softwareprobleme verursacht. Bei 5 % der größten Schäden lag die Ursache in der Infrastruktur beziehungsweise deren Ausfall begründet. Einbruch/Diebstahl sowie menschliche Irrtümer waren für jeweils 2 % verantwortlich. Ein knappes Zehntel (9 %) entfiel auf sonstige beziehungsweise nicht kategorisierbare Ursachen.

Die mit dem jeweils schlimmsten Ereignis verbundenen direkten Kosten lagen durchschnittlich bei rund 45 Tsd. € (KMU unter 6 Tsd. € / Große 80 Tsd. €) – die Ausfallzeiten über alle betroffenen Systeme summierten sich im Mittel auf etwa 25 Std. (15 Std. / 36 Std.).

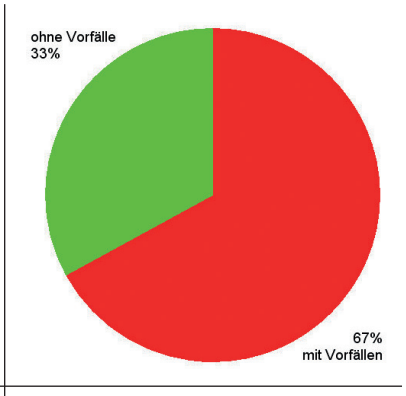


Abbildung 3: Organisationen mit Malware-Vorfällen
Basis: 97 Antworten

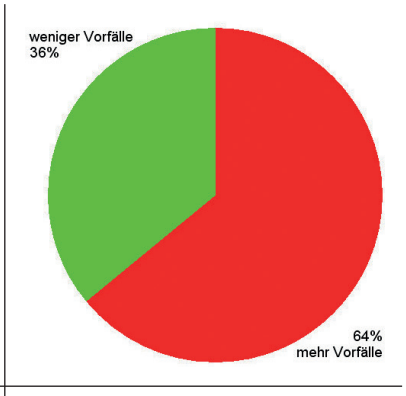


Abbildung 4: Tendenz der Malwarevorfälle (2017 ggü. 2016)
Basis: 69 Antworten

Die Medianwerte lagen deutlich darunter bei 8 Stunden Ausfallzeit (sowohl KMU als auch Große – 2016: dito) und 3000 € direkten Kosten (1200 € / 10.000 € – 2016: 2000 € – 1000 € / 10.000 €)

Die gezogenen Konsequenzen aus den „schlimmsten Ereignissen" zeigt Tabelle 4. Hier zeigt sich überwiegend die gewohnte Reihenfolge, wobei die aktuelle Stichprobe deutlich häufiger neue Sicherheitsmechanismen eingerichtet hat (+7 %-Pkt.) als das Teilnehmerfeld von 2016, wodurch dieser Punkt auf den zweiten Rang vorrückt.

Malware

Die aktuelle Stichprobe litt über das gesamte Teilnehmerfeld betrachtet etwas seltener unter Vorfällen mit (Abb. 3) und nennenswerten Schäden durch Malware als die Teilnehmer der Studie von 2016 – aufgrund der kleineren Teilnehmerzahl und weiterer Parameter (s. u.) sollte man hieraus jedoch keinesfalls schon eine Entwarnung ableiten.

Von den aktuell antwortenden Organisationen hatten allerdings insgesamt „nur" noch zwei Drittel von Malwarevorfällen im Jahr 2017 berichtet (67 %, Studie 2016: 75 %, 2014: 74 %, 2012: 63 %, 2010: 65 %). Wie üblich (und naheliegenderweise), traf es die Großen häufiger, wobei in dieser Teilmenge der Wert im Vergleich zur vorigen Erhebung sogar wieder stieg (90 %, 2016: 83 %, 2014: 89 , 2012: 77 %, 2010: 71 %) – bei den jetzt befragten KMU waren indessen nur noch 43 % generell von Malwarevorfällen betroffen (2016: 67 %, 2014: 58 %, 2012: 53 %, 2010: 58 %).

Konsequenterweise berichtete denn auch die Mehrheit dieser KMU von einer abnehmenden Tendenz der Vorfälle: Nur 38 % der (wie angemerkt, allerdings recht kleinen) Teilmenge haben 2017 *mehr* Vorfälle mit Malware registriert als im Jahr zuvor. Anders sah das bei den „Großen" aus, wo 82 % von einer weiteren Verschärfung der Lage sprachen. Über das gesamte Feld der mit Malwarevorfällen konfrontierten Teilnehmer zeigt sich daher noch immer eine überwiegende Zunahme der Vorfälle (Abb. 4), was ja auch mit den Fallzahlschätzungen (s. o.) der Studienteilnehmer korrespondiert.

Bei der Frage nach mindestens einem mittleren bis größeren Schaden durch Malware in den

Konsequenzen	*ja, bei*
bestehende Mechanismen verstärkt	80%
Sicherheitsmechanismen neu eingerichtet	71%
Angriffspunkte beseitigt	66%
organisatorische Konsequenzen gezogen	60%
Produkt-/Anbieterwechsel vollzogen	18%

Basis: Ø 54 Antworten, 14 (Produkt-/Anbieterwechsel), Mehrfachnennungen möglich

Tabelle 4: Konsequenzen aus „größten Schadensereignissen"

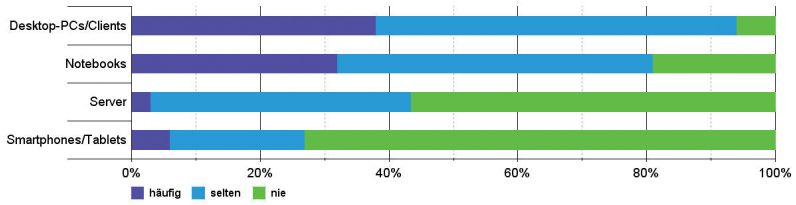


Abbildung 5: Betroffene Systeme in Organisationen mit Malware-Vorfällen

Basis: Ø 60 Antworten

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

Infektionswege	häufig	selten	nie	*Bedeutung**
E-Mail	53%	42%	5%	2,02
WWW-Seite (aktive Inhalte)	25%	59%	16%	1,35
unerwünschte Anwendungen	22%	51%	28%	1,16
Internet (Würmer)	19%	40%	41%	0,96
Speichermedien	12%	37%	51%	0,74
mobile Endgeräte	10%	38%	52%	0,67
unbekannte Herkunft **	1%	29%	22%	0,33
internes Netz / Intranet (Würmer)	2%	23%	74%	0,30

Tabelle 5: Infektionswege von Malware

Basis: Ø 82 Antworten, 43 (unbekannte Herkunft, prozentuiert auf das Mittel der anderen Antworten)**

vorausgegangenen zwei Jahren differierten die Angaben ebenfalls deutlich: Während 50 % der großen Organisationen hier mit Ja antworteten, waren es bei den KMU dieses Mal nur 18 % (32 % im Mittel aller Teilnehmer).

Der Faktor „Mensch“ spielt bei alldem weiterhin eine wesentliche Rolle: Fast vier Fünftel der Befragten gaben an, dass ein nennenswerter Teil der beobachteten Vorfälle durch abweichendes Nutzerverhalten hätte vermieden werden können (79 %, 2016: 85 %, 2014: 69 %, 2012: 67 %).

Die Verteilung der von Malware-Infektionen befallenen Systeme bei betroffenen Organisationen zeigt ebenfalls keine großen Veränderungen (Abb. 5). In der aktuellen Erhebung waren Server etwas seltener „häufig“ betroffen (–2 %-Pkt.), Desktop-PCs/Clients (+6 %-Pkt.) und Notebooks (+4 %-Pkt.) etwas öfter – an der generellen Bedeutung für Malwareinfektionen änderte das jedoch kaum etwas.

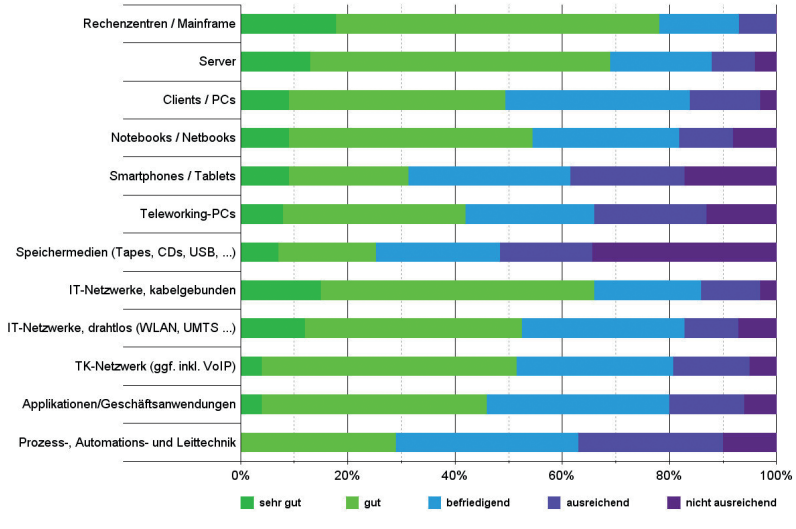


Abbildung 6: Einschätzung der Sicherheit im eigenen Hause

Basis: Ø 94 Antworten, 62 (Teleworking-PCs), 41 (Industrial-IT)

Bei den Einfallstoren für digitale Schädlinge (Tab. 5) konnte die E-Mail ihren fragwürdigen Spitzenplatz auf hohem Niveau noch etwas ausbauen: Erneut gab mehr als die Hälfte der Befragten als „häufigen“ Infektionsweg für Malware-Vorfälle E-Mails an (53 %, +1 %-Pkt.), infektionsfrei blieb dieser Kanal nur noch bei 5 % der Befragten (–2 %-Pkt.). Obwohl einige „Nicht-Internet“-Quellen bei den Teilnehmern bis zu 5 Prozentpunkte weniger „häufig“ für Probleme gesorgt haben, bleibt die generelle Rangfolge unverändert.

Sicherheitslage

Die aktuelle Stichprobe wiederholt viele der selbstkritischen Einschätzungen zur Sicherheit verschiedener Infrastrukturkomponenten im eigenen Haus (vgl. Abb. 6). Um eine Drittelnote besser als 2016 schnitten dieses Mal jedoch die Notebooks ab, die nunmehr quasi gleichauf mit stationären Clients/PCs bei einer „Drei plus“ landen. Auch Smartphones/Tablets haben die jetzigen Studienteilnehmer deutlich besser bewertet als das in früheren Erhebungen der Fall war – mit einer knappen „Drei“ verlassen sie die Schlussposition.

Dennoch hat über ein Drittel der Teilnehmer hier Sicherheitsbedenken, die keine befriedigende Bewertung zulassen. Ähnliches gilt für Telearbeitsplätze sowie die Prozess-, Automations- und Leittechnik, die von dieser Stichprobe deutlich schlechter bewertet wurde als 2016 (–9 %-Pkt „sehr gut/gut“, +6 %-Pkt. „ausreichend/nicht ausreichend“ – allerdings haben nur wenige Teilnehmer hierzu Angaben gemacht).

Die „rote Laterne“ verbleibt bei den Speichermedien, deren Sicherheit erneut über die Hälfte der Teilnehmer in ihrem Hause als nicht oder gerade einmal ausreichend einschätzen – mit 34 % (+3 %-Pkt.) vergab sogar mehr als ein Drittel

unbefugter Zugriff durch	ja		nein		*sicher oder vermutlich ja*	
	sicher	vermutlich	vermutlich	sicher	*2018*	2016
Social-Engineering / Phishing / Unachtsamkeit	11%	21%	55%	13%	32%	30%
Missbrauch/Weitergabe durch Berechtigte	2%	22%	63%	13%	24%	20%
Verlust/Diebstahl von Speichermedien	8%	11%	53%	28%	19%	25%
Verlust/Diebstahl mobiler Systeme	5%	12%	46%	37%	17%	24%
Datenlecks/Probleme bei Partnern	0%	15%	69%	15%	15%	16%
Online-Angriff	8%	5%	58%	29%	13%	15%
Abgehörte Kommunikation	0%	13%	69%	18%	13%	15%
Einbruch in Gebäude	4%	2%	32%	62%	6%	10%

Basis: Ø 94 Antworten (2016: Ø 257)

Tabelle 6: Vertraulichkeitsbrüche

die schlechteste Note „nicht ausreichend".

Vertraulichkeitsbrüche

Vertraulichkeitsbrüche bleiben auch in der aktuellen Stichprobe ein Problem: 58 % der Teilnehmer *vermuten,* dass ihre Organisation in den vorausgegangenen zwei Jahren mindestens einmal von einem Vofall betroffen war, bei dem Unbefugte Zugriff auf schutzwürdige Daten erlangt haben (2016: 49 %, 2014/2012: 53 %, 2010: 54 %, 2008: 53 %). Wie in der vorigen Studie gab rund ein Fünftel an, *sicher* von mindestens einem solchen Vorfall in diesem Zeitraum zu wissen (20 %, 2016: 21 %, 2014: 27 %, 2012: 32 %, 2010: 30 %, 2008: 26 %).

Bei den vermutlichen oder ermittelten Ursachen von Datenlecks (Tab. 6) stehen Social-Engineering, Phishing und Unachtsamkeit erneut an erster Stelle (+2 %-Pkt.). Missbrauch und Weitergabe durch Berechtigte haben die Befragten dieses Mal etwas häufiger beobachtet (+4 %-Pkt.). Die größten Rückgänge im Vergleich zur Erhebung von 2016 waren bei Verlust und Diebstahl von mobilen Systemen (–7 %-Pkt.) und Speichermedien (–6 %-Pkt.) zu verzeichnen. Datenlecks und Probleme bei Partnern blieben auf dem gesunkenen Niveau der vorigen Studie.

Erstmals haben wir im Umfeld von Vertraulichkeitsbrüchen gefragt, ob Betroffene oder Aufsichtsbehörden unterrichtet worden sind, was bei 19 % beziehungsweise 13 % der Befragten der Fall war, oder Vorfälle öffentliche Aufmerksamkeit erregt hatten (ja, bei 11 %). Die Antworten zu diesen und weiteren Konsequenzen von Vertraulichkeitsbrüchen sind in Tabelle 7 aufgeführt.

Mitschuld von Mitarbeitern

Seit unserer Studie von 2014 fragen wir, ob die Teilnehmer bei den Mitarbeitern ihres Hauses eine Mitverantwortung für die Mehrzahl der Datenlecks sehen. Auch in diesem Jahr bejahten das rund vier Fünftel (82 %, 2016: 79 %, 2014: 79 %). Die vermuteten Gründe dafür zeigen die bekannte Reihung: Allem voran seien den Mitarbeitern die Konsequenzen ihres Handelns nicht bewusst (87 %, 2016: 90 %, 2014: 91 %) – 71 % der Teilnehmer sahen ein mangelndes Verständnis der Systeme als ursächlich an, weil Datenschutz- und Sicherheitslösungen schlicht zu kompliziert sind (2016: 78 %, 2014: 73 %). Gut die Hälfte unterstellt zudem eine Unkenntnis von Firmen-Policies (52 %, 2016: 49 %, 2014: 53 %) – der vermutete Vorsatz, dem eigenen Unternehmen schaden zu wollen, landet mit gewohnt großem Abstand auf dem letzten Platz (8 %, 2016: 11 %, 2014: 14 %)

Bezüglich einer beruflichen Nutzung von Filesharing-Diensten, die auf den privaten Gebrauch zugeschnitten sind, zeigen sich kaum Veränderungen zu den vorigen Studien: 10 % der Befragten gaben an, dass dies im eigenen Hause „häufig" geschehe, 44 % votierten für „selten" und 47 % sagten „nie" (2016: 47 %, 2014: 50 %). Wie vor zwei Jahren ist bei 72 % der Befragten eine solche Nutzung verboten. Dabei scheinen diese Verbote in der aktuellen Stichprobe besser zu wirken als bei den damaligen Studienteilnehmern: Während 2016 auch dort, wo ein Verbot in Kraft war, noch 7 % der Teilnehmer von einer „häufigen" Nutzung ausgingen, waren das dieses Mal nur noch etwa 2 %.

Zum ersten Mal haben wir darüber hinaus gefragt, ob für derart fragwürdige Nutzungen von „Consumer-Clouds" eine spezielle Sicherheitslösung im Einsatz ist – 44 % sagten „ja", weitere 23 % gaben an, dass das in Planung sei.

Konsequenzen	*ja, bei*
technische/organisatorische Maßnahmen	52%
Imageschaden	29%
personelle Maßnahmen	27%
Strafanzeige gegen Verursacher	27%
missbräuchliche Verwendung durch Dritte	21%
Benachrichtigung von Betroffenen	19%
verlorene Kunden/Aufträge	13%
Benachrichtigung von Aufsichtsbehörde(n)	13%
öffentliche Aufmerksamkeit/ Berichterstattung	11%
externe Sanktionen gegenüber eigenem Haus/Mitarbeiter	5%
Sonstige	11%
keinerlei Konsequenzen	*21%*

Basis: 62 Antworten – Mehrfachnennungen möglich

Tabelle 7: Konsequenzen aus Vertraulichkeitsbrüchen

Gibt es im Unternehmen... ?	ja	bei Unternehmen mit ISi-Strategie	bei Unternehmen ohne ISi-Strategie
schriftliche Strategie zur Informations-Verarbeitung (IT-Betrieb)	67%	86%	15%
schriftliche Strategie zur Informations-Sicherheit	73%	100%	0%
spezifische Konzepte/Richtlinien			
... zur Handhabung sensitiver/kritischer Daten	78%	89%	48%
... zur Weitergabe/Bereitstellung von Daten an berechtigte Dritte	73%	86%	40%
... zur Nutzung von Cloud-/Web-Services (inkl. SOA, SaaS, ...)	60%	76%	15%
... zur E-Mail-Nutzung	89%	100%	60%
... zur Nutzung von Web 2.0, Social Networks, ...	49%	58%	27%
... zur Gestaltung/Nutzung von Passwörtern	82%	92%	58%
... zur Abwehr von Advanced Persistent Threats (APTs)	20%	25%	4%
... für das Incident-Management	59%	76%	12%
... zum Softwareeinsatz auf PCs	77%	93%	35%
... zum Einsatz von Verschlüsselung / elektronischen Signaturen	58%	73%	15%
... zur Nutzung mobiler Endgeräte	77%	89%	46%
... zur Nutzung mobiler Speicher und Plug&Play-Peripherie	63%	79%	19%
... für Telearbeit/Home-Office	65%	79%	24%
... zur dienstlichen Nutzung privater IT-Systeme	74%	82%	54%
... Sonstige	7%	9%	4%
Die (fortdauernde) Eignung von Konzepten/Richtlinien wird geprüft	86%	94%	60%
schriftlich formulierte ISi-Maßnahmen	62%	88%	5%
Die Einhaltung vorgesehener Maßnahmen wird geprüft	91%	96%	82%
Übereinstimmung von Praxis und Konzepten/Richtlinien			
... organisatorisch [Schulnote]	3,14	3,06	3,38
... technisch [Schulnote]	2,65	2,54	2,91

Tabelle 8: Strategien, Richtlinien und Konzepte

Basis: Ø 94 Antworten, 71 (schriftl. Maßnahmen)

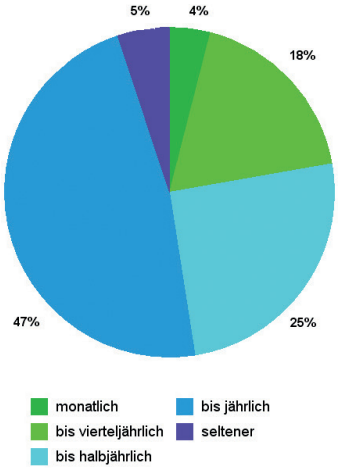


Abbildung 7: Häufigkeitsintervalle von Eignungsprüfungen für Konzepte und Maßnahmen (nachträglich klassifiziert)

Basis: 55 Antworten

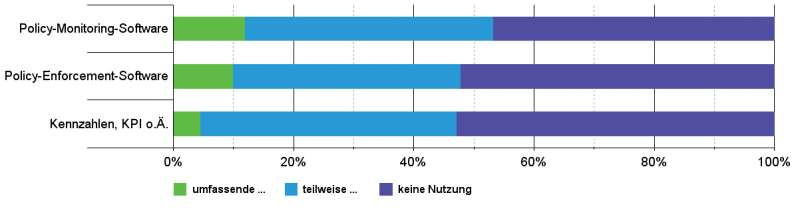


Abbildung 8: Einsatz von Hilfsmitteln zum Richtlinien-Management

Basis: Ø 90 Antworten

Konzepte / Policies

Bei den Fragen nach schriftlich fixierten Strategien und Maßnahmen liegt die aktuelle Stichprobe ziemlich genau im Mittel der vorausgegangenen Dekade (Studien 2008–2016). Tabelle 8 fasst die Antworten der Teilnehmer zu solchen Vorgaben zusammen. Wie üblich haben wir dabei alternativ auch wieder die Antworten der Befragten mit und ohne ISi-Strategie separat aufgeführt. Da die zweite Gruppe dieses Mal jedoch nur 26 Befragte umfasst, sind in diesem Punkt keine sinnvollen Längsschnittvergleiche mit früheren Studien möglich, da die Angaben einzelner Teilnehmer zu starke Auswirkungen auf die Ergebnisse haben.

Vergleicht man indessen die Antworten der gesamten Stichprobe mit den vorausgegangenen Studien, so zeigen sich klare Zuwächse bei Konzepten und Richtlinien zur Nutzung von Cloud- und Web-Services (60 %, 2016: 50 %, 2014: 41 %, 2012: 26 %, 2010: 14 %) sowie der Nutzung mobiler Endgeräte (77 %, 2016: 68 %, 2014: 71 %, 2012: 63 %, 2010: 69 %). In Sachen Verschlüsselung und Signatur knüpfen die jetzigen Teilnehmer wieder an die Ergebnisse früherer Stichproben an (58 %, 2016: 49 %, 2014: 57 %, 2012: 58 %, 2010: 51 %), wo bei der deutlich höheren Teilnehmerzahl von 2016 ein gewisser Einbruch zu erkennen war.

Neu aufgenommen haben wir in dieser Studie Fragen nach spezifischen Konzepten beziehungsweise Richtlinien für das Incident-Management, die es bei 59 % der Befragten gibt, sowie für Telearbeit und Home-Office, die fast zwei Drittel der teilnehmenden Organisationen besitzen (65 %). Die 2016 ergänzte Frage nach Konzepten gegen Advanced Persistent Threats (APTs) zeigt mit einem Zuwachs von +2 Prozentpunkten keine nennenswerte Veränderung – dieser Punkt bleibt offenbar weiterhin klares Schlusslicht der Sicherheitsplanung.

Prüfungen

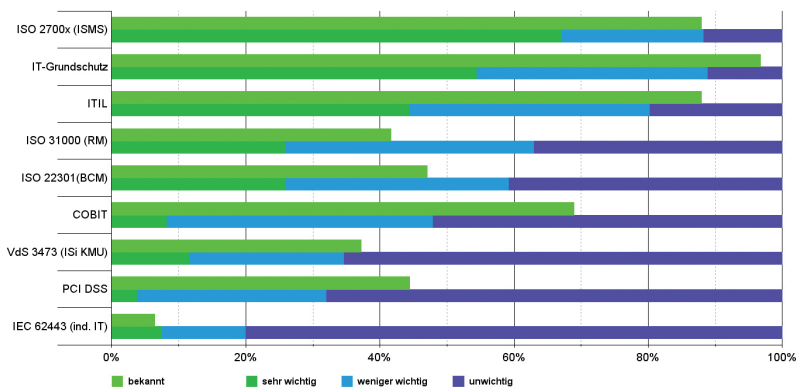
Die Bereitschaft zur Prüfung der fortdauernden Eignung von Konzepten und Richtlinien liegt mit 86 % innerhalb der Angaben vorausgegangener Studien, die von 2010 bis 2016 zwischen 84 % und 91 % schwankten (Ø 88 %) – die Prüfung vorgesehener Maßnahmen auf Einhaltung ist in der aktuellen Stichprobe mit 91 % etwas häufiger

als in den vorigen Erhebungen (80–88 %, Ø 85 %). Die Einschätzung der Übereinstimmung von Theorie und Praxis zeigt organisatorisch mit einer knappen Drei und technisch mit einer „Drei plus“ ein gewohntes Bild.

Die Prüfung der *Eignung* von Policies erfolgt bei gleich vielen Befragten regelmäßig (43 %, –2 %-Pkt. ggü. 2016/2014) beziehungsweise anlassbezogen (43 %, 2016: 39 %, 2014: 46 %). Die dabei eingesetzten Methoden sind weiterhin vor allem erneute Risiko- (81 %) oder Schwachstellenanalysen (69 %) – 54 % setzen dabei Penetrationstests ein, 42 % Übungen (etwa zu Notfallplänen oder Wiederanlauf). Simulationen und Szenarien bleiben weiter die Ausnahme (15 %).

Im Mittel erfolgten derartige Prüfungen bei den Befragten etwa alle neun Monate – Abbildung 7 zeigt die Verteilung anhand einer nachträglich vorgenommenen Staffelung. Wie üblich haben solche Prüfungen in sehr vielen Fällen zur Aufdeckung von Schwachstellen geführt (75 %, 2016: 68 %, 2014: 77 %, 64 %, 2012: 68 %). Ebenfalls üblich ist, dass längst nicht alle Teilnehmer dabei alle geschäftskritischen Systeme einbeziehen (34 %, 2016: 41 %, 2014: 38 %, 2012: 38 %, 2010: 39 %).

Die Prüfung der *Einhaltung* von Richtlinien und Maßnahmen erfolgt weiterhin überwiegend anlassbezogen (55 %). Zuständig waren für eine derartige Überwachung vor allem die IT- (59 %) und ISi-Abteilungen (51 %) sowie Datenschützer (40 %) und interne Revision (35 %). Externe Berater und Wirtschaftsprüfer oder die jeweils zuständige Fachabteilung waren jeweils bei etwa einem Viertel der Teilnehmer hieran beteiligt – bei 14 % war dabei die Geschäftsführung aktiv (Mehrfachantworten).



Basis: Ø 86 Antworten (Bekanntheit), Ø 65 (Relevanz)

Abbildung 9: Bekanntheit und praktische Bedeutung von ISi-Kriterienwerken (sortiert nach Bedeutung)

Technisch-organisatorische Hilfsmittel sind beim Richtlinien-Management auch heute nur bei grob der Hälfte der Studienteilnehmer im Einsatz – die umfassende oder teilweise Nutzung von Policy-Monitoring- und -Enforcement-Software sowie Kennzahlen zeigt Abbildung 8.

Risikobewertung

Bei einem Viertel der Teilnehmer wurden *alle* Anwendungen und Systeme hinsichtlich ihrer Bedeutung für Geschäftsprozesse und bestehender Risiken klassifiziert – bei 51 % war das zumindest für einzelne Systeme und/oder Anwendungen der Fall. Dabei haben 13 % kein strikt methodisches Vorgehen angewendet – in den anderen Organisationen lagen (wie üblich) standardisierte Verfahren an erster Stelle (67 %), gefolgt von eigenen Verfahren/Software (33 %), spezieller Risikomanagement-Software (11 %) sowie Verfahren von Herstellern oder Beratern (6 %) und sonstigen Methodiken (3 %).

Erneut war das Risikomanagement (RM) der IT bei rund der Hälfte der Teilnehmer (55 %) in ein allgemeines RM des (Gesamt-) Unternehmens eingebunden. Die angelegten Kriterien zur Klassifizierung von Risiken zeigt – ohne Überraschungen – Tabelle 9.

Standards

Die Bekanntheit und Bedeutung veschiedener Kriterienwerke zur Informations-Sicherheit fasst Abbildung 9 zusammen (sortiert nach Bedeutung). Die ISO-27000-Familie

Folgende Kriterien sind …	sehr wichtig	wichtig	unwichtig	*Vergleichszahl **
Verstöße gegen Gesetze / Vorschriften / Verträge	62%	36%	2%	1,60
Imageverlust	52%	40%	9%	1,43
Schaden bei Dritten / Haftungsansprüche	45%	45%	11%	1,34
direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	41%	45%	14%	1,27
Verzögerung von Arbeitsabläufen	22%	59%	19%	1,03
indirekte finanzielle Verluste	27%	37%	37%	0,90
Verlust oder Schaden von oder an Hardware u. Ä.	23%	43%	34%	0,89
Verstöße gegen interne Regelungen	12%	62%	26%	0,87

Basis: Ø 93 Antworten

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

Tabelle 9: Kriterien zur Risikobewertung

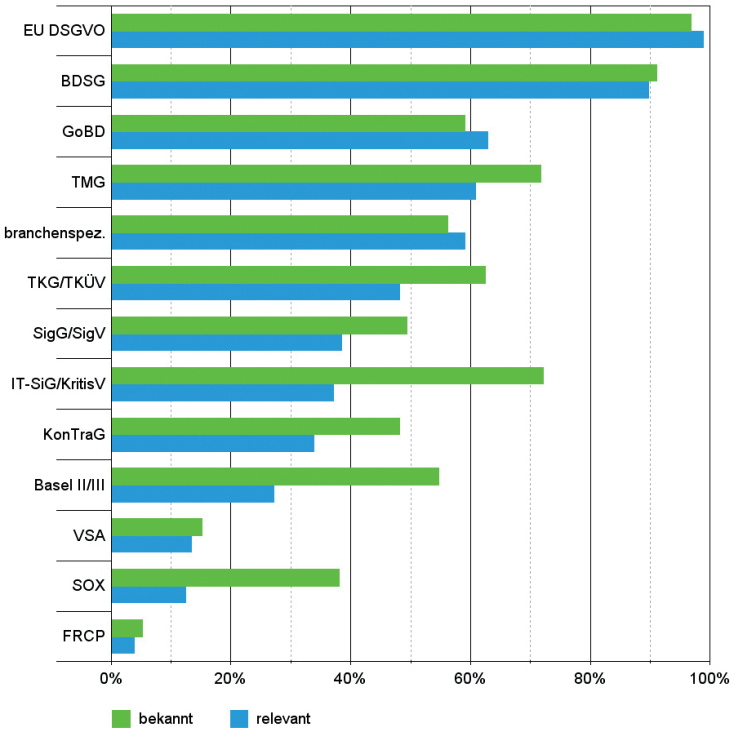


Abbildung 10: Bekanntheit und Relevanz von Gesetzen und Regularien (sortiert nach Relevanz)

Basis: Ø 84 Antworten (Bekanntheit), Ø 71 (Relevanz)

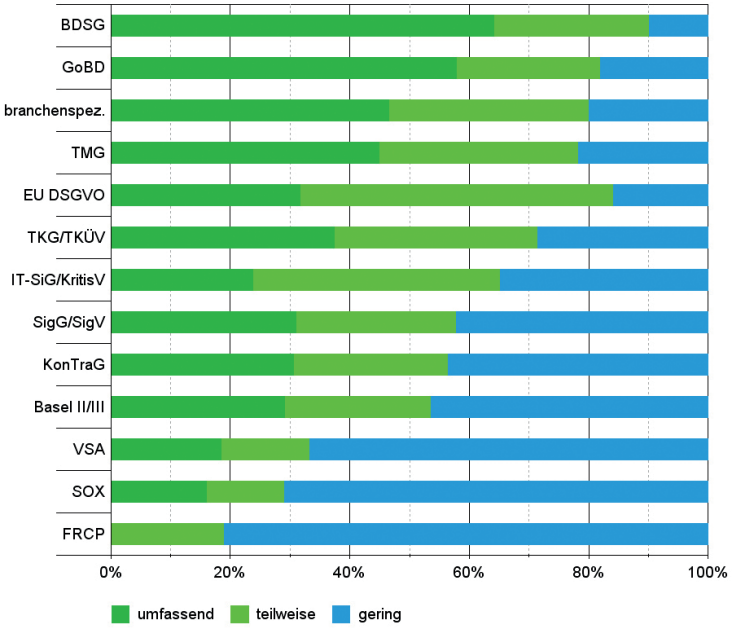


Abbildung 11: Umsetzungsgrad von Gesetzen und Regularien (sortiert nach Umsetzungsgrad: umfassend = 3, teilweise = 2, gering = 1)

Basis: Ø 48 Antworten

liegt dabei erneut an erster Stelle, dicht gefolgt vom IT-Grundschutz, der in Sachen Bekanntheit weiterhin führend bleibt. Darüber hinaus waren wieder nur COBIT und ITIL noch über der Hälfte der Befragten hinlänglich bekannt, wobei COBIT bereits für ebenfalls mehr als 50 % der Studienteilnehmer keine praktische Bedeutung besitzt.

Speziellere Normen und Frameworks zu Risikomanagement, Business-Continuity sowie für Zahlungsdienstleistungen und KMU erreichen in der aktuellen Stichprobe Bekanntheitsgrade zwischen 37 % und 47 %. Dabei sind die – erstmals erfragten und noch relativ neuen (Version 1.0 aus 2015) – Cybersecurity-Richtlinien des VdS für KMU (VdS 3473) zwar das Schlusslicht dieser Verfolgergruppe in Sachen Bekanntheit, landen in ihrer praktischen Bedeutung jedoch noch vor dem Data-Security-Standard der Payment-Card-Industry (PCI DSS). Auch bei den teilnehmenden KMU ist die VdS 3473 übrigens nur wenig bekannter (40 % vs. 37 % über das ges. Teilnehmerfeld) und bedeutender (61 % „unwichtig“ vs. 65 %) als im gesamten Teilnehmerfeld.

Auf dem letzten Platz rangiert dieses Mal die IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“, die naturgemäß nur für einen Teil der Befragten eine praktische Bedeutung besitzt. Mit 6 % Bekanntheitsgrad war sie allerdings in der Stichprobe dieser Studie auch deutlich seltener überhaupt jemals ein Thema als bei

Angemessenheit deutscher Gesetzgebung	überzogen	angemessen	unzureichend	Vergleichszahlen * 2018	2016	2014	2012	2010
TK-/Internet-Überwachung	33%	51%	16%	+ 0,17	+ 0,03	- 0,02	+ 0,20	+ 0,30
Datenschutz	19%	67%	13%	+ 0,06	- 0,07	- 0,06	- 0,08	- 0,06
Signaturgesetz	9%	70%	20%	- 0,11	- 0,15	+ 0,05	- 0,02	+ 0,01
E-Business (Verträge, Haftung, ...)	1%	64%	34%	- 0,33	- 0,24	- 0,22	- 0,29	- 0,16
Risikomanagement	3%	62%	35%	- 0,33	- 0,32	- 0,26	- 0,20	- 0,26
Kritische Infrastruktur	5%	57%	38%	- 0,33	- 0,30	–	–	–
Strafgesetze (bzgl. Computer-Kriminalität)	10%	43%	47%	- 0,36	- 0,49	- 0,39	- 0,23	- 0,23

Tabelle 10: Angemessenheit deutscher Gesetzgebung

Basis: Ø 81 Antworten (2016: Ø 231, 2014: Ø 115, 2012: Ø 119, 2010: Ø 125)

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

den Befragten von 2016, von denen immerhin 11 % diese Norm kannten.

Gesetze und Regularien

Von Null auf (nahezu) Hundert ist in Sachen Gesetze und Regularien mit Bezug auf Schutz- und Sicherheitsprobleme die Datenschutzgrundverordnung der EU (DSGVO) „eingeschlagen" – zumindest bezüglich Bekanntheitsgrad (97 %) und Relevanz (99 %) landete das neue Gesetz noch vor dem Bundesdatenschutzgesetz (BDSG) auf dem ersten Platz (Abb. 10). „Umfassend" hatten die Bestimmungen der DSGVO allerdings erst 32 % der teilnehmenden Organisationen umgesetzt – 52 % gaben an, dass dies „teilweise" erfolgt sei, 16 % sagten „gering" (Abb. 11). Ebenfalls 52 % der Befragten haben erwartet, dass die Prozesse und Systeme ihres Hauses bis zum Stichtag Ende Mai „compliant" zur DSGVO sein würden.

Im Übrigen entspricht der jeweilige Umsetzungsgrad recht gut der Relevanz der Regularien. Hoch im Kurs standen in der aktuellen Stichprobe die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD). Am unteren Ende landeten wie üblich die „Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen" (VSA) sowie der US-amerikanische Sarbanes-Oxley Act (SOX) und die US Federal Rules of Civil Procedure (FRCP), die auch Regeln zum sogenannten E-Discovery von Informationen umfassen (also Auskunftspflichten zu elektronisch gespeicherten Daten; vgl. <kes> 2009#4).

Die einschlägige deutsche Gesetzgebung wird erneut mit Ausnahme der Strafgesetze zur Computerkriminalität von jeweils mindestens der Hälfte der Befragten als angemessen beurteilt (Tab. 10). Größere Unzufriedenheit zeigt die aktuelle Stichprobe bezüglich der TK-/Internetüberwachung (+10 %-Pkt. „überzogen"). Und in Sachen Datenschutz (+9 %-Pkt. „überzogen") gibt es nunmehr ebenfalls wieder einmal einen kleinen Überhang der Kritiker einer Überregulierung – dennoch bleiben aber zwei Drittel der Befragten auch in den Zeiten der DSGVO beim Urteil, dass dies „angemessen" sei.

Mindestens ein Drittel nannte im Übrigen die Regulierung von E-Business, Risikomanagement und kritischer Infrastruktur noch „unzureichend" – bei den Strafgesetzen war das erneut fast die Hälfte (47 %).

Hindernisse

Auf Rang eins der schlimmsten Hindernisse für eine Verbesserung der Informations-Sicherheit (Tab. 11) steht erneut fehlendes Bewusstsein bei den Mitarbeitern – 71 % der Befragten haben das moniert, womit fast wieder der Negativrekord der vorigen Studie (72 %) erreicht wurde. Historisch schlecht ist sogar das Ergebnis des weiterhin auf Platz zwei folgenden Problems von zu wenig Bewusstsein und Unterstützung im Top-Management: 62 % der Teilnehmer haben das als drastische Behinderung angesehen – damit wird der vormalige Negativrekord von 1992 um ganze 5 %-Punkte überboten. Auch wenn angesichts der kleinen Stichprobe dieser Studie hier besondere Vorsicht vor Verallgemeinerungen angebracht ist, erscheinen diese Werte doch sehr bedenklich.

Gleiches gilt für den ungewohnt hohen Anteil der Klage über einen Mangel an kompetenten und verfügbaren Mitarbeitern, die heuer auf Rang drei landet. Fehlende finanzielle Mittel steigen ebenfalls

Bei der Verbesserung der ISi behindern am meisten (Mehrfachnennungen möglich)	2018	2016	2014	2012	2010	2008
Es fehlt an Bewusstsein bei den Mitarbeitern	71%	72%	68%	64%	59%	69%
Es fehlt an Bewusstsein und Unterstützung im Top-Managment	62%	55%	53%	56%	47%	55%
Es fehlen verfügbare und kompetente Mitarbeiter	59%	50%	45%	37%	41%	43%
Es fehlt an Geld/Budget	58%	52%	58%	49%	57%	43%
Es fehlt an Bewusstsein beim mittleren Management	52%	52%	52%	49%	54%	45%
Die Kontrolle auf Einhaltung ist unzureichend	48%	38%	35%	38%	38%	41%
Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	46%	35%	19%	27%	31%	36%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	41%	44%	43%	34%	35%	38%
Die vorhandenen Konzepte werden nicht umgesetzt	36%	27%	27%	25%	27%	27%
Anwendungen sind nicht für ISi-Maßnahmen vorbereitet	32%	31%	31%	26%	27%	27%
Die Komplexität heutiger IT-Landschaften ist nicht mehr beherrschbar	28%	25%	22%	—	—	—
Es fehlen geeignete Methoden und Werkzeuge	28%	23%	21%	17%	14%	16%
Es fehlen realisierbare (Teil-)Konzepte	24%	30%	21%	20%	21%	25%
Es fehlen geeignete Produkte	20%	19%	18%	16%	13%	16%
Es fehlt an praxisorientierten Sicherheitsberatern	18%	22%	13%	11%	16%	14%
Die Menge der verarbeiteten Daten ist nicht mehr beherrschbar	13%	12%	18%	—	—	—
Sonstiges	2%	3%	5%	2%	4%	3%
keine	2%	1%	1%	3%	2%	1%

Basis: 90 Antworten (2016: 262, 2014: 131, 2012: 133, 2010: 133)

Tabelle 11: Hindernisse für bessere Informations-Sicherheit

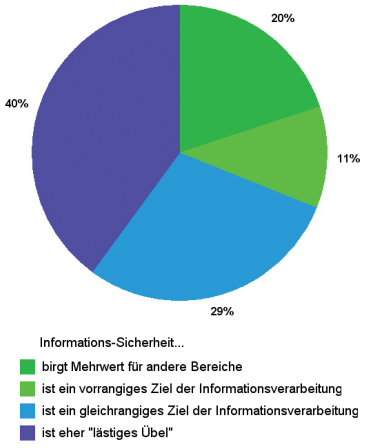


Abbildung 12: ISi-Stellenwert beim Top-Management

Basis: 90 Antworten

wieder in der Beachtung und platzieren sich vor dem Dauerbrenner fehlenden Bewusstseins im mittleren Management, der eine unveränderte Bewertung erfährt.

Dass die Teilnehmer der diesjährigen Studie mehr „schlimmste" Hindernisse angaben, kann zwar durchaus mit der konkreten Stichprobe zusammenhängen. Allerdings zeigte sich durchaus schon zuvor ein Trend dazu, an dieser Stelle mehr Kreuze zu machen: Während die Befragten der Studien von 2008, 2010 und 2012 im Mittel noch recht beständig 4,7–4,9 Kategorien gewählt hatten, lag dieser Wert 2014 schon bei 5,5 und stieg 2016 auf 5,9 (bei erheblich höherer Teilnehmerzahl) – nunmehr gab es durchschnittlich 6,4 Klagen pro Teilnehmer. Die weitere Entwicklung bleibt zu beobachten.

Uneinheitlich zeigen sich Veränderungen bei der Einschätzung zum ISi-Stellenwert im Top-Management: Zu den schlechten Bewertungen der Chefetage passt ein leicht gestiegener Anteil der Studienteilnehmer, die ihrem Top-Management unterstellen, in der ISi eher ein „lästiges Übel" zu sehen (40 %, +4 %-Pkt.). Auf der anderen Seite gibt es aber in der aktuellen Stichprobe auch einen höheren Anteil von Teilnehmern, deren Chefs in der Sicherheit einen Mehrwert oder ein vorrangiges Ziel der Informationsverarbeitung sehen (+4 %-Pkt.) – die veränderten Extremwerte gehen somit zulasten des „Mittelfelds", das eine Gleichrangigkeit von Informationsverarbeitung und -Sicherheit propagiert (Abb. 12).

Kenntnisstand und Weiterbildung

An den ISi-Kentnissen von Managern und Mitarbeitern lässt sich eine schlechtere Bewertung von Bewusstsein und Unterstützung scheinbar aber nicht festmachen. Jedenfalls haben die Studienteilnehmer in dieser Erhebung ihre Kollegen durchweg gleich gut oder etwas besser eingeschätzt als das in der vorigen Studie der Fall war (Abb. 13). Fachleute erhalten erneut eine gute Zwei, Anwender in hochsensitiven Bereichen eine „Drei plus". Die Top-Manager erreichen sogar haarscharf wieder eine knappe Drei, das mittlere Managament bleibt bei „Drei minus". Die „größte" Veränderung ist eine um zwei Zehntel bessere Einschätzung der Kenntnisse von Mitarbeitern in weniger sensitiven Bereichen, die in der aktuellen Stichprobe wieder – wie früher – bei „Drei bis Vier" landen.

Schulungen waren in der aktuellen Stichprobe allerdings bei internen Mitarbeitern auch wieder häufiger anzutreffen als in den beiden vorausgegangenen Studien – eine Ausnahme bildet die Gruppe der Revisoren und Prüfer, die erneut nur ein Viertel der teilnehmenden Organisationen regelmäßig oder häufig schult. Abbildung 14 zeigt eine genauere Verteilung der Schulungsfrequenzen.

Die in Tabelle 12 dargestellte Nutzung verschiedener Ausbildungsmethoden entspricht in etwa den zurückhaltenden Werten der vorigen Studie, wobei Online-Trainings-Anwendungen und Tools noch einmal seltener „häufig" eingesetzt wurden (–8 %-Pkt.). Interne Veranstaltungen nach klassischer Manier bleiben daher mit vergrößertem Abstand die meistgenutzte Option in den befragten Organisationen.

Die Einschätzung der Bedeutung beziehungsweise Aussagekraft von Berufszertifikaten bleibt ebenfalls in etwa gleich: Herstellerspezifische Zertifikate finden erneut etwa ein Viertel der Teilnehmer „unwichtig" (25 %, 2016: 24 %) und sogar nur noch 15 % „sehr wichtig" (2016: 20 %). Höher im Kurs stehen herstellerunabhängige Zertifikate, die 45 % „sehr wichtig" (2016: 43 %) und 14 % „unwichtig" finden (2016: 16 %). Die verbleibenden Anteile der Studienteilnehmer votierten jeweils für „weniger wichtig".

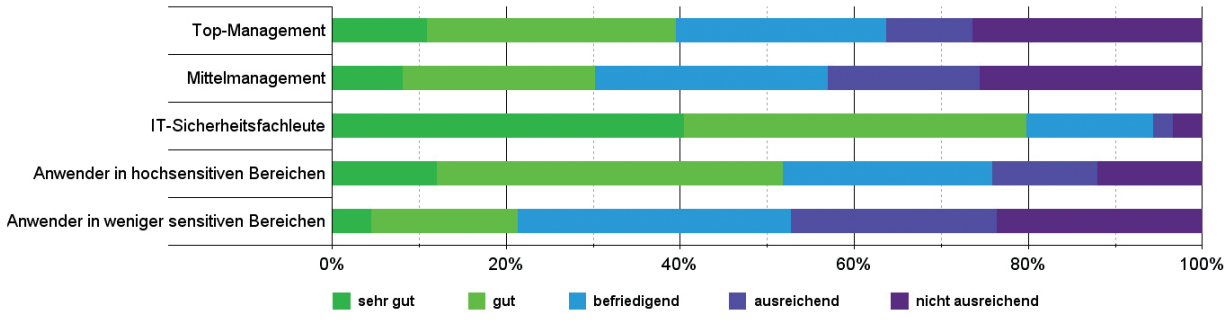


Abbildung 13: Kenntnisstand der Manager und Mitarbeiter

Basis: Ø 88 Antworten

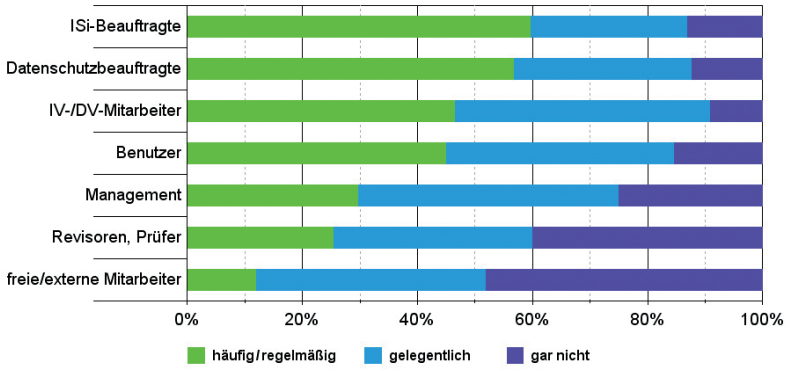
Awareness

Auch bei den Fragen zum Thema Awareness, die nun zum zweiten Mal Teil der Studie waren, zeigte sich in der aktuellen Stichprobe eine größere Bereitschaft für Trainings. Eine entsprechende Maßnahme hatten in den vorausgegangenen zwei Jahren 45 % der befragten Organisationen häufig oder regelmäßig durchgeführt (+14 %-Pkt.) – 36 % schulten gelegentlich oder zu speziellen Anlässen (2016: 34 %). Nur bei 19 % gab es hierzu im erfragten Zeitraum überhaupt keine Schulung (2016: 35 %).

Ausrichter solcher Schulungen waren weiterhin vor allem interne Kräfte (Mehrfachnennungen): bei 78 % Mitarbeiter der eigenen IT- oder ISi-Abteilung, bei 15 % auch Kollegen aus anderen Abteilungen. Externe waren bei gut einem Drittel im Einsatz (36 %) – spezielle Tools, Templates oder Anleitungen wurden bei 28 % genutzt.

Im Mittel liefert die höhere Bereitschaft, entsprechende Maßnahmen vorzusehen, zwar auch etwas bessere Ergebnisse beim Anteil der Belegschaft, den die Studienteilnehmer hinsichtlich Datenschutz und -sicherheit für ausreichend geschult ansehen: Der Durchschnitt lag nun bei 49 % (2016: 42 %), der Median aller Angaben bei 50 %, in den Teilgruppen der KMU bei 70 %, bei großen Organisationen ab 500 Mitarbeitern bei 20 % (2016: 30 %, KMU: 50 % / „Große“ 30 %).

Betrachtet man jedoch die gestaffelten Angaben des als „fit“ angesehenen Anteils der Kollegen, zeigt sich weiterhin eine starke Streuung (Abb. 15). Und auch dieses Mal hat fast die Hälfte der Teilnehmer keine allzu große Zuversicht bezüglich der Verbreitung von Wissen zu Datenschutz und Informations-Sicherheit: Denn auch dieses Mal schätzen 48 % weniger als die Hälfte der Mitarbeiter im eigenen Haus als ausreichend geschult ein (2016: 52 %).



Basis: Ø 79 Antworten

Abbildung 14: ISi-Schulungsfrequenz verschiedener Mitarbeitergruppen

	häufig	gelegentlich	nie	*Vergleichszahl**
interne Schulungen	40%	46%	14%	1,65
Online-Trainings-Anwendungen/-Tools	21%	49%	30%	1,11
Materialien (Unterlagen, CDs/DVDs) zum Selbstlernen	15%	51%	34%	0,95
externe Schulungen	10%	57%	33%	0,88

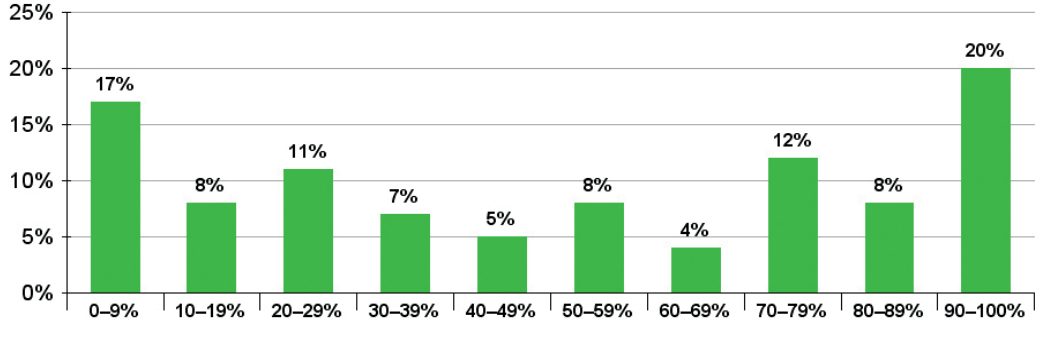
Basis: Ø 89 Antworten

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

Tabelle 12: Genutzte Ausbildungsmethoden

Maßnahmen

Die Antworten der Teilnehmer zu einer Reihe realisierter, geplanter beziehungsweise nicht vorgesehener Sicherheitsmaßnahmen auf Servern, Clients und mobilen Systemen zeigt Tabelle 13. Aufgrund der stark abweichenden Stichprobengröße sind Vergleiche dieser Ergebnisse mit der vorigen Studie heikel und kaum als Trend zu interpretieren – auch wenn die meisten Antworten nur geringe Schwankungen im üblichen Rahmen zeigen, könnten doch auch größere



Basis: 75 Antworten

Abbildung 15: Anteil der Belegschaft mit ausreichender Schulung hinsichtlich Datenschutz und -sicherheit

	Server / Zentrale			Clients / Endstellen			mobile Endgeräte		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
Firewalls	95%	2%	2%	78%	5%	17%	63%	7%	29%
Intrusion-Detection-/ Prevention-Systems (IDS/IPS)	56%	18%	26%	27%	8%	66%	17%	9%	73%
Netzwerkzugangskontrolle (EAP, NAC, NAP ...)	45%	18%	38%	46%	17%	37%	34%	16%	49%
Schnittstellenüberwachung/-schutz (USB, ser., par., Bluetooth, ...)	35%	8%	58%	42%	18%	40%	32%	22%	46%
Identity- und Access-Management (IAM)	51%	23%	27%	48%	20%	32%	36%	25%	39%
Authentifizierung									
... Hardware-Token	23%	5%	71%	22%	10%	68%	22%	5%	73%
... Passwort	98%	0%	2%	95%	0%	5%	93%	0%	7%
... Chipkarte / Smartcard	7%	9%	84%	9%	12%	79%	11%	9%	80%
... biometrische Verfahren	7%	4%	89%	8%	11%	81%	30%	9%	61%
... TLS-/SSL-/X.509-Zertifikate	51%	5%	44%	37%	17%	46%	33%	16%	51%
Application-Management (Schutz vor Installation/Nutzung unerw. App.)	51%	5%	44%	55%	12%	33%	45%	18%	38%
zentralisiertes Schwachstellen-Management (Vulnerability-Mgmt.)	37%	29%	34%	29%	22%	49%	19%	25%	57%
zentralisiertes System-/ Configuration-Management (CMDB)	58%	20%	22%	51%	17%	32%	47%	18%	35%
Patch-Management	85%	12%	4%	85%	9%	6%	65%	12%	22%
Virtualisierung	90%	2%	7%	40%	6%	54%	22%	1%	77%
Malware-/Spyware-Abwehr	93%	0%	7%	93%	2%	5%	75%	9%	16%
Spam-Abwehr	90%	0%	10%	89%	2%	9%	71%	3%	27%
Content Inspection/Filtering (Adress-/Inhaltsfilter eingehend)	76%	0%	24%	63%	8%	29%	47%	8%	45%
Data-Leakage/Loss-Prevention (DLP, Inhaltskontrolle abgehend)	20%	14%	66%	18%	21%	62%	15%	21%	64%
Digital-/Enterprise-Rights-Management (DRM/ERM)	15%	11%	74%	14%	13%	74%	11%	13%	76%
Public-Key-Infrastructure (PKI)	55%	10%	35%	43%	16%	41%	38%	15%	47%
Verschlüsselung									
... sensitive Daten	60%	11%	29%	61%	10%	29%	57%	12%	31%
... Festplatten/eingebaute Speicher ... (komplett/partitionsweise)	48%	13%	40%	60%	15%	26%	72%	10%	18%
... mobile Speichermedien (USB, SDcard, ...)	27%	10%	63%	37%	24%	38%	37%	21%	42%
... Archivdatenträger/Backups	54%	10%	35%	38%	11%	51%	28%	6%	66%
... LAN/Intranet-Verbindungen (VPN)	56%	6%	38%	51%	12%	37%	48%	8%	44%
... WLAN-Verbindungen (WPA/WPA2, VPN, ...)	76%	1%	23%	83%	4%	13%	86%	1%	13%
... WAN/Internet-Verbindungen (VPN)	81%	0%	19%	82%	1%	17%	73%	1%	26%
... mobile Verbindungen (VPN via UMTS/LTE, Hotspots, ...)	44%	2%	54%	58%	8%	35%	66%	8%	25%
... Telefon / Fax (Festnetz/GSM)	23%	2%	75%	23%	5%	72%	20%	3%	76%
... Voice over IP (VoIP)	34%	12%	54%	35%	15%	50%	30%	13%	57%
... E-Mail	52%	18%	30%	56%	22%	23%	55%	20%	25%
Datensicherung (Backup)	74%	5%	21%	44%	4%	51%	33%	3%	64%
Langzeit-Archivierung	56%	16%	28%	30%	5%	65%	15%	7%	78%
physische Sicherheit									
... Zutrittskontrolle, biometrisch	15%	8%	77%	9%	1%	90%	–	–	–
... Zutrittskontrolle, sonstige	93%	1%	6%	73%	0%	27%	–	–	–
... Bewachung	49%	4%	47%	33%	1%	66%	–	–	–
... Video-Überwachung	58%	2%	40%	23%	2%	75%	–	–	–
... Einbruchmeldesysteme	76%	4%	20%	49%	2%	48%	–	–	–
... Sicherheitstüren	84%	1%	14%	50%	0%	50%	–	–	–
... Brandmeldesysteme	90%	4%	6%	65%	1%	34%	–	–	–
... Löschanlagen	63%	4%	33%	26%	1%	73%	–	–	–
... andere Meldesysteme (Gas, Staub, Wasser, ...)	56%	3%	42%	13%	1%	86%	–	–	–
... Datensicherungsschränke/-räume	78%	5%	17%	26%	4%	70%	–	–	–
... Schutz gegen kompromittierende Abstrahlung (Tempest)	12%	3%	85%	3%	0%	97%	3%	2%	95%
... sonstige Maßnahmen gegen Hardware-Diebstahl	32%	9%	59%	28%	11%	61%	39%	12%	49%
physikalisches Löschen von Datenträgern	84%	2%	14%	69%	6%	25%	62%	7%	32%
unterbrechungsfreie Stromversorgung (USV)	94%	1%	5%	20%	1%	78%	15%	0%	85%
Überspannungsschutz für Stromleitungen	94%	0%	6%	33%	4%	63%	18%	2%	80%
Überspannungsschutz für Daten-/IT-Leitungen	76%	1%	23%	26%	4%	69%	13%	4%	82%
Reserve-Netzzugang (IT/TK) zur Ausfallüberbrückung	69%	4%	27%	35%	0%	65%	30%	13%	57%

Tabelle 13: Realisierte und geplante Sicherheitsmaßnahmen

Basis: Ø 78 Antworten (Server und Clients), Ø 73 (mob. Systeme)

Unterschiede in der Planung und Umsetzung einzelner Maßnahmen auf die konkrete Zusammensetzung der aktuellen Stichprobe zurückzuführen sein. Die deutlichsten Abweichungen sollen hier dennoch kurz aufgeführt werden.

So sind bei den Teilnehmern dieser Studie realisierte „sonstige Maßnahmen gegen Hardware-Diebstahl" bei Servern und zentraler IT deutlich seltener zu finden als in der Stichprobe von 2016 (–18 %-Pkt.) – im Bereich von Clients und mobilen Systemen hingegen fast gleich oft (–2 %-Pkt. / –1 %-Pkt.). In Sachen Überspannungsschutz sind zentrale Systeme und Server sogar minimal häufiger gesichert als 2016 (je +1 %-Pkt.) – bei den Endpunkten sind solche Maßnahmen in der aktuellen Erhebung jedoch deutlich seltener realisiert: –20 %-Punkte bei Strom-, –17 %-Punkte bezüglich Daten- und TK-Leitungen bei ortsfesten Clients, je –8 %-Punkte bei mobilen Systemen.

Die auffälligsten Zuwächse realisierter Maßnahmen zeigten sich bei der biometrischen Authentifizierung mobiler Systeme (+16 %-Pkt.) sowie der vollständigen oder partitionsweisen Verschlüsselung von Festplatten und eingebauten Speichern (+10/+14/+15 %-Pkt.).

Die am häufigsten *in Planung* befindliche Sicherheitsmaßnahme der aktuellen Stichprobe war ein zentralisiertes Schwachstellen-Management (Vulnerability-Mgmt.), das bei 29 % der Teilnehmer zentral (bzw. für Server), bei 22 % für Clients/Endstellen und bei 25 % für mobile Systeme implementiert werden soll – auch Identity- und Access-Management (IAM) hat offenbar noch viel Potenzial (bei 23/20/25 % „geplant").

Nachholbedarf sehen die Studienteilnehmer vor allem auf Endpunkten und mobilen Systemen bei der Verschlüsselung mobiler Speichermedien (10/24/21 % „geplant") sowie von E-Mails (18/22/20 % „geplant"). Auch Data-Leakage/Loss-Prevention (DLP) sowie zentralisiertes System-/Configuration-Management (CMDB) hat in bestimmten Bereichen noch mehr als jeder fünfte Befragte in Planung.

Am wenigsten gefragt sind – wenig überraschend – weiterhin Schutzmaßnahmen gegen kompromittierende Abstrahlung (Tempest, 85/97/95 % „nicht vorgesehen"), doch auch Chipkarten und Hardware-Token zur Authentifizierung, biometrische Verfahren, Sprachverschlüsselung für Telefonate und Digital-/Enterprise-Rights-Management (DRM/ERM) haben in vielen Organisationen keinen guten Stand.

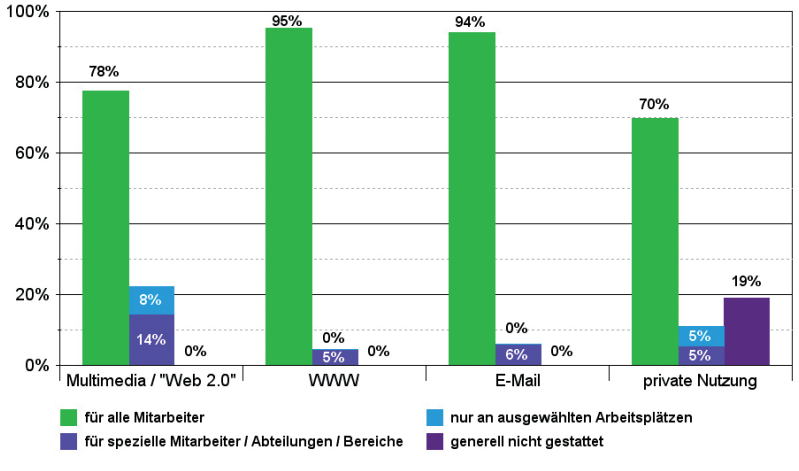
In Sachen „Backup" wiederholt diese Studie das erstaunliche Bild der vorigen Erhebung: Nur 77 % der Teilnehmer (2016: 76 %) gaben an, auf mindestens einer Ebene eine Datensicherung „realisiert" zu haben – bei 14 % hieß es sogar in allen drei Kategorien (Server/Clients/Mobilgeräte), Backupmechanismen seien „nicht vorgesehen" (2016: 13 %). An dieser Stelle kann man nur wiederholen, dass statt einer klassischen Datensicherung in diesen Organisationen hoffentlich andere Maßnahmen dafür sorgen, dass Daten bei Unfällen oder Angriffen nicht unwiederbringlich verloren gehen.

Vertraulichkeit und Netznutzung

Bei 83 % der Befragten erfolgt eine Klassifikation von Daten hinsichtlich ihrer Sensitivität (z. B. als geschäftskritisch, vertraulich, Verschlusssache usw.); 7 % konnten dabei auf automatisierte Verfahren zurückgreifen, bei 76 % erfolgt die Kategorisierung manuell. Räumliche Bereiche, die als besonders risikobehaftet oder gefährdet klassifiziert werden (z. B. aufgrund von Publikumsverkehr, als Produktionsumgebung usw.), existieren bei 62 % der Teilnehmer.

Wo eine Klassifizierung erfolgt, werden sensitive Daten oder Systeme bei 78 % gegenüber dem restlichen Haus in der einen oder anderen Form abgeschottet. Dabei kommen weiterhin vor allem allgemeine Sicherheitssysteme (z. B. Firewalls – bei 63 %) oder Netzwerkmechanismen (VLAN, NAC usw. – bei 51 %) zum Einsatz. Spezielle Systeme für eingestufte Daten nutzen 24 %; bei 31 % gibt es eine vollständige physische Trennung vom allgemeinen Hausnetz.

Für die Überwachung und das Berechtigungsmanagement privilegierter Accounts haben 55 % der befragten Organisationen einen Security-Prozess bereits realisiert



Basis: Ø 80 Antworten

Abbildung 16: Beschränkungen geschäftlicher und privater Internetnutzung

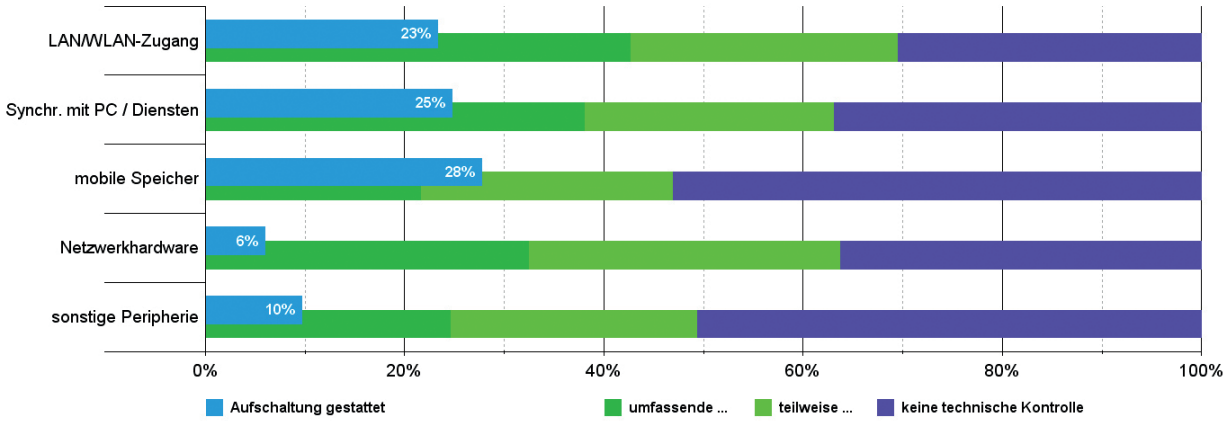


Abbildung 17: Zulässigkeit und Kontrolle privater Systeme

Basis: Ø 84 Antworten (Aufschaltung), Ø 82 (Kontrolle)

(+19 %-Pkt. ggü. der Stichprobe von 2016) – weitere 19 % planen, einen solchen zu implementieren, nur bei 26 % ist dies nicht vorgesehen (2016: 38 %).

Ohne Internetdienste geht immer weniger – das zeigt sich auch in den Antworten zu Beschränkungen der dienstlichen und privaten Nutzung am Arbeitsplatz: Ein generelles Verbot von Multimedia/„Web 2.0“, WWW und E-Mails gab es in dieser Studie überhaupt nicht mehr (2016: 9 %/1 %/1 %) und auch der Anteil der Organisationen, die entsprechende Zugriffe auf ausgewählte Arbeitsplätze (je –3 %-Pkt.) oder spezielle Mitarbeiter, Abteilungen oder Bereiche (–12/–5/–3 %-Pkt.) beschränken, fiel in der aktuellen Stichprobe deutlich geringer aus (Abb. 16).

Ein Berechtigungskonzept für aktive Inhalte (Javascript, ActiveX, Java, Flash usw.) im Web-Browser – etwa per IE-Zonenmodell oder URL-basierten Beschränkungen – nutzen 59 % der befragten Organisationen. Bei 73 % werden entsprechende Berechtigungen zentral gesteuert (z. B. per Gruppenrichtlinie).

Zum ersten Mal haben wir nach einer Einschätzung der Sicherheit interner Web-Anwendungen gefragt, wobei die Teilnehmer überwiegend gute Noten vergaben: Die Beschränkung der Erreichbarkeit auf das interne Netzwerk nannten 86 % „sehr gut“ oder „gut“, die Kompatibilität mit aktuellen Browsern 59 %, Verschlüsselung/Authentifizierung durch TLS-/SSL-Zertifikate 56 %, Pflege und Monitoring von Zugriffsrechten immerhin noch 50 %. Am „schlechtesten“ wurden regelmäßige Updates und Weiterentwicklung bewertet, wo 44 % „sehr gut“ oder „gut“ gaben und es im Mittel nur für eine „Drei plus“ reichte.

Hinsichtlich eines generellen Verbots privater Netznutzung landen die aktuellen Ergebnisse mit 19 % (Abb. 16) etwas unterhalb des Mittelwerts der vorausgegangenen Dekade (2016: 27 %, 2014: 18 %, 2012: 28 %, 2010: 16 %, 2008: 21 %). Die Zulässigkeit einer Verbindung privat beschaffter oder administrierter Systeme mit Unternehmenshardware oder -netzen zeigt ebenfalls ein gewohntes Bild (Abb. 17), auch wenn technische Kontrollen einer solchen Aufschaltung in der aktuellen Stichprobe seltener implementiert sind als beim letzten Mal.

Der – auch externe – Einsatz von IPv6 hat sich gegenüber den Ergebnissen von 2016 etwas erhöht: Dieses Mal gaben 39 % an, das „neue“ Internetprotokoll zu verwenden (2016: 32 %, 2014: 34 %), wobei 14 % hierüber auch Verbindungen nach außen routen (2016: 8 %, 2014: 3 %). 18 % nutzen IPv6 (auch) in-

Tabelle 14: Wesentliche Standards für Sicherheits-/Datenschutzmanagement-Systeme

ISO 2700x	66%
BSI 200-1	30%
BSI 100-1	29%
BS 10012	11%
VdS 3473	2%
Sonstige	14%

Basis: 87 Antworten

Tabelle 15: Maßnahmen zu Lagebild und „Situational Awareness“

	realisiert	geplant	nicht vorgesehen
zentrales Speichern aller Log-Informationen	45%	23%	32%
zentrales, regelmäßiges Auswerten aller Log-Informationen	23%	43%	35%
zentrales Echtzeit-Monitoring der Logs	21%	35%	44%
zentrales Korrelieren der Logs	13%	35%	53%
Integration von Helpdesk-Information in das zentrale Logging	12%	23%	65%
zentrales Compliance-Reporting	14%	29%	57%
firmenweites Security-Information- und -Event-Management (SIEM)	19%	42%	38%
Nutzung externer Dienste zur Früherkennung neuer Bedrohungen	30%	27%	43%
Melden eigener Informationen an solche Dienste oder an Behörden	29%	20%	51%

Basis: Ø 80 Antworten

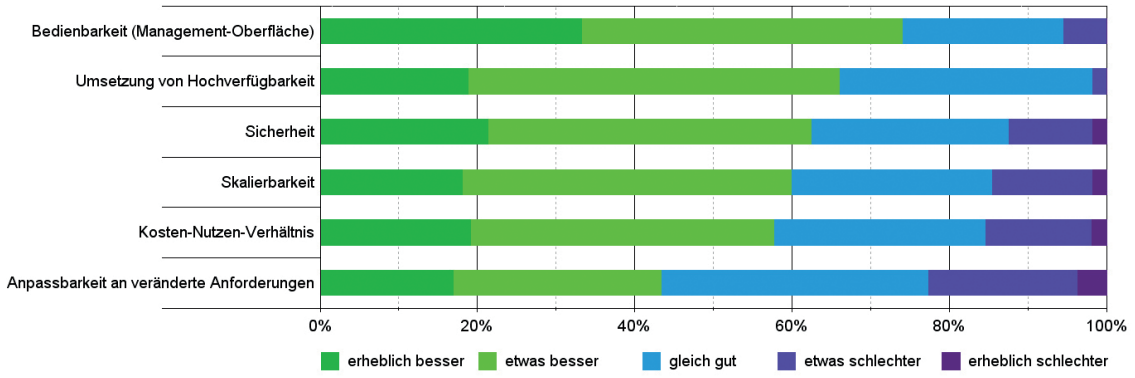


Abbildung 18: Unified Threat-Management (UTM) im Vergleich zu „Best of Breed" (sortiert nach UTM-Vorzügen)

Basis: 53 Antworten

tern, bei 16 % läuft es im Pilotbetrieb. Die Frage, ob ihre Netzwerk- und Sicherheitssysteme für den Einsatz von IPv6 bereit seien, beantworteten 56 % mit „ja" – hinsichtlich DNSSEC waren das 51 %.

Sicherheits- und Datenschutz-Management

Ein Informationssicherheits-Managementsystem (ISMS) ist bei 52 % der Befragten bereits realisiert, knapp ein Drittel plant es noch. Ebenfalls ein Drittel plant zudem die Implementierung eines Managementsystems für personenbezogene Daten – bei 39 % ist ein solches bereits im Einsatz. Die für die Studienteilnehmer wesentlichen Standards zu Konzeption und Betrieb von Security- und Datenschutz-Managementsystemen fasst Tabelle 14 zusammen.

Bei knapp der Hälfte (44 %) hatte die EU-Datenschutzgrundverordnung (DSGVO) Auswirkungen auf Managementsysteme. Dabei kam es allem voran zu vereinzelten Anpassungen von Sicherheitsmaßnahmen (58 %) und dem Neuaufbau eines Datenschutz-Managementsystems (55 %). Auch die Integration des Datenschutzes in ein ISMS war häufig zu beobachten (bei 42 %). Umfangreiche Anpassungen im ISMS wurden aufgrund der DSGVO bei 25 % notwendig.

Tabelle 15 zeigt die zusammengefassten Antworten zu getroffenen Maßnahmen zur „Situational Awareness" und zum Erstellen eines Lagebilds – hier ergibt sich ungefähr dieselbe Situation wie in den vorausgegangenen Studien. Auch die sicherheitsbezogene Auswertung von Endgeräte-Logfiles bleibt im gewohnten Rahmen: Bei 18 % der Teilnehmer werden diese regelmäßig geprüft (2016: 16 %, 2014: 19 %, 2012: 18 %, 2010: 11 %) – bei gut der Hälfte davon sogar täglich, im Mittel circa alle 11 Tage (2016: 6,5 Tage, 2014: 10 Tage, 2012: 13,5 Tage, 2010: 5,5 Tage). Wie in der vorigen Studie wertet jedoch auch etwa jede zehnte Organisation solche Quellen überhaupt nicht aus (11 %, 2016: 12 %, 2014: 8 %, 2012: 3 %, 2010: 16 %). Bei den verbleibenden 71 % erfolgt eine anlassbezogene Auswertung.

Die Einschätzung der Teilnehmer, wie Unified-Threat-Management-(UTM)-Systeme im Vergleich zu einem „Best of Breed"-Ansatz abschneiden, ist Abbildung 18 zu entnehmen. Dabei sah nur ein kleiner Anteil UTM-Lösungen in Sachen Sicherheit als nachteilig an (13 % „etwas" oder „erheblich" schlechter – 2016: 15 %, 2014: 20 %, 2012: 19 %, 2010: 23 %). Dessen ungeachtet bleibt der Einsatz von Produkten mehrerer verschiedener Anbieter auf verschiedenen Systemen oder Netzwerksegmenten, vor allem bei Server-Betriebssystemen und Anti-Virus-Software, aus Sicherheitsgründen durchaus verbreitet (siehe Tab. 16). Ein zentrales Management-Tool zur Verwaltung heterogener Security-Systeme haben 17 % realisiert, 24 % in Planung.

Systemauswahl und -sicherheit

Bei der Auswahl von Systemen und Lösungen für den (allgemeinen) IT-Betrieb bleibt der Preis das wichtigste Kriterium – dicht gefolgt von Aspekten der Anpassbarkeit und Sicherheit. Nur bei Securitysystemen steht – wie gehabt – die Sicherheit an erster Stelle (vgl. Abb. 19). Davon und von der Bedeutung von Sicherheits-Zertifikaten abgesehen, zeigt sich im Wesentlichen für beide Kategorien dieselbe Rangfolge der Kriterien. Die Herkunft von Anbietern aus dem deutschsprachigen Raum oder der EU rangiert weiterhin in der zweiten

Im Einsatz sind Lösungen von ...	nur einem Anbieter	zwei Anbietern	drei oder mehr Anbietern	*Mittelwert**
Server-Betriebssysteme	45%	30%	26%	1,81
Anti-Virus-Software	40%	41%	19%	1,79
Applikations-Server	55%	21%	24%	1,69
Web-Server	59%	25%	16%	1,57
Router/Netzwerkhardware	61%	26%	13%	1,53
Firewalls	57%	39%	4%	1,47

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

Basis: Ø 73 Antworten

*berechnet mit „drei oder mehr" = 3

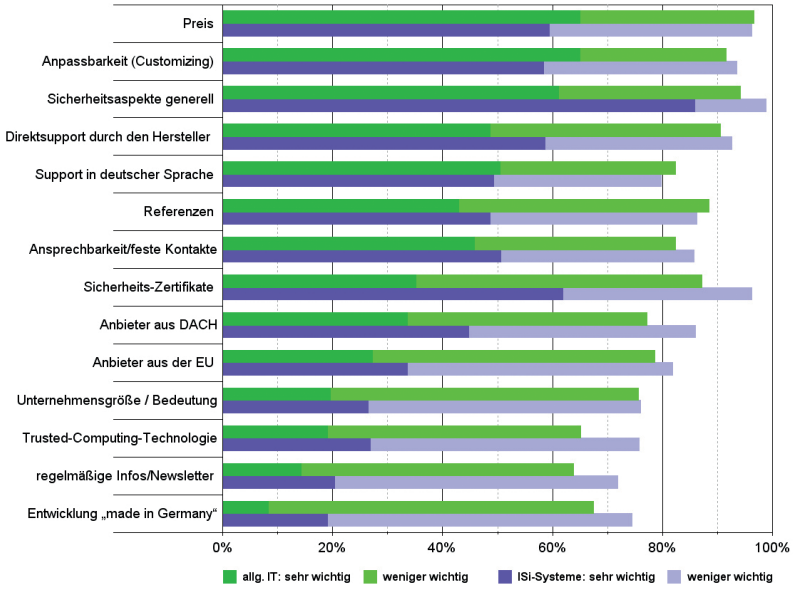


Abbildung 19: Kriterien zur Auswahl von IT-Systemen und -Lösungen (sortiert nach Wichtigkeit für allg. IT)

Basis: Ø 84 Antworten (allg. IT), Ø 78 (ISi-Systeme)

Tabellenhälfte, eine Entwicklung „made in Germany“ hat erneut eine ähnlich niedrige Bedeutung wie regelmäßige Newsletter. Konsequenterweise haben dieses Mal auch nur 26 % der Teilnehmer angegeben, dass in ihren Augen ein deutsches Development einen höheren Preis rechtfertigt (2016: 39 %, 2014: 34 %).

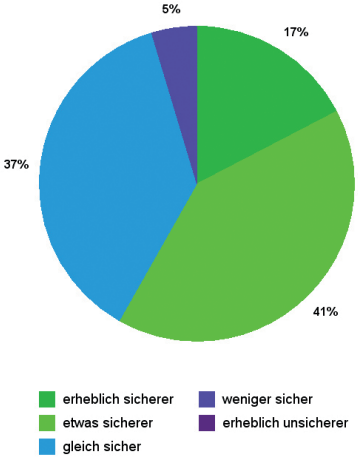


Abbildung 20: Einschätzung der Sicherheit von Open-Source-Software (OSS) gegenüber Programmen mit nicht-offengelegtem Quellcode

Basis: 86 Antworten

Höher im Kurs stehen da schon Sicherheits-Zertifikate, für die 66 % einen höheren Preis als angemessen ansehen. Auch in der aktuellen Stichprobe nannte sie gut ein Drittel „sehr wichtig“ für die Auswahl allgemeiner IT (34 %, 2016: 34 %, 2014: 25 %) – bei Security-Lösungen waren das sogar 62 % (2016: 60 %, 2014: 58 %).

Die Erfüllung von ISi-Anforderungen als Voraussetzung für die Inbetriebnahme von IT-Systemen und -Lösungen verifiziert in der aktuellen Stichprobe mit 56 % ein erhöhter Anteil der Befragten (2016: 44 %, 2014: 51 %, 2012: 37 %, 2010: 43 %).

Die Nutzung von Open-Source-Software (OSS) stieg ebenfalls an: Nunmehr 93 % der Befragten gaben an, dass in ihrem Haus zumindest gelegentlich OSS zum Einsatz kommt (2016: 86 %, 2014: 80 %, 2012: 84 %, 2010: 82 %) – bei 30 % ist dies „häufig“ der Fall (+1 %-Pkt.). Bei den Gründen für einen OSS-Einsatz dominieren weiterhin die Kosten (bei 66 %) – eine bessere Funktionalität nannten 45 % der Teilnehmer als Grund, bessere Interoperabilität und Sicherheit nur jeweils 29 % (Mehrfachantworten). Auch bei der Arbeit mit (Open-)Source-Code ist die Security nur selten der Treiber – Tabelle 17 fasst die Antworten der Befragten zusammen, warum und wie oft sie oder ihre Kollegen OSS-Code prüfen oder bearbeiten. Trotz geringer Neigung, OSS-Code selbst hinsichtlich seiner Sicherheit zu prüfen, sind die Befragten dieser Studie mehrheitlich der Meinung, dass solche Software sicherer ist als „Closed Source“ (58 %, 2016: 48 %, 2014: 46 %, 2012: 52 %, 2010: 43 % – vgl. Abb. 20).

Die Abbildungen 21 und 22 zeigen die jeweiligen Anteile der Studienteilnehmer, in deren Haus die angegebenen Betriebssysteme „in nennenswertem Umfang“ im Einsatz sind.

Erstmals haben wir nach einer Schätzung der durchschnittlichen Zeitspanne gefragt, die bei den Teilnehmern zwischen dem Erscheinen und einer umfassenden Verbreitung von Patches vergeht: „Normale“ Updates benötigten demnach bei Betriebssystemen im Mittel etwa drei Wochen (Median: 10 Tage – bei Anwendungen: Ø 38 Tage / 15 Tage), Security-Patches durchschnittlich etwa neun Tage (Median: 3 Tage – bei Anwendungen: Ø 14 Tage / 7 Tage). Um Versions- oder Funktions-Upgrades („Major Releases“) zu verbreiten, lassen sich die Befragten in beiden Kategorien durchschnittlich knapp drei Monate Zeit (Median: 30 Tage).

Smartphones / Tablets

Die aktuelle Stichprobe speichert deutlich häufiger schutzwürdige Daten auch auf Smartphones und Tablets (51 % realisiert oder geplant, 2016: 33 %, 2014: 41 %)

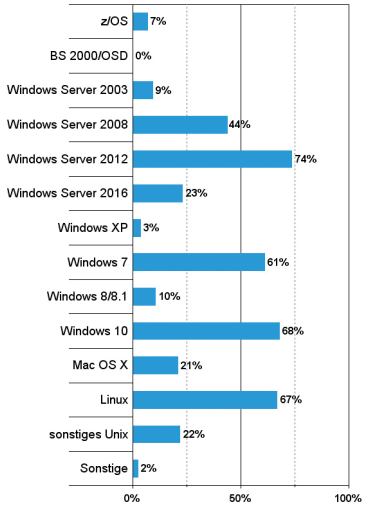
Tabelle 17: Arbeit mit Open-Source-Code

	häufig	gelegentlich	nie	*Vergleichszahl**
Prüfungen hinsichtlich funktionaler Aspekte	18%	40%	42%	0,93
Modifikationen / lokale Anpassungen	8%	39%	53%	0,64
Prüfungen hinsichtlich der Sicherheit	7%	36%	57%	0,56

Basis: Ø 74 Antworten

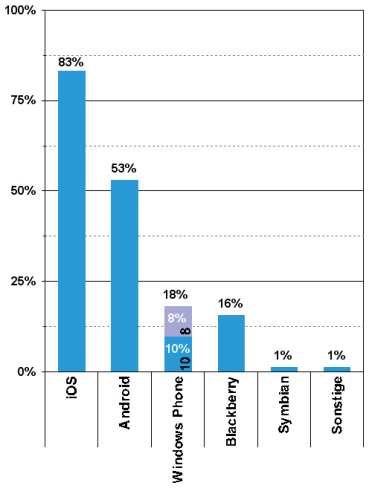
*häufig = 3, gelegentlich = 1, nie = 0

oder greift hierauf online zu (65 %, 2016: 53 %, 2014: 58 %). Damit geht konsequenterweise eine gesteigerte Installation von Sicherheitssoftware einher: Eine Verschlüsselung gespeicherter Daten ist nun bei 79 % realisiert oder geplant (2016: 56 %, 2014: 65 %), Security-Suites sind bei 63 % implementiert oder vorgesehen (2016: 54 %, 2014: 62 %). Erstmals gefragt haben wir nach Lösungen zur Trennung dienstlicher und persönlicher Daten und Apps, die bei 58 % realisiert oder geplant sind (Tab. 18). Die Angaben zum zentralisierten Management mobiler Apps und Daten bleiben hingegen auf dem Niveau der vorausgegangenen Studien.



Basis: 87 Antworten

Abbildung 21:
Anteil der Befragten, bei denen die genannten Betriebssysteme in „nenneswertem Umfang" im Einsatz sind



Basis: 83 Antworten

Abbildung 22:
Anteil der Befragten, bei denen die genannten Smartphone-Betriebssysteme in „nennenswertem Umfang" im Einsatz sind

Content- und E-Mail-Sicherheit

Tabelle 19 zeigt den gewünschten Funktionsumfang bei Lösungen zur Endpoint-Security. Hier hatten die aktuellen Teilnehmer teils deutlich abweichende Prioritäten gegenüber denjenigen der vorigen Studie: Am deutlichsten war das bei Device- und Schnittstellenkontrolle sowie Data-Leak/Loss-Prevention (DLP), die mit jeweils +16 Prozent-Punkten fünf beziehungsweise vier Ränge aufstiegen – auch eine zentrale Administration erzielte gesteigerte Beachtung. Applikationskontrolle, Desktop-/Client-Firewallfunktionen und Reporting-Tools blieben in etwa auf der gestärkten Position von 2016. Weniger wichtig als der vorigen Stichprobe waren den jetzigen Studienteilnehmern hingegen die Spam-Abwehr (–13 %-Pkt., –4 Ränge) sowie in geringerem Maße Anti-Spyware- und -Phishing-Funktionen sowie Inhaltsfilter.

Eine stetige Malware-Prüfung (On-Access-Scanner bzw. „Virenwächter") haben 81 % der Teilnehmer auf PCs, Notebooks und/oder Tablets im Einsatz (2016: 80 %, 2014: 75 %, 2012: 82 %, 2010: 83 %) – isolierte Testumgebungen zur Malware-Analyse stehen bei 46 % zur Verfügung (2016: 39 %, 2014: 46 %, 2012: 53 %, 2010: 45 %). Die Updatezyklen lagen im Mittel bei Firewalls und Gatewaysystemen sowie Mail-, File- und Applikationsservern bei gut 7 Stunden – auf PCs, Workstations und mobilen Endgeräten bei 10,5 beziehungsweise 11 Stunden. Dabei wurden bei *allen* Befragten dieser Stichprobe ortsfeste Systeme mindestens einmal täglich, mobile Geräte mindestens einmal alle zwei Tage aktualisiert.

Der Anteil von Spam, der die Organisationen per E-Mail erreichte, liegt im Mittel bei 33 % (2016: 37 %, 2014: 34 %) – 32 % der Teilnehmer gaben an, dass ihr Haus 50 % oder mehr Spam erhält (2016: 37 %, 2014: 26 %). Erneut beruhen dabei die weitaus meisten Angaben auf Schätzungen – nur 15 % der Befragten konnten auf ermittelte Werte zurückgreifen. Eine grafische Darstellung der gestaffelten Anwor-

	realisiert	geplant	*nicht vorgesehen*
Verschlüsselung gespeicherter Daten	60%	19%	21%
Online-Zugriff auf schutzwürdige Unternehmensdaten	53%	12%	35%
Security-Suite (Virenschutz, Personal-Firewall, ...)	46%	17%	37%
zentrales Management (Apps, Patches, ...)	45%	17%	38%
Lösung zur Trennung dienstlicher und persönlicher Daten/Apps	43%	16%	42%
Speicherung schutzwürdiger Daten auf dem Gerät	44%	7%	48%
Verschlüsselung von Sprachkommunikation	13%	8%	79%

Basis: Ø 79 Antworten

Tabelle 18: Sicherheitsaspekte bei Smartphones/Tablets von Mitarbeitern oder Partnern

Gewünschter Funktionsumfang (Mehrfachnennungen)	
Virenschutz	95%
zentrale Administration	87%
Spyware-Schutz	83%
Phishing-Abwehr	74%
Device-/Schnittstellenkontrolle	73%
Reporting-Tools	68%
Desktop/Client-Firewall	65%
Intrusion Detection/Prevention (IDS/IPS)	65%
Monitoring/Alerting	65%
Spam-Abwehr	60%
Data-Leak-/Loss-Prevention (DLP)	60%
Applikationskontrolle	58%
Verschlüsselung	55%
Prüfung von SSL/TLS-Übertragungen	46%
Inhaltsfilter	43%

Basis: 84 Antworten

Tabelle 19: Anforderungen an Endpoint-Security-Lösungen

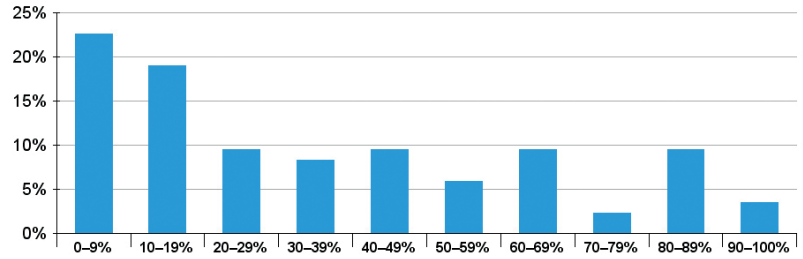


Abbildung 23: Spam-Anteil bei eingehenden E-Mails

Basis: 84 Antworten

Tabelle 20: Herkunft von Zertifikaten zur Sicherung von E-Mails / Datenaustausch

von einer kommerziellen CA (Root-Zert. üblicherweise mitgeliefert/vorinstalliert) *	65%
von einer Community-/Verbands-/Konzern-CA (Root-Zert. nachzuinstallieren) *	26%
von kleineren Organisationseinheiten / Einzelnen (self-signed) *	14%
keine Zertifikate im Einsatz	15%

Basis: 78 Antworten *Mehrfachnennungen

ten zum Spamaufkommen zeigt Abbildung 23.

Bei der E-Mail-Verschlüsselung liegt der Anteil der „Kryptoverweigerer", die auch dann nie chiffrieren, wenn der Kommunikationspartner über einen Kryptoschlüssel verfügt, mit 22 % – teils deutlich – unter den Werten der vorausgegangenen Dekade (2016: 29 %, 2014: 23 %, 2012: 32 %, 2010: 38 %, 2008: 44 %). In den Unternehmen von 70 % der Befragten würden in solchen Fällen zumindest sensitive Nachrichten verschlüsselt, bei 25 % externe und bei 18 % alle E-Mails (Mehrfachantworten).

IT-Notfall-/Wiederanlaufkonzept	
... existiert	71%
... ist schriftlich fixiert	84%
berücksichtigt explizit spezielle Anforderungen für/bei...	
... Hardware-Ausfall/ -Wiederbeschaffung	92%
... physische Einwirkungen	90%
... Software-Sicherheitsvorfälle	67%
... Malware-/Exploit-Epidemien	57%
... Zusammenbruch externer Infrastrukturen	56%
... Hochverfügbarkeit des E-Business	53%
... gezielte Angriffe durch Einzeltäter	45%
... Denial-of-Service-Attacken	43%
unternehmenswichtige Daten liegen räumlich getrennt vor	84%

Tabelle 21: Existenz und Besonderheiten von IT-Notfall-/Wiederanlaufplänen

Basis: 83 Antworten, Ø 51 Antworten (Fixierung und Anforderungen), 85 Antworten (räuml. Trennung)

Wie üblich sind kryptografische Signaturen etwas unbeliebter. Der Anteil derer, die grundsätzlich *nicht* signieren, bleibt mit 33 % jedoch auf dem relativ geringen Wert der vorigen Erhebung – beim Vorliegen von Kommunikationsschlüsseln signieren die Organisationen von 51 % der Teilnehmer nun zumindest sensitive Nachrichten, 29 % alle externen E-Mails und 37 % sogar *alle* E-Mails.

Eine „virtuelle Poststelle" zur zentralen Ver-/Entschlüsselung und/oder Signaturerstellung/-prüfung am Gateway oder auf einem Server nutzen 36 % (2016: 26 %, 2014: 23 %, 2012: 25 %, 2010: 17 %), weitere 14 % planen dies für die Zukunft. Das deutlich erhöhte Vorkommen solcher Systeme in der aktuellen Stichprobe dürfte sicherlich zum Teil auch für die gesteigerte Bereitschaft zum Einsatz von Kryptografie in der E-Mail-Kommunikation verantwortlich sein. Die – erstmals erhobenen – Erkenntnisse zur Herkunft von Zertifikaten für die Sicherung von E-Mails und Datenaustausch zeigt Tabelle 20.

In Sachen eingesetzter Standards baut S/MIME seinen Vorsprung weiter aus und war dieses Mal bei 80 % der Befragten im Einsatz (2016: 59 %, 2014: 67 %), während (Open)PGP nur noch bei 38 % der Teilnehmer genutzt wurde (2016: 42 %, 2014: 47 %) – 14 % nutzen (zumindest auch) sonstige Verfahren (Mehrfachantworten). Zum ersten Mal haben wir gefragt, ob in nennenswertem Umfang zum Schutz von Attachments oder beim Datenaustausch auch Lösungen auf Anwendungs- oder Dienste-Ebene zum Einsatz kommen – 76 % bejahten das: Am verbreitetsten war dabei die Archiv-Verschlüsselung (ZIP o. Ä.) bei 60 % der Teilnehmer, gefolgt von chiffrierten PDFs (35 %), verschlüsselt speichernden Cloud-Services (21 %), anderen Clouddiensten, die jedoch nur eine Authentifizierung verlangen (11 %), sowie den Schutzfunktionen für Officedateien (5 %) – ein Viertel der Teilnehmer gab zudem an, auch sonstige Verfahren einzusetzen.

Notfallvorsorge

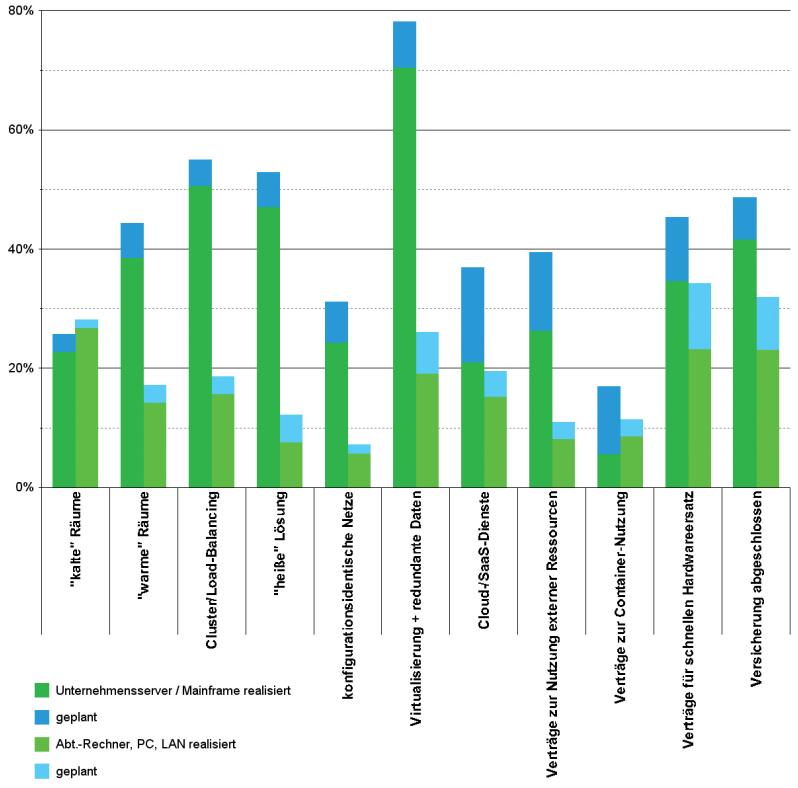
Tabelle 21 zeigt die Existenz sowie Besonderheiten von IT-Notfall- und -Wiederanlaufplänen. Mit einem erneuten Wert von 71 % für das Vorliegen entsprechender Konzepte bleibt auch die aktuelle Stichprobe wieder am unteren Ende der Spannweite unserer Studien mit der aktuellen Formulierung dieser Frage (2016: 71 %, 2004–2014: 69–82 %). Die Angaben der Teilnehmer zu Bereitstellungen für längere Ausfälle sind in Abbildung 24 zu finden.

8 % der Befragten, die einen Recovery-Vertrag abgeschlossen haben, mussten diesen 2016/2017 auch tatsächlich in Anspruch nehmen – die Hälfte davon mehrmals. Eine Spezialversicherung hinsichtlich von IT-Risiken (z. B. Datenlöschung/-diebstahl, Betriebsunterbrechung durch Malware/Angriffe, Imageschäden, Spionage o. Ä.) haben die Organisationen von 35 % der Stichprobe abgeschlossen. Dabei musste etwa jede siebte für den Abschluss mindestens einer Versicherung ein ISi-Audit durchlaufen oder ein anerkanntes ISi-Zertifikat vorlegen – jede

fünfte erhielte für solche Maßnahmen günstigere Konditionen bei mindestens einem ihrer Verträge.

Die Dokumentation für den Notfall erfolgt noch immer überwiegend mittels eines manuellen Handbuchs (bei 61 %) – onlinegestützte Handbücher sind bei 45 % bereits im Einsatz, eine Online-Anwendung etwa bei jedem Sechsten (16 %). Die Aktualisierung der Notfalldokumentation vollziehen 23 % der Teilnehmer regelmäßig (im Mittel etwa jährlich), bei 71 % passiert das anlassbezogen und 6 % aktualisieren diese wichtigen Informationen „nie".

Ein Security-Operations-Center (SOC) für das eigene Haus haben 12 % der Befragten realisiert, weitere 23 % in Planung (65 % „nicht vorgesehen"). Ein eigenes Computer-Emergency- oder Security-Incident-Response-Team (CERT/CSIRT) betreiben 23 % – 41 % nutzen die Dienstleistungen eines externen Teams, wobei jedoch nur 6 % der Befragten auch kostenpflichtige Services in Anspruch nehmen.



Basis: Ø 73 Antworten (Unternehmensserver/Mainframes), Ø 71 (Abt.-Systeme/PCs)

Abbildung 24: Bereitstellungen für längere Ausfälle

Datenverluste und Forensik

Etwa jeder fünfte Studienteilnehmer (22 %) berichtete für den Zeitraum 2016/2017 von nennenswerten Problemen mit (zumindest zeitweise) unverfügbaren oder verlorenen Daten – die Ursachen für diese Vorkommnisse zeigt Abbildung 25, wobei die neu aufgenommene Kategorie „Ransomware" an der Spitze steht; von „höherer Gewalt" war dieses Mal keine Organisation betroffen. Letztlich ließen sich in allen Fällen durch die eine oder andere Methode alle Daten wiederherstellen: Am häufigsten war eine Rekonstruktion aus dem Backup (bei 89 %) – 28 % der Befragten griffen auf eine manuelle Neuerfassung zurück, 11 % auf Datenrettung durch Externe und 6 % haben mit eigenen Mitarbeitern erfolgreich Datenrettungs-Tools eingesetzt (Mehrfachantworten). Tabelle 22 zeigt die geschätzten Verluste, die bei einer totalen Vernichtung aller elektronisch gespeicherten Daten zu erwarten gewesen wären.

Mindestens eine rechtliche Verfolgung eines Sicherheits-Vorfalls gab es in den Jahren 2016/2017 bei 17 % der Befragten. Wo dies *nicht* der Fall war, lag das bei 75 % an dem glücklichen Umstand, dass

Datenwert / Verlust	Nennungen
unter 10 Tsd. €	9
unter 100 Tsd. €	6
unter 1 Mio. €	9
unter 100 Mio. €	23
unter 500 Mio. €	2
unter 1 Mrd. €	3
ab 1 Mrd. €	4

Basis: 56 Antworten

Tabelle 22: Geschätzter Verlust bei Vernichtung aller elektronisch gespeicherten Daten (nachträgliche Staffelung)

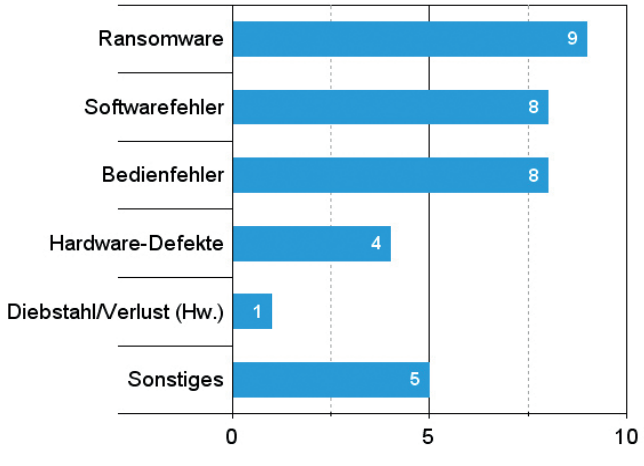


Abbildung 25: Ursachen für Verluste oder (zumindest zeitweilige) Nichtverfügbarkeit von Nennungen

genutzte Consulting-Dienstleistungen (Mehrfachnennungen)	
Penetrationstests	71%
Strategie- und Managementberatung	44%
Risikoanalysen und Konzeptentwicklung	44%
Schwachstellenanalysen	38%
Durchführung von Inhouse-Schulungen	36%
Kontrolle vorhandener Konzepte	36%
Produktberatung und Kaufunterstützung	33%
Umsetzung von Konzepten und Maßnahmen	29%
Prozess-Entwicklung und -Optimierung	29%

Tabelle 23: ISi-Beratung

Basis: 45 Antworten

genutzte Outsourcing-Dienstleistungen (Mehrfachnennungen)	
Vernichtung von Datenträgern (Papier, IT)	80%
Wachschutz / Bewachung	52%
Spamabwehr	48%
E-Mail-Betrieb	48%
Anwendungssysteme	43%
gesamte(s) Rechenzentrum/IT	41%
Datensicherung, Backup-Lösungen	34%
Netzwerk-Management	32%
Managed Firewall/IDS/IPS	30%
Datenbank-Systeme/-Werkzeuge	30%
Betriebssystempflege/Administration	23%
Haustechnik	23%
Archivierung, Dokumentation	14%
Content-Security/Virenabwehr	11%
Personaleinsatz/-entwicklung, Mitarbeiterweiterbildung	9%
Notfallvorsorge/Business-Continuity	9%
Datenschutz	7%
externer ISi-Beauftragter	4%

Tabelle 24: Outsourcing

Basis: 56 Antworten

es keinerlei entsprechende Vorfälle gegeben hatte – 23 % sahen kein Verfolgungsinteresse und 2 % verzichteten mangels Wissen um Ermittlungsmöglichkeiten auf ein juristisches Nachspiel.

Dienstleistungen

Die Organisationen von 10 % der Befragten nutzen häufig externe ISi-Beratung – 46 % tun dies „gelegentlich". Die dabei beauftragten Dienste listet Tabelle 23. Die Zufriedenheit mit den Beratungsleistungen benoteten die Studienteilnehmer im Mittel erneut knapp mit einer „Zwei minus". Nur wenig schlechter sieht die Bewertung von Outsourcingleistungen aus, die im Mittel „Zwei bis Drei" lautet, wobei jedoch schon etwa jeder Zehnte nur ein „ausreichend" vergab, 2 % nannten die Outsourcingleistungen sogar „nicht ausreichend". Generell nutzen 68 % der befragten Organisationen Outsourcing – die beauftragten Leistungen sind Tabelle 24 zu entnehmen.

Im Vergleich mit Inhouse-Lösungen schneiden externe Dienste (Outsourcing/MSS/Cloud-Services) in der aktuellen Stichprobe besser ab als zuvor: Skalierbarkeit ist weiterhin der größte Pluspunkt, wird dieses Mal aber bereits von der Sicherheit gefolgt, welche die Teilnehmer ebenfalls höher einschätzen als im Eigenbetrieb. Damit wird die höhere „Anpassbarkeit an veränderte Anforderungen" auf den dritten Platz verdrängt. Das Kosten-Nutzen-Verhältnis liegt ebenfalls noch leicht im Plus, der Datenschutz erzielt eine neutrale Bewertung. Nur in Sachen „Transparenz/Kontrollierbarkeit" bewerten die Teilnehmer externe Dienste mehrheitlich schlechter. Details zeigt Abbildung 26.

Service-Level-Agreements (SLAs) oder sonstige vertragliche Vereinbarungen mit Outsourcern gibt es bei 80 % der Teilnehmer – 41 % kontrollieren diese Vorgaben regelmäßig, 51 % anlassbezogen. Ebenfalls 80 % haben dabei explizite Anforderungen an den Datenschutz vorgesehen (Kontrolle: 33 %/61 %), 57 % explizite ISi-Anforderungen (Kontrolle: 39 % /54 %). Regelungen zu Haftungsübernahme oder Schadensersatz gibt es bei 56 %.

Applikationen oder Sicherheitssysteme, die auf Cloud-/Web-Services zurückgreifen, sind bei ungefähr der Hälfte der Befragten im Einsatz: 38 % wissen das sicher, 15 % vermuten es – „vermutlich nicht" sagten 9 %, 39 % waren sich sicher, dass bei ihnen keine solchen Systeme genutzt werden. Die mit derartigen Lösungen verbundene Kommunikation sowie die Weitergabe von Daten an die jeweiligen Dienstleister nannten 68 % hinreichend transparent nachvollziehbar.

Abbildung 26: Externe Dienste (Outsourcing/MSS/Cloud) im Vergleich zu Inhouse-Lösungen

Basis: Ø 76 Antworten

Informationsquellen

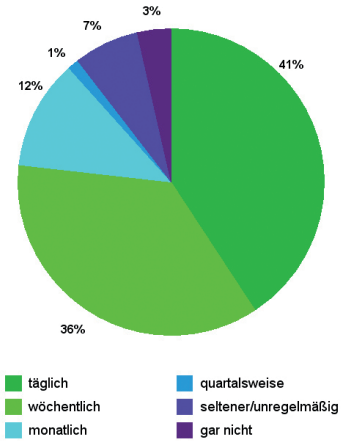
Als Quelle für ISi-Informationen nutzen rund zwei Drittel der Befragten (67 %) die it-sa, 44 % den BSI-Kongress, 39 % die CEBIT, 16 % die Infosecurity in London sowie ferner 5 % die Essener Security, 4 % die RSA-Konferenz und 2 % die ISSE. Die weiteren, nachträglich kategorisierten „Top-3"-Quellen führt das Internet an (19 Nennungen), gefolgt von Fachzeitschriften (15), Verbänden und Organisationen (15), Konferenzen und Seminaren (13) sowie ferner Herstellern (7), Fachliteratur (5) und Newsletter (4).

Für aktuelle Sicherheits-Updates bleibt die aktive Information durch Hersteller knapp die erste Wahl (69 %), dicht gefolgt von der aktiven wie passiven Information durch Dritte (jeweils 65 %) sowie Informationsseiten der Hersteller (46 %) und aktive Infos durch Anbieter (Systemhäuser, Händler usw. – 40 %, Mehrfachnennungen). Die Frequenz, mit der die Befragten im Mittel passive Kanäle prüfen, illustriert Abbildung 27 – die Bewertung der Qualität von Hersteller-Advisories fasst Tabelle 25 zusammen.

	sehr gut	gut	befriedigend	ausreichend	nicht ausreichend	*Note*
Umfang/Vollständigkeit	0%	54%	33%	6%	6%	2,64
Verständlichkeit	0%	36%	51%	10%	4%	2,81
Geschwindigkeit	0%	31%	46%	20%	4%	2,96

Basis: 81 Antworten

Tabelle 25: Qualität von Herstellerinfos



Basis: 86 Antworten

Abbildung 27: Prüfung passiver Kanäle

Teilnehmer

Bezogen auf das gesamte Teilnehmerfeld wurde über die Hälfte der eingegangenen Fragebögen (51 %) durch Angehörige einer IT-Sicherheits-Abteilung ausgefüllt (ISi-Admins, -Beauftragte und -Verantwortliche bzw. CISO/CSO) – bei den großen Unternehmen („Große") waren es sogar 74 %, bei Organisationen unter 500 Mitarbeitern (KMU) immerhin noch 31 %. Jeder achte Fragebogen kam von einem RZ-/IT-Leiter (10 %) oder CIO (2 %). Weitere größere Ausfüllergruppen bei den KMU waren allgemeine IT-Mitarbeiter (19 %), Berater (13 %) sowie Geschäftsführer (10 %). Bei den „Großen" kamen 7 % der Antworten aus der Revision. Tabelle 26 fasst die Funktionsbezeichnungen der Ausfüller im gesamten Teilnehmerfeld zusammen.

IT-Sicherheitsbeauftragter	32%
IT-Sicherheitsverantwortlicher/CISO	12%
IT-Mitarbeiter	11%
RZ-/IT-Leiter	10%
Berater	7%
IT-Sicherheits-Admin/-Mitarbeiter	7%
Geschäftsführer	6%
Administrator/Systemtechniker	4%
Datenschutzbeauftragter	3%
Revisor	3%
CIO	2%
Sonstiges	2%

Basis: 90 Antworten

Tabelle 26: Funktionsbezeichnung der Fragebogenausfüller

Tabelle 27 zeigt hingegen den Anteil der teilnehmenden Organisationen, in denen es bestimmte Funktionsträger *gibt*. Dabei besitzt heuer ein großer Teil der Stichprobe einen expliziten ISi-Verantwortlichen/CISO (69 % vs. 2016: 54 %, 2014: 62 %, 2012: 57 %). Da man vermuten könnte, dass solche Organisationen bei knappen Ressourcen bereitwilliger an unserer Studie teilgenommen haben könnten, lässt sich durch die stark abweichende Größe der Stichprobe gegenüber den früheren Erhebungen hieraus jedoch noch keine Steigerung bei der Einrichtung solcher Posten folgern.

Abbildung 28 zeigt die Nationalität des Hauptsitzes der befragten Unternehmen und Behörden, ihre Branchenzugehörigkeit ist in Tabelle 28 erfasst. Eine Staffelung der Unternehmens-/Organisationsgrößen der Studienteilnehmer ist Abbildung 29 zu entnehmen – 51 % sind KMU zuzuordnen, 43 % den „Großen". Weitere 6 % haben zur Organisationsgröße keine Angaben gemacht.

Die „durchschnittliche Organisation", die an dieser Studie teilgenommen hat, beschäftigt 5645 Mitarbeiter, davon 131 in der IT, der 9 ISi-Spezialisten zur Verfügung stehen. Beim mittleren Großunternehmen dieser Stichprobe waren es 12 030 Mitarbeiter mit 221 in der IT – für die Informations-Sicherheit stehen dort 7 Spezialisten bereit.

Die teilnehmenden KMU haben im Mittel 153 Mitarbeiter, davon 53 in der IT inklusive sogar 12 ISi-Spezialisten. Diese Zahlen werden aber stark von drei Beratungshäusern mit einer enorm großen Zahl von

Im Unternehmen gibt es ...	
ISi-Verantwortlicher/C(I)SO	69%
ISi-Ausschuss (o.Ä.)	33%
Datenschutzbeauftragter	87%
Leiter IT/DV/RZ	84%
IT-/DV-Revision	21%
Leiter Organisation	46%
Leiter Sicherheit/Werkschutz	28%
IT-Administratoren	82%
DV-orientierter Jurist	22%

Basis: 90 Antworten – Mehrfachnennungen möglich

Tabelle 27: Vorhandene Funktionsträger in den befragten Organisationen

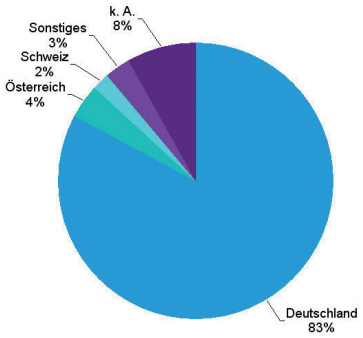


Abbildung 28: Hauptsitz der teilnehmenden Unternehmen und Behörden

Basis: 99 Antworten

Behörden/öffentliche Hand	21%
Berater	17%
Kreditwirtschaft	7%
Outsourcing-Dienstleister	7%
Handel	5%
Transport/Verkehr	5%
IT-Anbieter/-Dienstleister	4%
übrige Industrie	4%
Energieversorgung	3%
Versicherungen	3%
Wissenschaft/Forschung/Schulen	3%
chemische Industrie	2%
Gesundheitswesen	2%
Handwerk	2%
Telekommunikationsdienstleister/ Provider	2%
Verlage/Medien	1%
Sonstiges	3%
k. A.	8%

Tabelle 28: Branchenzugehörigkeit der Studienteilnehmer

Basis: 99 Antworten

ISi-Experten beeinflusst. Unter Auslassung dieser Teilnehmer zeigt sich ein „durchschnittliches KMU“ mit 150 Beschäftigten, von denen 48 in einer IT-Abteilung arbeiten – inklusive 3 ISi-Spezialisten.

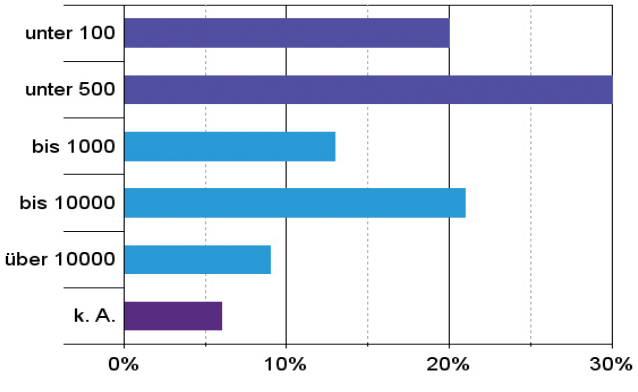


Abbildung 29: Größe der teilnehmenden Organisationen

Basis: 99 Antworten

Infrastruktur

Die gemittelte IT-Landschaft des „Durchschnittsunternehmens“ dieser Studie umfasst – bei Auslassung eines stark dezentral ausgerichteten Ausreißerwerts – 1 Mainframe (KMU 0 / Große 2), 685 Server (49 / 1435), 2560 Clients/PCs (81 / 5341) und 131 Heim-Telearbeitsplätze (22 / 259). Hinzu kommen 993 Notebooks (66 / 2034), 653 Smartphones und Tablets (70 / 1306) sowie 1269 Voice-over-IP-(VoIP)-Systeme (64 / 2659). Vernetzt sind die Teilnehmer-Organisationen im Mittel – nach Ausschluss eines weiteren Ausreißerwerts – über 105 Wide-Area-Networks (58 / 162 – jeweils inkl. VPNs und Mietnetzen), 676 LAN-/PC-Netze (9 / 1528) sowie 30 Wireless LANs (7 / 59).

Betrachtet man die Zahl der Endgeräte (ohne VoIP-Systeme) für jede einzelne befragte Organisation, so liegt der Durchschnitt bei 6103 (KMU 240 / Große 12 525). Der mittlere Anteil mobiler Endpoints betrug über das gesamte Teilnehmerfeld 48 % (KMU 56 % / Große 40 %).

Budgets

Wie in unseren Erhebungen üblich, hat nur etwa ein Drittel der Teilnehmer konkrete Zahlen zu Umsatz (27 Befragte) oder Bilanzsummen (6 Befragte) seines Hauses genannt – weitere 27 Befragte gaben an, dass entsprechende Kenngrößen für ihre Organisation nicht relevant seien, da es sich dabei um eine Behörde oder Ähnliches handele. Der genannte Umsatz betrug im Mittel circa 1,36 Mrd. € (KMU 30 Mio. € / Große 3,6 Mrd. €) – die durchschnittliche angegebene Bilanzsumme belief sich auf rund 44,5 Mrd. € (KMU 28 Mrd. € / Große 47,8 Mrd. €). Für eine gestaffelte Darstellung siehe Abbildung 30.

Der Anteil der Teilnehmer, die Angaben zu verfügbaren Finanzmitteln für die IT und Informations-Sicherheit gemacht haben, lag mit 30 von 99 ebenfalls im üblichen Rahmen. Gleichermaßen üblich ist dabei, dass nur ein Sechstel davon auf ermittelte Zahlen zurückgreifen konnten (5/99, 2016: 15/82) – in diesem Fall allerdings sowohl für das IT-Budget als auch den ISi-Anteil daran. Drei dieser fünf „Glücklichen“ gehörten dabei zu einer Behörde oder sonstigen Organisation der öffentlichen Hand.

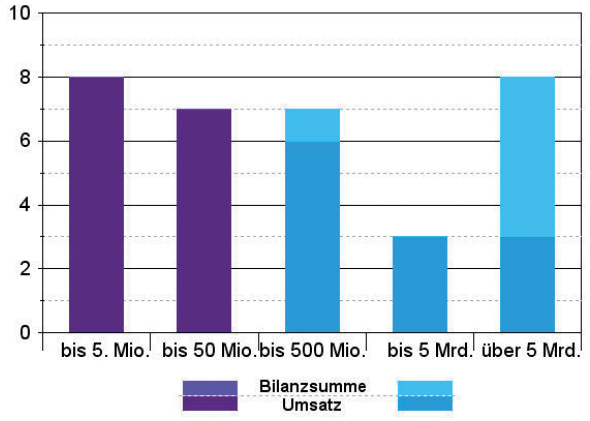
Die „durchschnittliche Teilnehmer-Organisation“ verfügte 2017 auf Basis dieser 30 Angaben über ein IT-Budget – inklusive Personalkosten – von knapp 19,3 Mio. € (KMU 597 Tsd. € / Große 31,7 Mio. €).

Die Spannbreite des jeweiligen Anteils der Informations-Sicherheit am IT-Budget zeigen die Boxplots der Abbildungen 31 und 32. Das rechnerische Mittel lag bei 9,46 % (KMU 13,6 % / Große 6,34 %), der Median bei 10 % (13,3 % / 4,5 %).

Absolute ISi-Budgets ließen sich aus 27 Fragebögen errechnen, die sowohl Angaben zum IT-Budget als auch zum Anteil der Informations-Sicherheit enthielten. Hieraus ergibt sich eine durchschnittliche finanzielle Ausstattung der „mittleren Organisation“ in der Stichprobe von rund 1 Mio. € (KMU 92 Tsd. € / Große 1,7 Mio. €). Eine gestaffelte Auswertung dieser Ergebnisse zeigt Abbildung 33.

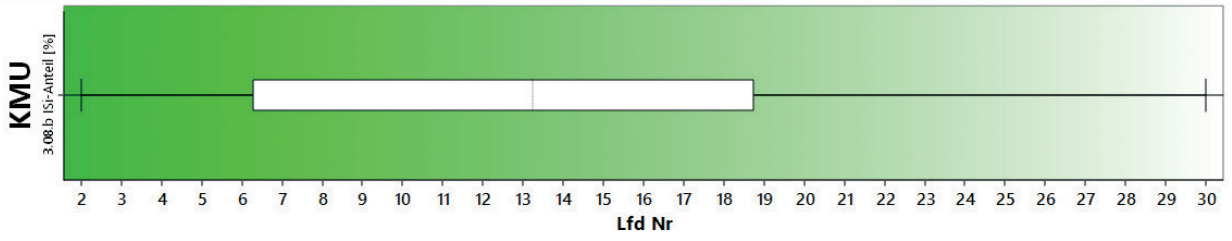
Wie immer gilt: Unsere Studie ist nicht repräsentativ – weder für bestimmte Branchen noch für die gesamte Wirtschaft im deutschsprachigen Raum. Durch die von uns erreichten Zielgruppen dürfte sich die erfasste Stichprobe eher überdurchschnittlich intensiv mit der Informations-Sicherheit (ISi) auseinandersetzen. Aufgrund der dieses Mal recht geringen Teilnehmerzahl sind zudem erhöhte Schwankungen möglich. Um möglicherweise verwirrende Angaben durch Bruchteile möglichst weitgehend zu vermeiden, haben wir in der Regel auch bei kleineren Antwortzahlen zu konkreten Fragen eine Prozentuierung vorgenommen. Unter Tabellen und Grafiken ist die jeweilige Basis explizit angegeben – Studienteilnehmer finden zudem in der vollständigen tabellarischen Auswertung bei jeder Teilfrage die konkreten Antwortzahlen.

Vergleiche der Werte in abgedruckten Tabellen können aufgrund von Rundungsfehlern um ±1 %-Punkte von berechneten Vergleichen abweichen. ■



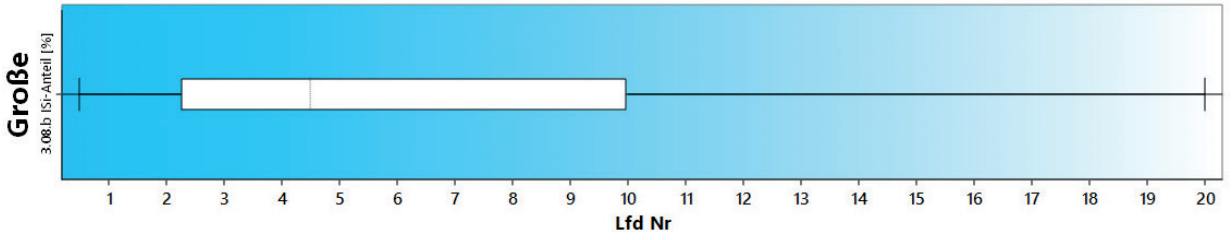
Basis: 27 Antworten (Umsatz), 6 (Bilanzsumme)

Abbildung 30: Geschäftszahlen (Umsatz bzw. Bilanzsumme) der teilnehmenden Organisationen [Nennungen]



Basis: 12 Antworten

Abbildung 31: Anteil der ISi am IT-Budget bei teilnehmenden KMU



Basis: 16 Antworten

Abbildung 32: Anteil der ISi am IT-Budget bei teilnehmenden großen Organisationen

Impressum

Sonderdruck aus <kes> – Die Zeitschrift für Informations-Sicherheit Ausgaben 2018#4, 2018#5 und 2018#6

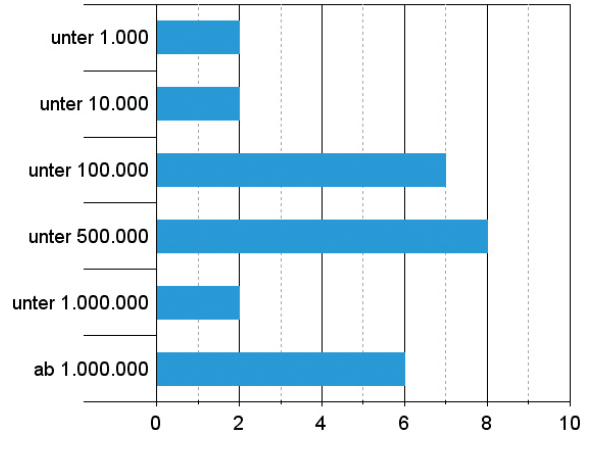
für UIMC Dr. Vossbein GmbH & Co. KG,
Otto-Hausmann-Ring 113, 42115 Wuppertal (www.uimc.de)

Tel. +49 2234 98949-30, Fax +49 2234 98949-32,
info@datakontext.com

Verantwortlich i.S.d.P.: Norbert Luckhardt (www.kes.info)

Satz und Layout: BlackArt-Werbestudio, 55413 Weiler

Druck: BWH GmbH, Beckstr. 10, 30457 Hannover



Basis: 27 Antworten

Abbildung 33: Budget für Informations-Sicherheit [Anzahl der errechneten Werte]

Guter Datenschutz kommt aus Wuppertal und Saarbrücken und Wien!
Und kommt überall dort hin, wo Sie ihn brauchen... auch EU-weit!

Datenschutz
Informationssicherheit
Organisation / Strategie

mehr unter www.uimc.de