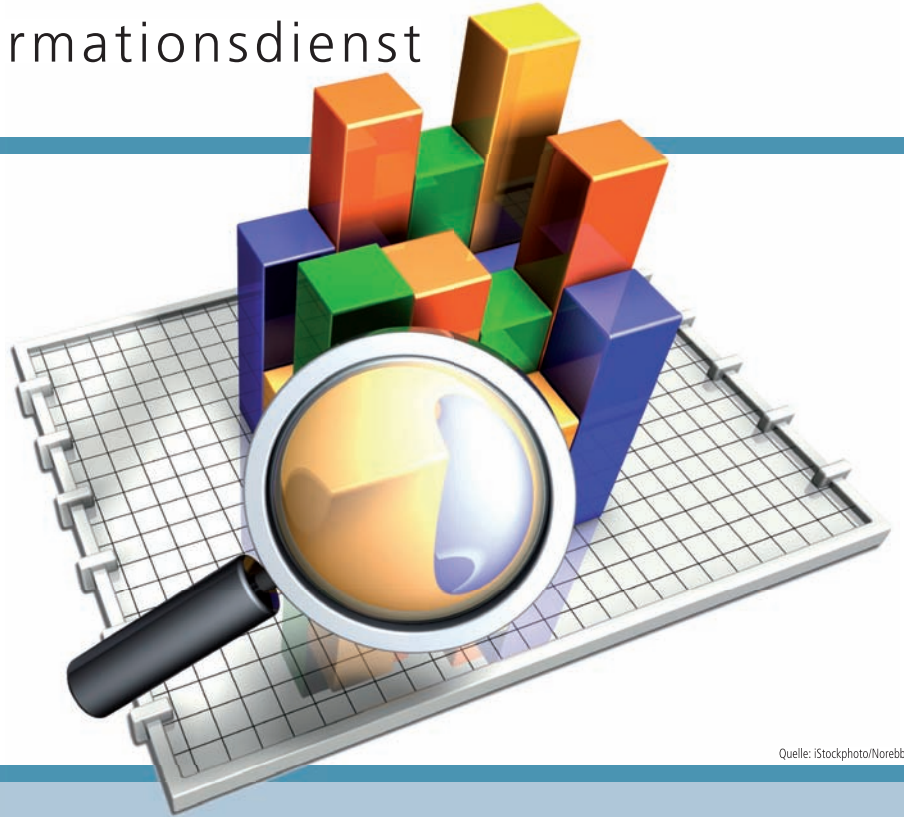




Special IT-Grundschutz

Informationsdienst



Quelle: iStockphoto/Norebbo

Sonderdruck für



FINANCE SECURITY

Studien und Analysen

Ergebnisse zur Umfrage „IT-Sicherheitsstandards und Notfallmanagement 2011/2012“

In Zusammenarbeit mit:



research
an der Universität
Regensburg GmbH



Bundesamt
für Sicherheit in der
Informationstechnik

SecuMedia
Der Verlag für
Sicherheits-Informationen

Dauerbrenner Akzeptanz und Notfallmanagement

Umfrage „Informationssicherheits- und Notfallmanagement: Trends 2012“

Elmar Török, bits+bites

Die zweite Auflage der Umfrage zu IT-Sicherheitsstandards wurde genauso gut angenommen wie ihr Vorgänger. Über 400 Teilnehmer füllten den Fragebogen zu „Informationssicherheits- und Notfallmanagement: Trends 2012“ aus. Wie im letzten Jahr gab es Überraschungen ebenso wie die Bestätigung von Trends und Einschätzungen der Redaktion.

Standards wie der IT-Grundschutz oder ISO/IEC 27001/2 sind in vielen Organisationen das Mittel der Wahl für die Sicherung der IT-Systeme. Um Informationen von den Anwendern über den Einsatz von IT-Standards zu gewinnen, führte ibi research in Zusammenarbeit mit dem SecuMedia Verlag und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Studie durch. Zudem sollten mit der Studie Zahlen und Daten über den Einsatz der Konzepte erhoben und Optimierungspotenziale sowie Wünsche vonseiten der Anwender aufgedeckt werden. Wie im Jahr 2010 hat auch die aktuelle Stu-

die ein Schwerpunktthema neben der allgemeinen IT-Sicherheit: Sie fokussiert sich auf die Thematik Notfallmanagement.

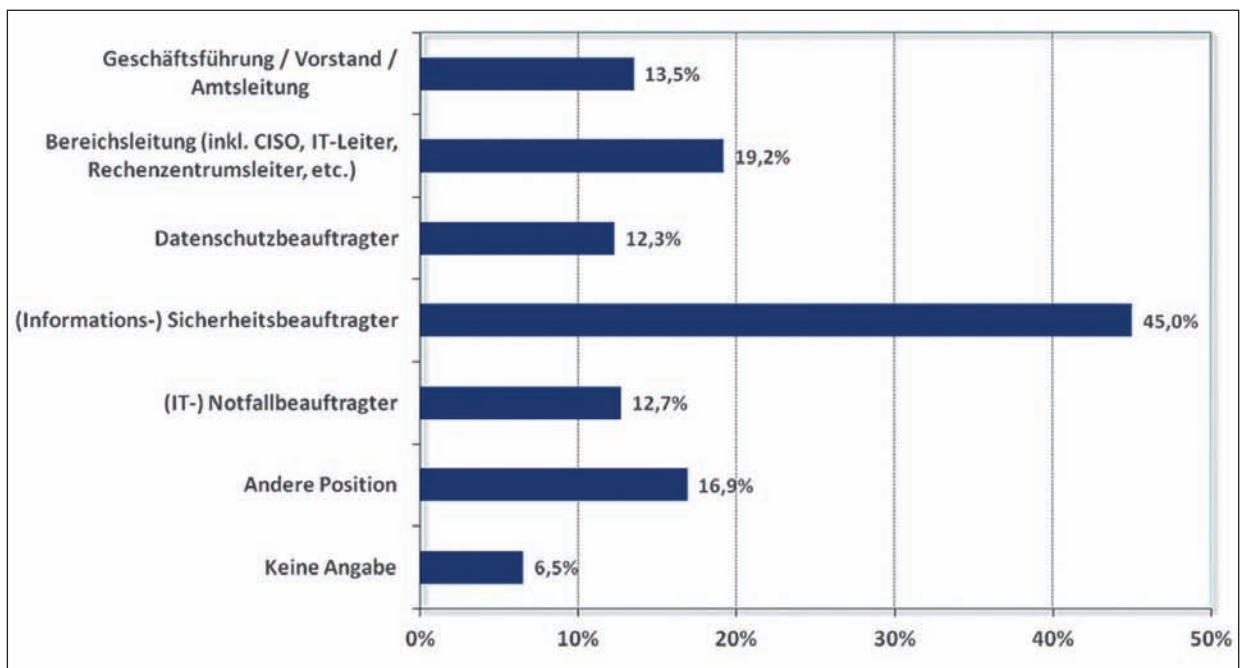
Teilnehmerzahl ungebrochen hoch

Die Teilnehmerzahl lag mit 423 ausgefüllten Fragebögen erneut erfreulich hoch. Nach Analyse der Daten blieben letztendlich 260 valide Datensätze übrig, welche in die Auswertungen eingingen. Es wurden ausschließlich vollständig ausgefüllte Fragebögen berücksichtigt. Den eindeutig größten Anteil

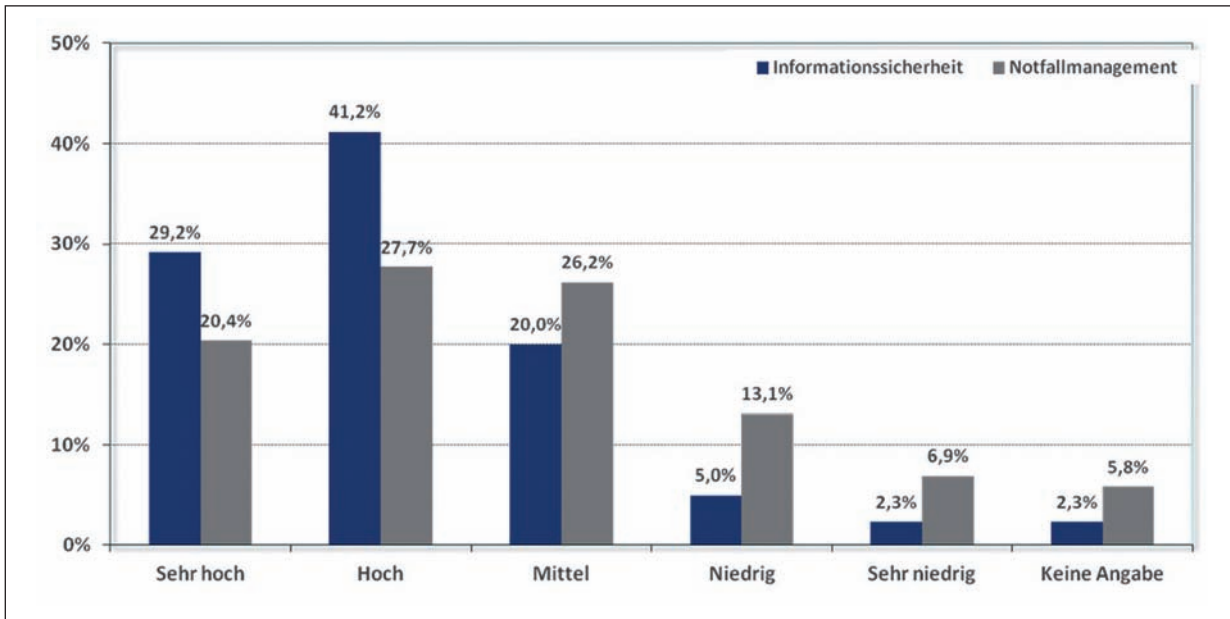
der Umfrageteilnehmer stellten die (Informations-) Sicherheitsbeauftragten (45 %). Die anderen Positionen wurden im Verhältnis dazu mit circa 10-20 % angegeben. 21,9 % der Teilnehmer haben mehrere Positionen inne.

Auch dieses Jahr waren zahlreiche Branchen unter den Teilnehmern vertreten. Der überwiegende Teil kommt allerdings mit 87,4 % aus dem Dienstleistungsbereich, 8,9 % aus dem produzierenden Gewerbe und 0,4 % lassen sich anderen Bereichen zuordnen. 3,5 % der Teilnehmer machten zu ihrer Branchenzugehörigkeit keine Angaben. Der

Position der Umfrageteilnehmer in den Institutionen



Bedeutung von Informationssicherheit und Notfallmanagement



Dienstleistungsbereich setzt sich aus 25,8 % öffentliche Verwaltung, Verteidigung und Sozialversicherung, 18,5 % Kredit- und Versicherungsgewerbe, 4,6 % Handel und 38,5 % sonstige Dienstleistung zusammen.

94,6 % der teilgenommenen Institutionen haben ihren Sitz in

Deutschland, der Rest verteilt sich auf Österreich und Schweiz. Nach der Größe analysiert, repräsentieren große Institutionen (mehr als 500 Mitarbeiter) mit 45 % und mittlere (11 – 500 Mitarbeiter) mit 41,2 % die beiden Hauptgruppen, gefolgt von den kleinen Institutionen mit nur 11,9 %.

Aufbau der Studie

Analog zur letztjährigen Studie „IT-Sicherheitsstandards und IT-Compliance 2010“ umfasst die neue Studie ebenfalls fünf Abschnitte. Nach Zielsetzung und Beschreibung des Aufbaus erfolgt ein kurzer fachlicher Exkurs zu den Themen Informati-

Gutschein
1 Ansichtsexemplar
Infodienst IT-Grundschutz



IT-Grundschutz
Informationsdienst
Für CIOs, IT-Manager und IT-Sicherheitsverantwortliche



Hintergrundwissen und Umsetzung in der Praxis

Diese Leser profitieren vom Informationsdienst IT-Grundschutz

- IT-Leiter
- Administratoren
- Sicherheitsbeauftragte
- Bezieher der IT-Grundschutzkataloge
- Datenschutzbeauftragte
- IT-Security-Officer zum schnellen Überblick und zur Weitergabe an Geschäftsleitung, IT-Leitung oder Administratoren.
- Für die Sicherheits-Verantwortlichen in Behörden und mittelständischen Unternehmen, in denen es keinen speziellen IT-Security-Officer gibt

Das Fachblatt Infodienst IT-Grundschutz informiert 8 x jährlich über aktuelle Bedrohungen und Sicherungsmöglichkeiten – stets mit Blick auf die Vorgaben in den Grundschutzkatalogen.

Lernen Sie den Informationsdienst unverbindlich kennen: Fordern Sie gleich kostenlos die aktuelle Ausgabe an!

Gratis-Anforderung

Bitte Gutschein einscannen und per Mail an vertrieb@secumedia.de oder per Fax einsenden.

FAX an: + 49 6725 5994

Bitte senden Sie mir ein Ansichtsexemplar per **Post** an neben stehende Anschrift.

Bitte senden Sie mir ein Ansichtsexemplar per **E-Mail** als PDF an folgende E-Mail-Adresse:

(Firmenstempel)

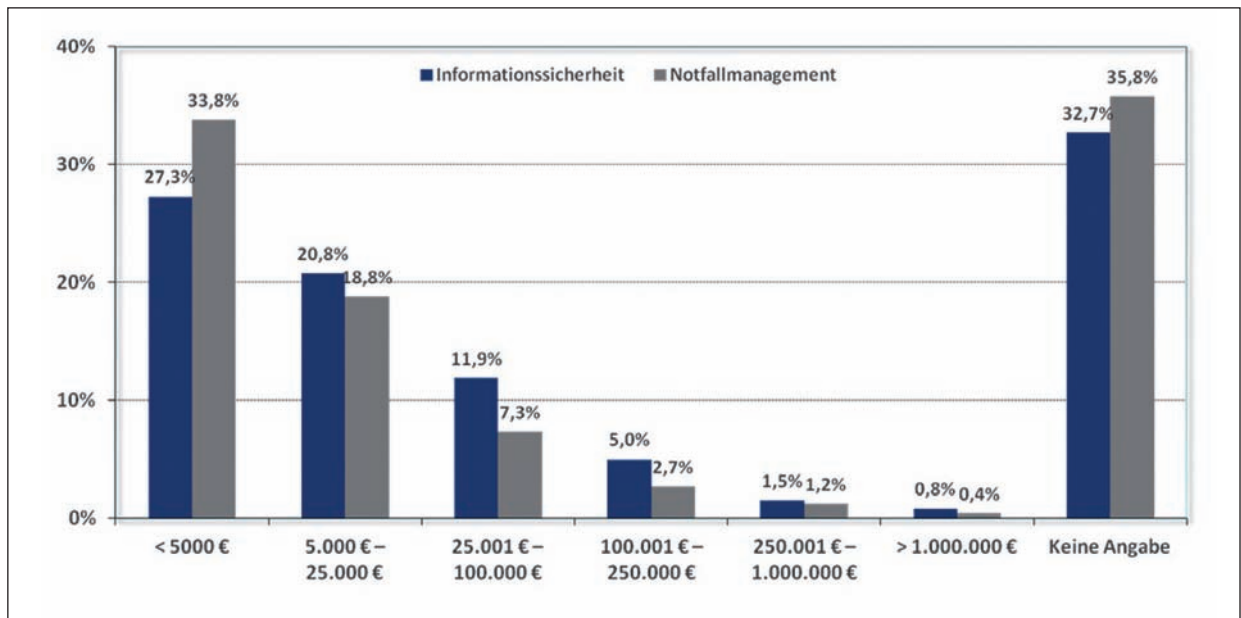
SecuMedia

Der Verlag für Sicherheits-Informationen

SecuMedia Verlags-GmbH
Postfach 12 34, 55205 Ingelheim
vertrieb@secumedia.de
Tel. +49 6725 9304-0

www.grundschutz.info

z.Hd.: _____



Informationssicherheit, Notfallmanagement sowie Standards und IT-Frameworks. Im dritten Abschnitt wird die methodische Vorgehensweise sowie die Aufbereitung und die Analyse der gewonnenen Daten erläutert. Danach folgen die Umfrageergebnisse und eine abschließende Bewertung mit einem Ausblick.

Um die großen Fragen vorweg zu nehmen: Die Bedeutung von Informationssicherheit und Notfallmanagement in der jeweiligen Institution ergibt ein sehr heterogenes Bild. 70,4 % der Teilnehmer räumen der Informationssicherheit eine sehr hohe bis hohe Bedeutung ein, dem Notfallmanagement hingegen nur 48,1 %. Bei 27,7 %

nimmt die Informationssicherheit und sogar bei nahezu der Hälfte der Befragten (46,2 %) das Notfallmanagement nur einen mittleren bis sehr niedrigen Stellenwert ein. Differenziert nach Unternehmensgröße zeigt sich überraschenderweise, dass selbst große Unternehmen (18,8 %) dem Notfallmanagement nur eine niedrige bis sehr niedrige Bedeutung zuordnen. Vergleicht man die Bedeutung der Informationssicherheit mit den Ergebnissen vom letzten Jahr, ist ein, wenn auch nur leichtes, Nachlassen der Wichtigkeit erkennbar. Ob das daran liegt, weil sich Firmen sicherer fühlen, oder weil sie von kontinuierlichen Meldungen über Sicherheitsvorfälle langsam abstumpfen ist nicht klar. Wenn man sich die nächsten Ergebnisse ansieht, dürfte eher ersteres der Fall sein. Mehr als die Hälfte geht von einer zunehmenden Bedeutung der Informationssicherheit und des Notfallmanagements aus. Ungefähr 40-45 % sind dieser Ansicht, etwa genauso viele gaben aber auch an, dass die Wichtigkeit nicht weiter steigen wird.

Studienergebnisse 2011 Informationssicherheits- und Notfallmanagement: Trends 2012

Der SecuMedia Verlag hat gemeinsam mit ibi research und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Studie über IT-Sicherheitsstandards und Notfallmanagement durchgeführt.

Die Studie zeigt den Status quo auf und ermittelt die Umsetzung relevanter IT-Absicherungs-Anforderungen sowie die Verwendung und Verbreitung von Standards bzw. IT-Frameworks.

- Bedeutung von IT-Sicherheit und Notfallmanagement
- Identifikation von Optimierungshemmnissen
- Darstellung der Probleme
- Analyse der verwendeten Standards und IT-Frameworks in Institutionen
- Probleme bei der Zertifizierung bzw. Rezertifizierung
- Analyse der vorhandenen Softwareunterstützung
- Schwierigkeiten und Herausforderungen

Ca. 80 Seiten, Preis: 295,00 €

Auslieferung voraussichtlich ab November möglich
Bestellung an vertrieb@secumedia.de

SecuMedia Verlags-GmbH
Postfach 1234 · D 55205 Ingelheim
Tel. +49 6725 9304-0 · Fax +49 6725 5994

SecuMedia
Der Verlag für
Sicherheits-Informationen



Budgets bleiben stabil

Der Großteil der Befragten hat in beiden Bereichen ein Budget von bis zu 25.000 € zur Verfügung (48,1 % Informationssicherheit, 52,6 % Notfallmanagement). Interessant ist die hohe Anzahl von Antworten mit „keine Angabe“. Hier liegt die Vermutung nahe, dass diese Teilnehmer kein Wissen über das Budget haben, zum Beispiel weil es nicht exakt definiert ist und nur bei Bedarf Investitionen getätigt werden. Möglicherweise ist die Höhe des Budgets aber auch Unternehmensinterna und damit geheim zu halten. Die Antwortmöglichkeit „keine Angabe“ wurde im Kredit- und Versicherungsgewerbe, in der öffentlichen Verwaltung, Verteidigung, Sozialversicherung sowie in großen Institutionen am häufigsten gewählt.

Wie schon bei der zukünftigen Bedeutung der Bereiche Informationssicherheit und Notfallmanagement gibt es auch bei der Budgetentwicklung zwei Hauptströmungen. Etwa 35 % gehen von einem steigenden Budget aus, wohingegen circa 40 % der Ansicht sind, dass das Budget zumindest konstant bleiben wird. Budgetkürzungen, in den letzten Jahren ein probates Mittel der Firmen zum Verbessern des Betriebsergebnisses, sind damit vom Tisch.

Insgesamt zeigt sich auch bei der qualitativen Einschätzung der Informationssicherheit und des Notfallmanagements ein sehr heterogenes Bild. 50,8 % der Umfrageteilnehmer schätzen ihre qualitative Ausgestaltung der Informationssicherheit als sehr gut bis gut ein, beim Thema Notfallmanagement sind es jedoch nur 33,5 %. Mit einer befriedigenden bis ausreichenden Qualität bewerten 40,8 % ihre Informationssicherheit und 46,2 % ihr Notfallmanagement. Eine mangelhafte qualitative Ausgestaltung attestieren 6,2 % ihrer Informationssicherheit und sogar 14,2 % ihrem Notfallmanagement.

Die Analyse nach den beiden größten Branchen (bezogen auf die Branchenzugehörigkeit der Umfrageteilnehmer) zeigt ein erstaunli-

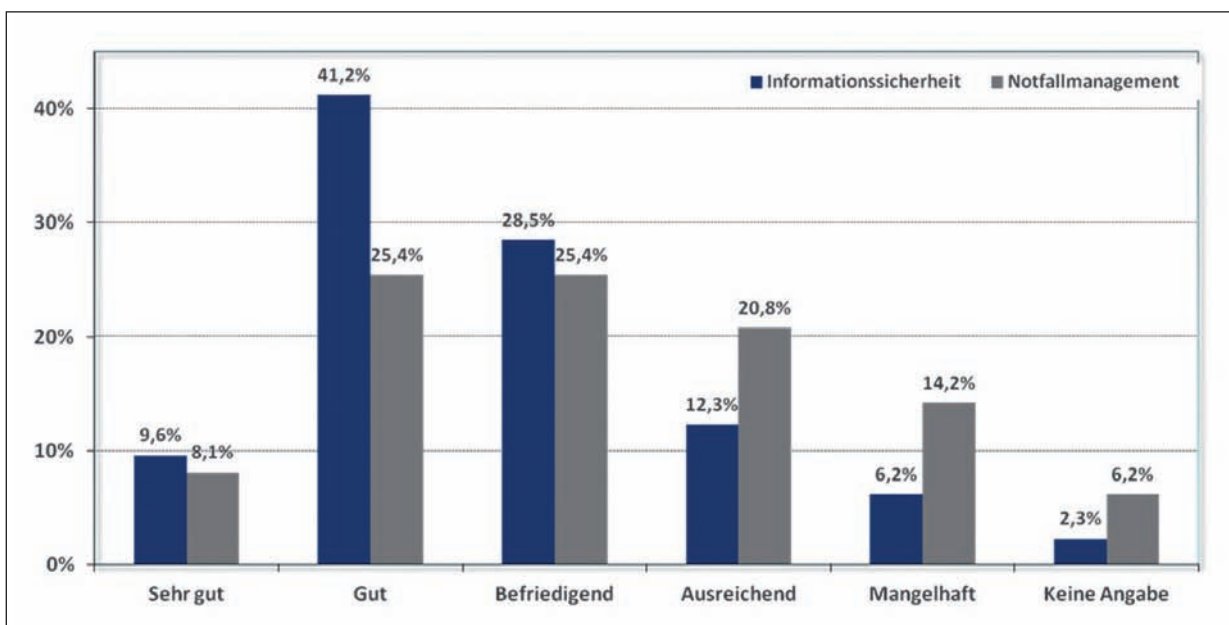
ches Ergebnis. Trotz eindeutiger gesetzlicher und aufsichtsrechtlicher Bestimmungen im Kredit- und Versicherungsgewerbe bewerten aus dieser Branche 29,2 % ihre Informationssicherheit und 37,5 % ihr Notfallmanagement nur mit befriedigend oder ausreichend. Auch in der Teilnehmergruppe öffentliche Verwaltung, Verteidigung, Sozialversicherung ist das Ergebnis eher ernüchternd. Nur 53,7 % der Befragten schätzen die Qualität ihrer Informationssicherheit mit sehr gut bis gut ein, 20,9 % mit befriedigend, 16,4 % mit ausreichend und 9 % sogar mit mangelhaft. Im Vergleich dazu sieht das Resultat zum Thema Notfallmanagement noch schlechter aus. Gerade einmal 20,9 % geben eine sehr gute bis gute Bewertung ab. Eine befriedigende Qualität wird von 26,9 % der Umfrageteilnehmer genannt, gefolgt von 23,9 % mit ausreichend und 19,4 % mit mangelhaft. 9 % wollten keine Qualitätsaussage zu ihrem Notfallmanagement abgeben.

Thesen zum Notfallmanagement

Warum das Notfallmanagement so deutlich hinter dem – ohnehin nicht optimalen – Abschneiden der Informationssicherheit zurückbleibt, ist

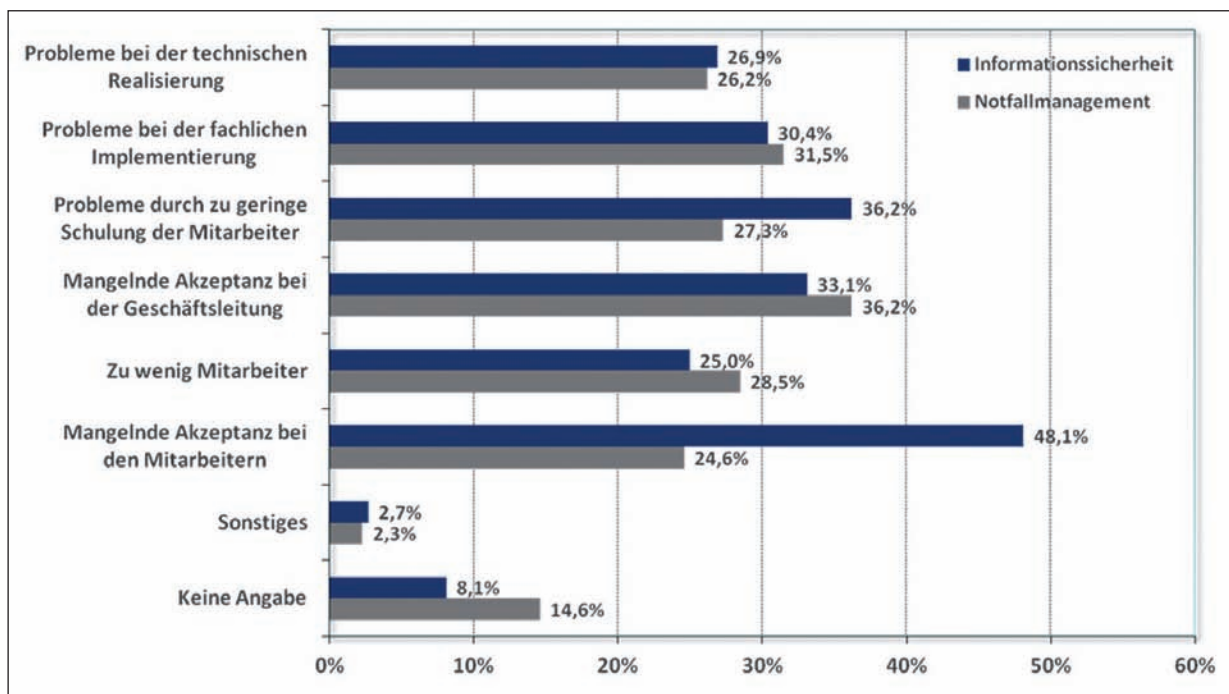
offen für Spekulationen. Eine These wäre, dass es sehr schwer ist, der Vielfalt der zugehörigen Aspekte Rechnung zu tragen. Ausfälle im IT-Umfeld sind vermutlich noch am einfachsten handhabbar, das zeigen auch weitere Detailbefragungen. Doch zum Notfallmanagement gehören auch katastrophale Ereignisse wie Feuer, Wasser oder Erdbeben. Krankheiten (Pandemien) oder Unfälle, die eine große Gruppe von Angestellten betrifft, fallen ebenfalls in den Bereich. Damit haben Firmen verständlicherweise mehr Mühe, als festzulegen, wie viel Ausfallzeit eine Anwendung verkraftet und wo die entsprechenden Backups aufbewahrt werden. Trotzdem: Je nach Branche hat Notfallmanagement mindestens den gleichen Stellenwert wie IT-Sicherheit. Um die eingehende Beschäftigung mit dem Thema wird in Zukunft niemand herum kommen.

Trotz dieser eher durchwachsenen qualitativen Einschätzungen hat das Informationssicherheits- und Notfallmanagement aber auch positive Effekte. So sind 47,3 % (Informationssicherheit) und 33,8 % (Notfallmanagement) der Ansicht, eine höhere Transparenz in ihrer Institution erreicht zu haben. Ebenso ist circa ein Drittel der Befragten der Meinung, dass beide Themen zu



Qualität von Informationssicherheit und Notfallmanagement

Größte Hindernisse
des Informationssicherheits- und
Notfallmanagements



einer Optimierung der Betriebsprozesse beigetragen haben. Während jedoch 16,9 % (Informationssicherheit) und 11,5 % (Notfallmanagement) eine Reduzierung der Komplexität der IT-Infrastruktur als positiven Effekt beobachten konnten, gibt es auch vereinzelt Meinungen, die das Gegenteil behaupten, nämlich eine Erhöhung der Komplexität der IT-Infrastruktur in ihren Institutionen. Keine Beurteilung zu positiven Effekten konnten oder wollten 19,2 % zum Informationssicherheitsmanagement und 29,2 % zum Notfallmanagement angeben.

Als Kehrseite zu den positiven Effekten sind nach wie vor auch Hindernisse im Informationssicherheits- und Notfallmanagement vorhanden. Dabei zeigt das Ergebnis, dass die mangelnde Akzeptanz bei den Mitarbeitern mit 48,1 % das am häufigsten genannte Problem in der Informationssicherheit darstellt, gefolgt von der geringen Schulung der Mitarbeiter (36,2 %) und der unzureichenden Unterstützung durch die Geschäftsleitung (33,1 %). Beim Notfallmanagement sind die größten Hindernisse die mangelnde Akzeptanz durch die Geschäftsführung (36,2%), Probleme bei der fachlichen Implementierung (31,5 %)

sowie das Fehlen von Mitarbeitern (28,5 %). Schon in der Studie letztes Jahr hatten sich viele der Befragten darüber beklagt, dass es ihnen an Rückhalt mangelt. Einerseits durch die Geschäftsführung, ohne die es schwierig ist, Sicherheitsmaßnahmen einzuführen und andererseits bei den Mitarbeitern, die IT-Sicherheit vor allem als Störfaktor bei der täglichen Arbeit betrachten.

Optimierungsbedarf

Zur Verbesserung der Situation wünscht sich gut ein Drittel in beiden Bereichen mehr Personal und mehr finanzielle Mittel. 20 % vermissen eine bessere Softwareunterstützung im Informationssicherheits- und Notfallmanagement. Nur 16,2 % (Informationssicherheit) und 17,3 % (Notfallmanagement) sind mit der aktuellen Situation zufrieden. 68,2 % der Befragten hat bereits Management-Software (nicht Anti-Virus-, Firewall-Software, etc.) im Bereich der Informationssicherheit im Einsatz oder plant dies. Im Gegensatz dazu setzen nur 42,3 % Software im Notfallmanagement ein oder haben dies vor. Die Gründe für die Nichtanwendung von Software in beiden Bereichen liegt nach Aussagen der Umfrage-

teilnehmer hauptsächlich an den zu hohen Kosten für Anschaffung und Anpassung sowie, und das ist am überraschendsten, am fehlenden Wissen über vorhandene Softwareprodukte.

Kann es sein, dass Firmen zu wenig Werbung für ihre Produkte machen? In einer anderen Frage nach den bereits eingesetzten Hilfsmitteln wurde ein sehr breites Feld an Lösungen genannt, angefangen von einer Excel-Liste über das GSTOOL bis hin zu spezialisierten Lösungen. Interesse an Produkten scheint also vorhanden zu sein, auch zeigen sich die Anwender flexibel beim Einsatz von Software. Möglicherweise halten Firmen bei Kombiprodukten auch den Aspekt des Notfallmanagements in der Beschreibung zu sehr im Hintergrund. Natürlich dürfte auch wieder die Größe des Fachgebietes eine Rolle spielen. Management von Pandemiefolgen ist so spezialisiert, dass man wirklich explizit danach suchen muss, um eine passende Lösung zu finden.

Das Thema Zertifizierung ist im Vergleich zum Umfrageergebnis des letzten Jahres nach wie vor von sehr geringem Interesse. Nur sehr

wenige Befragte planen eine Zertifizierung (6,5 % ISO/IEC 27001 auf Basis von Grundschutz, 5,8 % ISO/IEC 27001/2) oder besitzen eine Zertifizierung (6,5 % ISO/IEC 27001 auf Basis von Grundschutz, 4,2 % ISO/IEC 27001/2). Dies lässt die Vermutung zu, dass sich eine Zertifizierung nach anerkannten Sicherheitsstandards in den allermeisten Fällen unter wirtschaftlichen Aspekten gesehen anscheinend nicht lohnt. Jedoch bedeutet dies nicht, dass keine Standards und IT-Frameworks in den Institutionen eingesetzt werden. Laut aktuellem Umfrageergebnis setzen nämlich 58,1 % IT-Grundschutz, 25,4 % ISO/IEC 27001 auf Basis von Grundschutz, 16,9 % ISO/IEC 27001/2 und 10,8 % CobiT ein. Schaut man sich die Nutzung nach Firmengröße aufgeschlüsselt an, werden bei großen Unternehmen Werte von über 70 Prozent beim Einsatz von IT-Grundschutz erreicht. Das ist

ein beeindruckendes Testat für den Nutzen von IT-Grundschutz.

Schwerpunkt Notfallmanagement

Einige sehr interessante Ergebnisse liefert der Schwerpunktteil zum Thema Notfallmanagement. Nur 25,8 % aller Befragten führen jährlich oder häufiger eine Business Impact Analyse durch, 28,8 % alle 2-4 Jahre oder seltener und 20 % verzichten vollständig darauf. Ähnlich sieht es bei Risikoanalysen aus. 33,5 % haben einen jährlichen oder häufigeren Zyklus etabliert, 31,9 % nehmen Risikoanalysen nur alle 2-4 Jahre oder seltener vor und 14,2 % führen niemals Risikoanalysen durch. Dieses Ergebnis ist umso erstaunlicher, da der Risikomanagementprozess kontinuierlich ausgeführt werden sollte.

In nur knapp der Hälfte der befragten Institutionen sind offiziell Ver-

antwortliche für die Notfallvorsorge für die gesamte Organisation und für die Informations- und Kommunikationstechnologie (IKT) vorhanden. Bei etwa 40 % gibt es entweder einen informell benannten Verantwortlichen oder überhaupt keinen Zuständigen. Auch bei der Frage nach dem Vorhandensein von Verantwortlichen für die Notfallbewältigung ist die Verteilung ähnlich. Einen Krisenstab gibt es offiziell bei 45,4 %, für Sofortmaßnahmen (Retten, Löschen, Wiederaufnahme IT-Betrieb, etc.) sind Verantwortliche bei 50,4 % offiziell benannt und Notfallteams bei 33,8 %. Bei durchschnittlich 40 % sind diese nur informell oder überhaupt nicht vorhanden.

Eine spannende Frage stellte auch die Sinnhaftigkeit einer Zertifizierung nach BSI-Standard 100-4 dar. 36,2 % wünschen sich eine derartige Zertifizierung, wohingegen 28,8

Wir danken den Sponsoren der Studie IT-Notfallmanagement



FINANCE SECURITY
Technology talks business

ap=ec
applied security

consequa
continuity - security - quality

infodas
COLOGNE IT SOLUTIONS & SERVICES

ITSECURITY
Bavarian IT Security & Safety Cluster



secunet

TRIGONUM
consulting

Microsoft

UIMC
DR. VOSSBEIN GMBH & CO KG
Unternehmens- und
Informations-Management
Consultants

UIMCert
GMBH
Unternehmens- und
Informations-Management
Certification

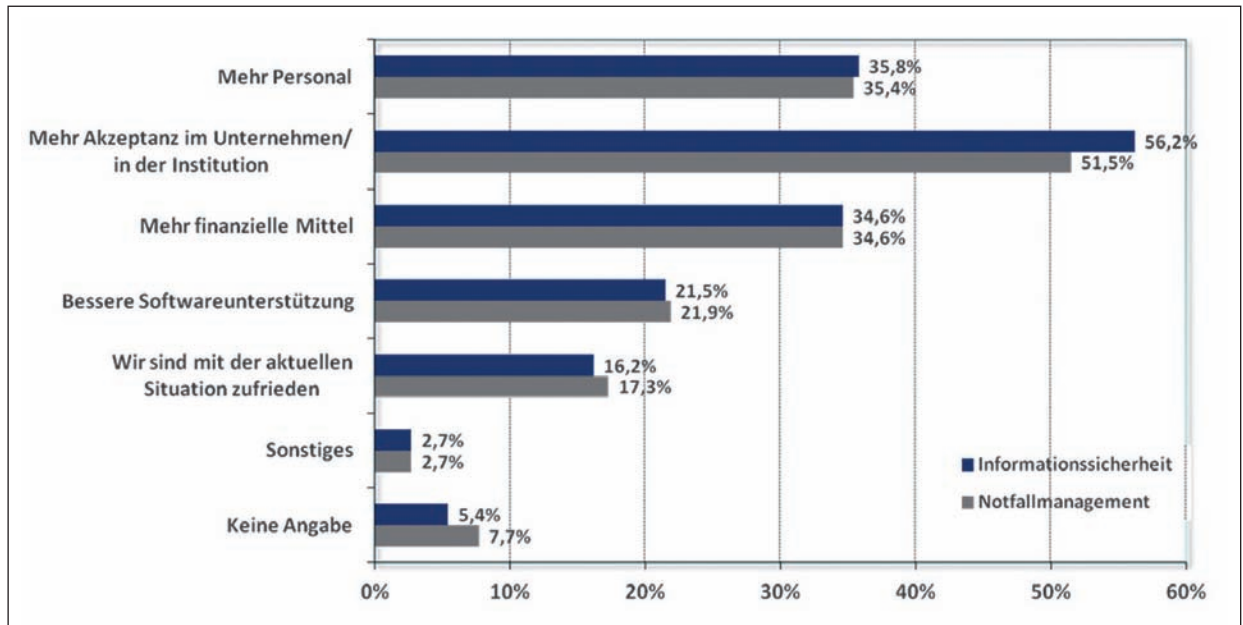
DuD
Datenschutz und Datensicherheit

**Wirtschaftsinformatik
& Management**

**VIEWEG+
TEUBNER**

itsa
Die IT-Security-Messe

Bedarfe für
Optimierung



% diese ablehnen. Soweit, so gut. Allerdings machen 35 % der Befragten keine Angabe, was an dieser Stelle verwundert. Weder rührt die Frage an Betriebsgeheimnisse noch ist sie mit zahlreichen Seiteneffekten verbunden.

Schwachpunkte bei Dokumentation

Grundsätzlich existieren bei einem Großteil der Umfrageteilnehmer strategische bzw. konzeptionelle Dokumente für das Notfallmanagement. 56,2 % haben eine Leitlinie bzw. Policy und 61,5 % besitzen ein Notfallkonzept. Jedoch sind die Vorgehensweisen nach Eintritt eines Notfalls (Ausfall Arbeitsplätze, IKT, Dienstleister/Lieferanten, Produktion, Lager und Logistik) nur bei durchschnittlich 11 % vollständig und bei durchschnittlich 14 % weitgehend dokumentiert. Die Vorgehensweise bei einem Ausfall der IKT ist unter allen Befragten am besten beschrieben, wohingegen insbesondere die Vorgehensweisen bei Ausfall des Personals (inkl. Pandemie) und der Dienstleister bzw. Lieferanten bei einem Großteil der Umfrageteilnehmer (31 %) überhaupt nicht dokumentiert sind. Hinzu kommt auch noch die Tatsache, dass nur bei durchschnittlich

17 % die Vorgehensweisen jährlich oder häufiger aktualisiert werden. In dieser Gruppe wird von den meisten (31,5 %) das Verfahren für den Ausfall der IKT jährlich oder häufiger einem Review unterzogen. Bei etwa durchschnittlich 20 % werden keine der Vorgehensweisen jemals aktualisiert.

Ergebnisse im Detail

Die ausführlichen Umfrageresultate werden offiziell auf dem BSI-Grundschutztag am XX.10.2011 im Rahmen der Sicherheitsmesse it-sa in Nürnberg vorgestellt. Sowohl der hohe Rücklauf an Fragebögen als auch die hohe Qualität der Datensätze zeigen, dass Institutionen ein großes Interesse an den Themenfeldern IT-Sicherheit und Notfallmanagement haben und ihre Situation mit denen anderer Institutionen vergleichen und Anregungen umsetzen wollen. Wie im letzten Jahr ist die mangelnde Akzeptanz seitens der Mitarbeiter der Hauptgrund für die mangelnde Umsetzung. Sichtbare Unterstützung der Sicherheitsmaßnahmen durch die Geschäftsleitung und eine durchdachte Integration in die Arbeitsprozesse dürften die Trumpfkarten sein, um das Problem anzugehen. Doch die Unterstützung durch die Geschäftsleitung

wird von den Befragten an zweiter Stelle der Hemmnisse genannt. Sicherheit ist wohl doch noch nicht Chefsache. Ebenfalls wie im letzten Jahr lässt die geringe Zahl der Zertifizierungen aufhorchen, obwohl drei Viertel der Befragten nach IT-Grundschutz handeln. Die Hürden scheinen zu hoch zu sein, damit sich Institutionen aufmachen, ihre tägliche Sicherheitspraxis mit einem Zertifikat bestätigen zu lassen. Zertifizierte IT-Sicherheit kann geldwerte Vorteile im Umgang mit Kunden und durch eine generell höhere Verfügbarkeit bringen, es scheint aber noch an Anreizen zu mangeln, um die Institutionen – unabhängig von der Unternehmensgröße – davon zu überzeugen. ■

Impressum

Sonderdruck aus Informationsdienst IT-Grundschutz, Ausgabe 7/11 aus 2011 zur Studie „IT-Sicherheitsstandards und Notfallmanagement 2011/2012“ für FINANCE SECURITY

Web: www.grundschutz.info

Redaktion: Elmar Török

Satz/Druckvorstufe
BLACKART Werbestudio
Schnaas und Schweitzer
Stromberger Str. 47, 55413 Weiler

Druck:
Hofmann Druck Nürnberg GmbH & Co. KG, Emmericher Straße 10, 90411 Nürnberg

Printed in Germany

Titelbild: iStockphoto/Norebbo