

Der Stand der Dinge, schwarz auf weiß

Umfrage „IT-Sicherheitsstandards und IT-Compliance 2010“

Elmar Török, bits+bites

Die Umfrageergebnisse sind da. Mehrere Hundert Anwender aus der Praxis haben an der Studie zu IT-Sicherheitsstandards und IT-Compliance 2010 teilgenommen. Auch wenn viele Daten kaum überraschen, ist die Bestätigung von Trends und Einschätzungen aus der Redaktion interessant. Und einige Überraschungen gibt es auch zu vermelden.

Im Mai startete der SecuMedia Verlag zusammen mit ibi research und dem Bundesamt für Sicherheit in der Informationstechnik eine Umfrage, die sich explizit mit IT-Sicherheitsstandards wie dem IT-Grundschutz des BSI und mit IT-Compliance befasste. IT-Grundschutz nach BSI wird in Deutschland und im Ausland von zahlreichen Firmen und Organisationen für die Sicherung von IT-Systemen angewandt. Zu den relevanten Themen gehörten unter anderem, wie die Umsetzung von IT-Grundschutz und Compliance vor Ort im Detail aussieht, welche Wünsche die Anwender haben und wie sie den IT-Grundschutz im Vergleich zu anderen IT-Sicherheitsstandards sehen.

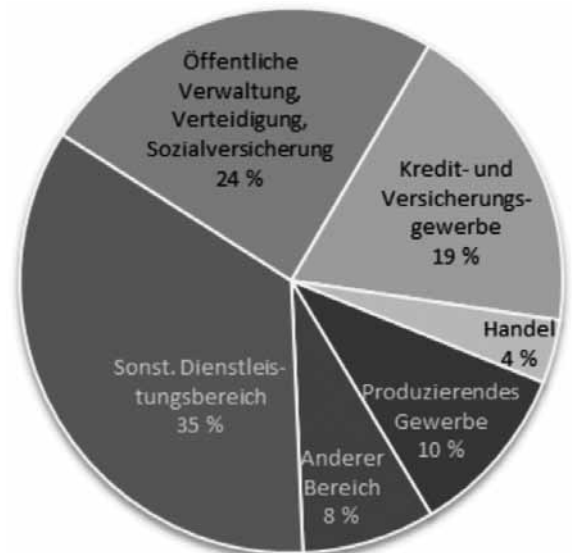
Die Studie verfolgte die Ziele, den Status quo und Entwicklungstendenzen hinsichtlich IT-Sicherheitsstandards und IT-Compliance aufzuzeigen. Dazu wurde die Umsetzung relevanter IT-Compliance Anforderungen sowie die Verwendung und Verbreitung von Standards beziehungsweise IT-Frameworks ermittelt. Zudem sollten Verbesserungspotenziale und Wünsche vonseiten der Anwender ermittelt und Schwächen von Softwarelösungen dargestellt werden. Das BSI unterstützte die Studie durch Vorschläge für die Formulierung der Fragen und eigene Themen.

Hohe Akzeptanz durch Anwender

Die Akzeptanz und Teilnahmefreudigkeit übertraf alle Erwartungen. Ausgefüllt wurden 565 Fragebögen, wobei die Fragen zu IT-Compliance optional waren. Nach Plausibilitätskontrollen blieben von den 565 Datensätzen letztendlich 294 valide Datensätze übrig. Zum größten Teil stammen die Antworten von IT-Mitarbeitern. Dabei machen (IT-) Sicherheitsbeauftragte, (IT-) Security Manager und (IT-) Sicherheitsmanager mit 48 % den größten Anteil aus. 25 % der Umfrageteilnehmer sind für mehrere Bereiche in der Institution verantwortlich. Zahlreiche Branchen waren vertreten: 82 % sind dem Dienstleistungsbereich, 10 % dem produzierenden Gewerbe und 8 % anderen Bereichen zuzuordnen.

Der Dienstleistungsbereich teilt sich weiterhin auf in 24 % öffentliche Verwaltung, Verteidigung und Sozialversicherung, 19 % Kredit- und Versicherungsgewerbe, 4 % Handel und 35 % sonstige Dienstleistung. Leider sind kleine Institutionen mit 13 % deutlich unterrepräsentiert. Allerdings dürfte der IT-Grundschutz in diesen Firmen aufgrund seiner Komplexität seltener eingesetzt werden, was sich direkt in den Umfrageteilnehmern widerspiegelt.

Auffallend ist, dass nur 15 % der kleinen Institutionen einen (IT-) Sicherheitsbeauftragten, (IT-) Security Manager oder einen (IT-) Sicherheitsmanager haben. Im Gegensatz hierzu setzen 42 % der mittelgroßen und 63 % der großen Institutionen derartige Fachkräfte ein. Wie zu erwarten war, sind überwiegend Institutionen mit Sitz in Deutschland vertreten, die Beteiligung der Nachbarländer war mit 8 % (Österreich, Schweiz, Italien, Belgien, Japan, Luxemburg, Niederlande und Norwegen) von untergeordneter Bedeutung. Dafür besitzen immerhin 28 % der Institutionen



Branchenzugehörigkeit der Institutionen
Basis: 291 Studienteilnehmer / © ibi research

Standorte im Ausland und müssen daher teilweise Gesetze und Normen mehrerer Länder befolgen.

Aufbau der Studie

Die Studie umfasst fünf Abschnitte. Der erste Abschnitt beschreibt die Ziele und den Aufbau der Studie. Der zweite Abschnitt geht auf den fachlichen Hintergrund der Bereiche IT-Compliance, IT-Sicherheit sowie Standards und IT-Frameworks ein. Im dritten Abschnitt folgt die Beschreibung der methodischen Vorgehensweise zur Planung und

Durchführung der Studie. Insbesondere werden Design und Aufbau des Fragebogens, die Durchführung der Befragung und die Auswahl und Aufbereitung der Daten beleuchtet. Der darauffolgende vierte Abschnitt diskutiert die Ergebnisse der Umfrage. Zum Schluss erfolgen eine abschließende Bewertung und ein Ausblick. Die Teilnahme war auch anonym möglich, aber nur Studienteilnehmer, die ihre E-Mail Adresse angaben, erhalten die kompletten Studienergebnisse.

Insgesamt legten die Befragten den Stellenwert der IT-Sicherheit sehr hoch an. In 38 % der Institutionen ist er sehr hoch und in weiteren 37 % hoch. Demzufolge sahen 18 % der Institutionen die Bedeutung IT-Sicherheit als mittlere und 7 % sogar als niedrige bis sehr niedrige Priorität. Das ist im Angesicht der heute fast täglich bekannt werdenden neuen Sicherheitslücken in Anwendungsprogrammen, Betriebssystemen und Web-Diensten erstaunlich, die Schäden durch Cybercrime erreichen pro betroffenes Unternehmen mittlerweile sechsstelligen Summen. Im Gegensatz hierzu ist die Bedeutung von IT-Compliance in 21 % der Insti-

tutionen sehr hoch und in 38 % hoch. 25 % der Institutionen messen der IT-Compliance eine mittlere und 16 % eine niedrige bis sehr niedrige Bedeutung bei. Weil nicht alle Firmen IT-Compliance im gleichen Umfang umsetzen müssen, sind die niedrigeren Werte erklärbar. Allerdings ist IT-Compliance oft ein nützliches Vehikel, um die IT-Sicherheit insgesamt zu steigern, daher sollten auch Institutionen, die mit „Niedrig“ bis „Sehr niedrig“ geantwortet hatten, ihre Haltung überdenken.

Obwohl die Bedeutung von IT-Sicherheit und IT-Compliance generell bereits auf einem relativ hohen Niveau ist, gehen ca. 68 % davon aus, dass diese in Zukunft noch steigen wird. Gleich bleibende Bedeutung prognostizieren 28 % für IT-Sicherheit und 33 % für IT-Compliance. Wenig überraschend ist, dass kaum jemand mit sinkender Bedeutung rechnet. Erstaunliches hingegen ergibt die Detailbetrachtung nach Unternehmensgröße. Sie zeigt, dass bei kleinen Institutionen IT-Sicherheit zu 58 % eine sehr hohe Bedeutung einnimmt. Dagegen kommt IT-Sicherheit in 35 % der mittelgroßen Institutionen eine sehr hohe und nur in 15 % der gro-

ßen Institutionen eine sehr hohe Bedeutung zu. Auch bei der IT-Compliance unterscheiden sich groß und klein drastisch, das ist jedoch durch die verschiedene Relevanz von gesetzlichen Bestimmungen in Abhängigkeit von der Unternehmensgröße leicht erklärbar.

Spekulationen über geringe Bedeutung

Woher der Umstand rührt, dass nur eine relativ geringe Zahl der Befragten in großen Unternehmen der IT-Sicherheit die Wichtigkeit „Sehr hoch“ einräumt, lädt zu Spekulationen ein. Möglicherweise glauben sich diese Firmen aufgrund Ihrer personellen und technischen Ressourcen bereits so gut geschützt, dass sie hier weniger Handlungsbedarf sehen. Andererseits sind auch in großen Firmen relativ wenige Mitarbeiter im Bereich IT-Sicherheit beschäftigt. Dort arbeiten zu 80 % keine bis maximal fünf Arbeitnehmer (IT-Compliance 81 %). Vor dem Hintergrund der Tatsache, dass 42 % der Studienteilnehmer aus großen Institutionen stammen, ist diese geringe Mitarbeiterzahl auffallend. Trotz der überwiegend

Wir danken den Sponsoren der Studie IT-Sicherheitsstandards und IT-Compliance

secunet

ap=ec
applied security

infodas
Global IT Solutions & Services

ITSECURITY
Bavarian IT Security & Safety Cluster

TRIGONUM
consulting

DB3

intersoft: consulting
services

JAKOB SOFTWARE

UIMCert
GmbH
Unternehmens- und
Informations-Management
Certification

DFN
CERT

Microsoft

seed forensics

UIMC
Dr. Volker Giesh & Co KG
Unternehmens- und
Informations-Management
Consultants

FINANCE SECURITY

securon
a security solutions

Tele-Consulting **TC**
security | networking | training gmbh

SONICWALL

VALIDD
DIGITAL FORENSICS

geringen Mitarbeiterzahl werden in den meisten Institutionen (71 %) IT-Sicherheitsziele definiert. Lediglich 8 % geben an, keine Sicherheitsziele definiert zu haben oder definieren zu wollen.

Ein heikler Punkt im Vorfeld war die Frage, ob man möglichen Folgen einer Missachtung von IT-Sicherheits- und Compliancevorgaben nachgehen sollte. Nach einigen Diskussionen wurde die Frage aufgenommen. 267 gültige Antworten zeigen, dass das Thema in der Praxis nüchtern gesehen und offen behandelt wird. Überwiegend führen solche Fälle zu einer Belehrung durch den Vorgesetzten (71 % IT-Sicherheit, 59 % IT-Compliance). Schon als zweite Konsequenz wurden aber Anpassungen der Prozesse (48 % IT-Sicherheit, 46 % IT-Compliance) genannt, um derartige Verstöße zukünftig zu verhindern. So werden auch negative Vorkommnisse genutzt, um die Sicherheitslage insgesamt zu optimieren. Rechtliche Konsequenzen leiten 16 % der Institutionen bei IT-Sicherheits- und 13 % bei IT-Compliance-Verstößen ein. Bedenklich ist hingegen, dass im Bereich IT-Sicherheit 14 % und im Bereich IT-Compliance 19 % der Studienteilnehmer die Konsequenzen einer Missachtung der Compliance- und Sicherheitsvorgaben nicht bekannt sind. Begründet wurde dies unter anderem, damit, dass eine Missachtung nicht geahndet wird, zum Beispiel um den Betriebsfrieden nicht zu stören oder das noch keine Missachtung bekannt wurde.

Hindernisse bei der Optimierung

Um den steigenden Anforderungen gegenwärtig und künftig gerecht zu werden, benötigen die Fachbereiche neben mehr finanziellen Mitteln auch mehr und qualifizierteres Personal. Knapp 45 % der Befragten klagten über den Mangel an Mitarbeitern in der IT-Sicherheit, was bei einer Personaldecke von meist nur fünf Mitarbeitern nicht erstaunlich ist. Übrigens würden auch 70 % der teilnehmenden Institutionen die Einführung einer Qualifikation „Qualified IT-Grundschutz Expert (BSI)“ als sinnvoll erachten. Als weiteres Optimierungshemmnis wird eine bessere Softwareunterstützung (19 % IT-Sicherheit, 22 % IT-Compliance) gesehen. Nur circa ein Fünftel ist mit der aktuellen Situation zufrieden. Werden Missstände aufgedeckt, zeigten sich viele Befragte mit der Art der Abhilfe unzufrieden. Obwohl es sich bei den Anforderungen aus dem Gebiet der IT-Compliance um die Umsetzung von IT-spezifischen Gesetzen und Regularien handelt, werden sicherheitsrelevante Anpassungen aus dem IT-Bereich in den Fachabteilungen schneller (sehr schnell 8 %, schnell 34 %) umgesetzt, als im Bereich IT-Compliance (sehr schnell 5 %, schnell 26 %). Im überwiegenden Teil der befragten Institutionen (37 % IT-Sicherheit, 45 % IT-Compliance) ist die Realisierungsgeschwindigkeit mittelmäßig. Großer Handlungsbedarf besteht bei circa 21 % der Institutionen, die Anforderungen langsam bis sehr langsam umsetzen.

Security Without Borders

- Award-winning email security & encryption
- Industry-leading comprehensive managed file transfer
- Policy-based file attachment management
- Start-to-finish enterprise visibility into every business interaction

Special offers and white paper downloads available for a limited time: www.axway.com/itsa



Axway

Kurfürstendamm 119
10711 Berlin

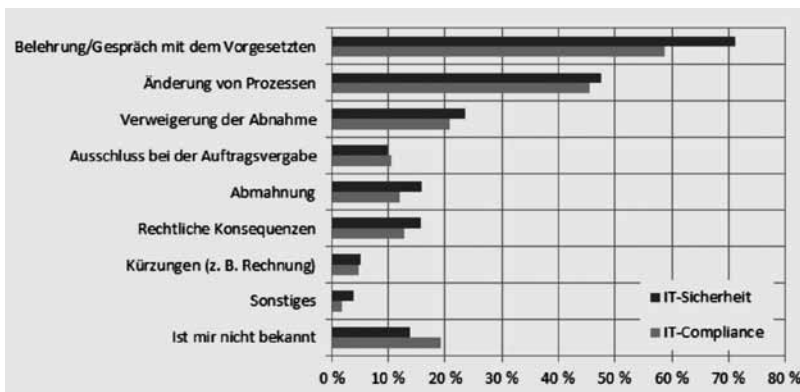
Tel. +49 30 8901-00
Fax +49 30 8901-0102

contactgermany@axway.com
www.axway.de



Wir freuen uns auf Ihren Besuch am Axway-Stand

Halle 12 Stand #517



Vorgehensweise bei Missachtung

Basis: Ø 267 Studienteilnehmer Mehrfachnennung möglich / © ibi research

Ein Grund hierfür mag in der Akzeptanz der Fachabteilungen gegenüber laufenden Anpassungen liegen. In der Mehrzahl ist sie befriedigend, ausreichend oder mangelhaft. Da die Impulse für die Weiterentwicklung meist nicht von (IT-) Governance Managern oder Nicht IT-Mitarbeitern ausgehen, kann geschlussfolgert werden, dass die Fachabteilungen nur unzureichend in die Anpassungsprozesse eingebunden werden. Durch Verbesserung des Business-IT-Alignments und der damit verbundenen kontinuierlichen Einbindung der Fachabteilungen könnte die Akzeptanz vermutlich gesteigert werden

Das größte Problem hinsichtlich des IT-Sicherheit und IT-Compliance Managements scheint mit über der Hälfte der Nennungen

die mangelnde Akzeptanz seitens der Mitarbeiter zu sein. Auch die Unterstützung durch die Geschäftsführung, den Vorstand oder die Amtsleitung ist eindeutig zu gering, selbst wenn diese für IT-Sicherheit bzw. IT-Compliance zuständig sind. Daher nannten 37 % der Studienteilnehmer die fehlende Akzeptanz der Geschäftsleitung als zweites Hauptproblem. Weiterhin genannt wurden Probleme bei der Schulung der Mitarbeiter, bei der fachlichen Implementierung und bei der technischen Realisierung.

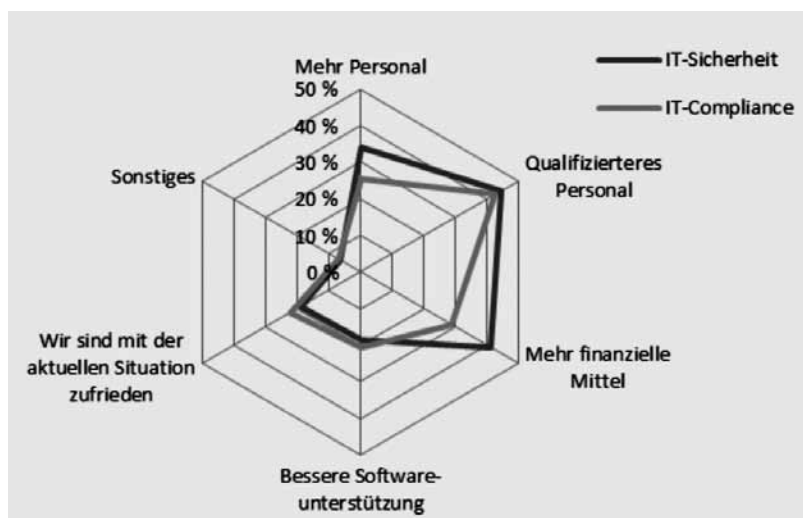
Ärger mit Software

Viele Institutionen lassen sich von Software bei der Umsetzung von Gesetzen/Regularien und Standards/IT-Frameworks unterstützen.

Die meisten arbeiten mit fremdentwickelten Produkten, nur annähernd 13 % wenden eigenentwickelte Software an. Bei der IT-Sicherheit verzichten gut 30 Prozent völlig auf Softwareunterstützung, bei IT-Compliance sogar fast die Hälfte. Das kann an den zahlreichen Mängeln liegen, die die Befragten offen angeben. Institutionen, die keine Standardsoftware einsetzen, führen als Hauptgrund zu hohe Anschaffungs- und Anpassungskosten an (53 % IT-Sicherheit, 55 % IT-Compliance). Ferner werden fehlende Anbindungsmöglichkeiten an vorhandene IT-Systeme (36 % IT-Sicherheit, 32 % IT-Compliance) und ein zu geringer Funktionsumfang (20 % IT-Sicherheit, 19 % IT-Compliance) bemängelt.

Von einigen Teilnehmern wurde als weiteres Hindernis die Weiterentwicklung eigener Prozesse, die nur mit Aufwand in die Standardsoftware eingearbeitet werden können, genannt. Weil heterogene IT-Umgebungen meist historisch gewachsen sind, lassen sie sich in Standardsoftware kaum effizient und mit einem angemessenen Kosten-/Nutzenverhältnis abbilden. Oft werden daher nur einzelne Bausteine der Software eingesetzt.

Ein eigenes Kapitel stellte die Softwareunterstützung zur Zertifizierung dar. Hier verzichtet der Großteil der Institutionen (64 %) bisher auf jegliche Hilfe durch Software bei der Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz. 31 % greifen zur Unterstützung auf Standardsoftware zurück, nur 5 % nutzen selbst entwickelte Software. 20 % der Institutionen hatten Probleme mit der Aufgabenbewältigung. Die aufgetretenen Hindernisse sind sehr vielschichtig und reichen von technischen Problemen bezüglich des Zugriffs bis hin zu Problemen mit dem Dokumentenmanagement. Eines der spannendsten Ergebnisse der Studie waren die Zahlen über die tatsächlich zertifizierten und rezertifizierten Institutionen. Trotz der hohen Beteiligung von Lesern des Infodienst IT-Grundschutz und des



Optimierungshemmnisse

Basis: Ø 282 Studienteilnehmer Mehrfachnennung möglich / © ibi research

BSI Newsletters, was ja auf eine aktive Beschäftigung mit dem Thema hinweist, sind nur sehr wenige Institutionen nach ISO 27001 auf Basis von IT-Grundschutz und ISO/IEC 27001 zertifiziert. Gerade einmal 5 % haben jeweils den Prozess abgeschlossen, und in etwa die gleiche Menge plant eine Zertifizierung. Dennoch zeigt die Studie, dass sehr viele Institutionen nach den Vorgaben dieser Standards handeln. Nach IT-Grundschutz sind dies beispielsweise annähernd 80 %. Das IT-Framework CobiT wird hingegen nur von knapp 20 % angewendet. Natürlich gibt es Unterschiede bezogen auf die Firmengröße, aber selbst die am häufigsten zertifizierten großen Institutionen kommen lediglich auf 11 % nach ISO 27001 auf Basis von IT-Grundschutz und 8 % nach ISO/IEC 27001. Das scheint auf eine generelle Akzeptanz der Maßnahmen und des Konzepts des IT-Grundschutzes hinzudeuten, aber auf zu hohe Hürden beim Zertifizierungsprozess.

Lange Laufzeit

Der Einsatz von IT-Grundschutz beruht überwiegend (63 %) auf Vorgaben durch Gesetze oder Regularien. Seit der Einführung des IT-Grundschutzes im Jahr 1994 erfuh dieser bei den Studienteilnehmern ein stetiges Wachstum. Signifikant sind die Anstiege in den Jahren 2004 bis 2009. Hier konnte der IT-Grundschutz seine Verbreitung im deutschsprachigen Raum weiter ausbauen. Ein überzeugendes Argument für den Grundschutz ist die Verbesserung der Sicherheitslage. Institutionen profitieren am meisten von der Anwendung des IT-Grundschutzes (93 %). 89 % konnten durch die Umsetzung von ISO/IEC 27001/2 die Sicherheitslage verbessern, bei CobiT verbesserte sich die Lage dagegen nur bei knapp jedem Dritten. Dabei gilt es selbstverständlich zu berücksichtigen, dass CobiT kein reines Framework für IT-Sicherheit ist.

Obwohl der Sicherheitsgewinn durch IT-Grundschutz also beträchtlich ist, zögern die Unternehmen und Behörden bei der Rezertifizierung. Bisher hat sich nur ein geringer Prozentsatz für eine Rezertifizierung entschieden, 86 % dagegen. Die Gründe sind überwiegend fehlende Ressourcen (27 %), kein erwiesener Nutzen (17 %) sowie zu hohe Kosten (14 %). Ressourcen und Kosten spiegeln sich auch in den detaillierten Gründen für die Verweigerung wieder. Wengleich 76 % der Institutionen für die Rezertifizierung weniger Zeit benötigten als für die Erstzertifizierung, sind dennoch 85 % der Meinung, dass eine Rezertifizierung zu zeitaufwendig ist.

Abschließende Betrachtung

Die ausführlichen Umfrageresultate werden offiziell auf dem BSI-Grundschutztag am 20.10.2010 im Rahmen der Sicherheitsmesse it-sa in Nürnberg vorgestellt und dort im Auditorium, einem offenen Forum in der Messehalle, diskutiert. Aber schon in dieser gedrängten Zusammenfassung werden verschiedene Brennpunkte sichtbar. 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 IT-Compliance haben und ihre Situation mit denen anderer Institutionen vergleichen und Anregungen umsetzen wollen. Nach wie vor fehlen finanzielle Mittel und qualifiziertes Personal, um alle Maßgaben korrekt umzusetzen, so dass sich die Situation hinsichtlich der Sicherheitslage in Institutionen in Zukunft noch verschärfen wird. Bestrebungen des IT-Managements, IT-Sicherheitsstandards und IT-Compliance besser umzusetzen, sind vorhanden. Erschwert wird der Prozess durch die mangelnde Akzeptanz seitens der Mitarbeiter. Diese könnten behoben werden, wenn die Geschäfts-

leitung den Mitarbeitern entsprechende Anweisungen geben und ausreichend Ressourcen zur Verfügung stellen würde. Obwohl schon viele Institutionen nach den Vorgaben von ISO 27001 auf Basis von IT-Grundschutz und ISO/IEC 27001 handeln, fordert die Mehrzahl der Studienteilnehmer die Einführung eines „Qualified IT-Grundschutz Expert (BSI)“. Davon versprechen sich die Befragten eine weitere Qualifizierung, die das eigene und auch externes Personal bei der Umsetzung des IT-Grundschutzes unterstützt.

Zusätzlich sollten Anreize geschaffen werden, um die Institutionen für eine Zertifizierung zu gewinnen. Dabei sind auch kleine Institutionen einzubeziehen. Damit sich zertifizierte Institutionen anschließend rezertifizieren lassen, sind Regularien zu erstellen, die es den Institutionen ermöglichen eine Rezertifizierung mit deutlich weniger Zeitaufwand als bisher, geringeren Kosten und mit einer geringeren Störung des Betriebsablaufs durchzuführen. ■

Vollständige Studie erhältlich

Ob zur Abklärung des eigenen Standpunkts gegenüber anderer Firmen oder als Argumentationshilfe bei Security-Projekten: Eine solide Datenbasis mit zahlreichen Fakten über IT-Sicherheitsstandards und IT-Compliance ist eine unbezahlbare Hilfe für alle, die professionell mit Sicherheit zu tun haben.

Sie finden die Studie mit den kompletten Ergebnissen für 295 € + MwSt. unter <http://buchshop.secumedia.de> oder bei ibi research www.ibi.de