research
an der Universität
Regensburg

Dr. Stefan Kronschnabl
Stephan Weber
Christian Dirnberger
Elmar Török
Isabel Münch

IT-Sicherheitsstandards und IT-Compliance 2010

Befragung zu Status quo, Trends und zukünftigen Anforderungen

Studie

IT-Sicherheitsstandards und IT-Compliance 2010

Autoren

Dr. Stefan Kronschnabl
Stephan Weber
Christian Dirnberger

Co-Autoren

Elmar Török
Isabel Münch

ibi research an der Universität Regensburg GmbH

IT·Grundschutz Informationsdienst

Bundesamt für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

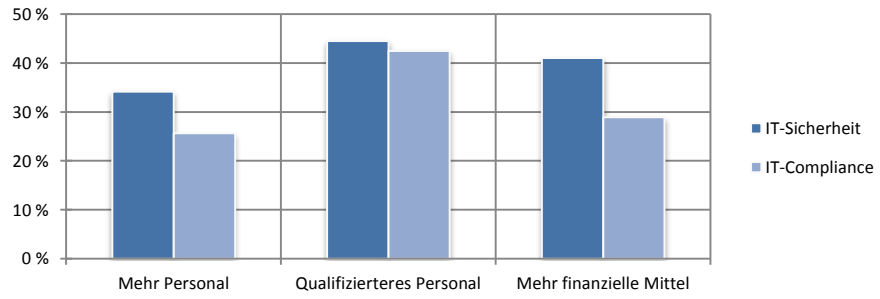
Management Summary

Hohe bis sehr hohe Bedeutung von IT-Sicherheit und IT-Compliance

Die Studie IT-Sicherheitsstandards und IT-Compliance wurde 2010 zum ersten Mal durchgeführt und zählt mit 294 gültigen Datensätzen zu einer der größten ihrer Art. Dabei wurde die Bedeutung von IT-Sicherheit von 75 % und die Bedeutung von IT-Compliance von 59 % der Institutionen als hoch bis sehr hoch bewertet. Obwohl die Mehrheit der Studienteilnehmer künftig in den Bereichen IT-Sicherheit und IT-Compliance von einer steigenden Bedeutung ausgehen, sind derzeit in der Mehrzahl der Institutionen maximal fünf Mitarbeiter in diesen Bereichen beschäftigt. Neben mehr finanziellen Mitteln ist damit auch mehr qualifiziertes Personal erforderlich (siehe Abbildung 1).

Hauptoptimierungshemmnisse qualifiziertes Personal und finanzielle Mittel

Abbildung 1: Hauptoptimierungshemmnisse in den Bereichen IT-Sicherheit und IT-Compliance



Basis: Ø 282 Studienteilnehmer *Mehrfachnennung möglich*

© ibi research

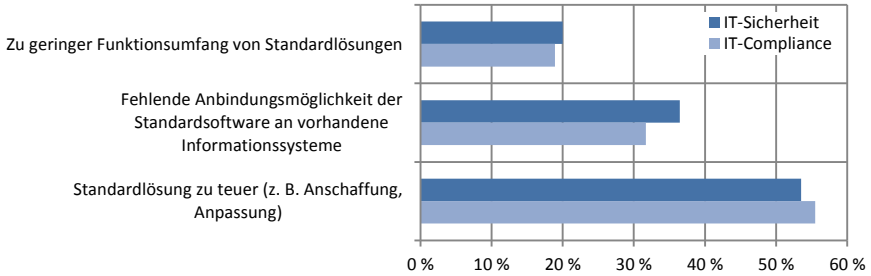
Qualitative Umsetzung nicht im Einklang mit hoher Bedeutung

Eklatant ist, dass die Bereiche IT-Sicherheit und IT-Compliance nur in durchschnittlich 7 % der Unternehmen sehr gut umgesetzt sind. Dies zeigt eine Diskrepanz zwischen der Bedeutung und der Umsetzungsqualität in den Institutionen.

Zu geringer Funktionsumfang von Standardsoftware

Zur Umsetzung von Gesetzen/Regularien und Standards/IT-Frameworks bedienen sich die meisten Institutionen fremdentwickelter Software und gewinnen dadurch signifikante Effektivitäts- und Effizienzvorteile. 41 % setzen noch keine Software ein. Diese Gruppe fordert mehr Funktionsumfang und Bedienerfreundlichkeit von Softwarelösungen sowie bessere Anbindungs- und Anpassungsmöglichkeiten an betriebliche Prozesse. Zudem wird ein niedrigerer Preis gefordert (siehe Abbildung 2).

Abbildung 2: Hauptmängel von Standardsoftware



Basis: Ø 167 Studienteilnehmer *Mehrfachnennung möglich*

© ibi research

Zertifizierungen kaum vorhanden

Insgesamt lassen sich nur sehr wenige Institutionen nach ISO 27001 auf Basis von IT-Grundschutz oder nach ISO/IEC 27001 zertifizieren. Gut die Hälfte der Studienteilnehmer greift zur Vorbereitung der Zertifizierung auf externe Partner zurück. 80 % waren mit diesen Partnern zufrieden.

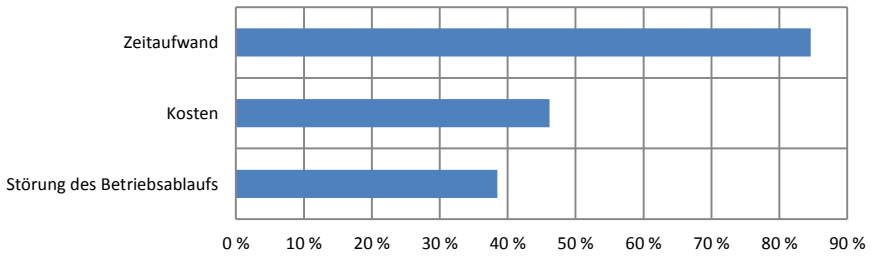
GSTOOL am weitesten verbreitet

Durch den Einsatz von Software zur Zertifizierung nach ISO/IEC 27001 erzielen die Institutionen im Allgemeinen eine bessere Umsetzungsqualität der Maßnahmen und Kontrollziele. Am häufigsten wird das GSTOOL des Bundesamtes für Sicherheit in der Informationstechnik eingesetzt. Trotzdem gaben 22 % der Befragten an, mit dieser Software Probleme zu haben.

Zeitaufwand für Rezertifizierung noch zu hoch

Institutionen, die bereits eine Rezertifizierung durchgeführt haben, verzeichnen einen geringeren Zeitaufwand gegenüber der Erstzertifizierung. Allerdings führten bisher 86 % noch keine Rezertifizierung durch und mehr als zwei Drittel wollen das auch künftig nicht tun. Hauptgründe hierfür sind nach Meinung der Studienteilnehmer der immer noch zu hohe Zeitaufwand, die anfallenden Kosten sowie die Störung des Betriebsablaufs.

Abbildung 3: Hauptpunkte, die bei der Rezertifizierung störten



Basis: 13 Studienteilnehmer *Mehrfachnennung möglich*

© ibi research

Datenschutzgesetze für mehr als 50 % der Teilnehmer ausreichend

Positive Effekte des IT-Compliance Managements sind eine höhere Transparenz, die Optimierung von Betriebsprozessen und die Reduzierung der Komplexität der IT-Infrastruktur. Mehr als die Hälfte ist der Meinung, dass die aktuellen gesetzlichen Regelungen bezüglich des Datenschutzes inhaltlich ausreichend sind. Bei fast 70 % der Studienteilnehmer nimmt die Umsetzung der Datenschutzgesetze die meiste Zeit in Anspruch. Auffallend ist, dass nur ein Fünftel der Studienteilnehmer umfassende Datenschutzaudits gemäß § 9 des Bundesdatenschutzgesetzes (BDSG) durchgeführt hat. Die Umsetzung der Anforderungen des BDSG wird dennoch als qualitativ gut bewertet.