Stand der IT-Sicherheit in Österreich

[Bedeutung und Umsetzung von Security Policies aus der Sicht der EDV-Anwender]

KURZFASSUNG

Autor: © Hans G. Zeger 1998

Durchgeführt mit Unterstützung des Jubiläumsfonds der Oesterreichischen Nationalbank

Die komplette Studie kann zum Preis von ATS 2.700.- + 10% Ust
bei der ARGE DATEN bestellt werden

I. GRUNDTENDENZEN DER STUDIE

(A) DAS KOMMUNIZIERTE SICHERHEITSBEWUßTSEIN IST GENERELL HOCH.

Die überwiegende Zahl der Teilnehmer bekennt sich zu einer integrierten Security Policy, Mängel sind in der operativen Umsetzung zu erkennen.

Diese Mängel finden sich bei der organisatorischen Verantwortung, besonders die Kontrolle der Einhaltung von Sicherheitsvorgaben.

Eine weitere Schwachstelle bildet die Produktevaluation und der Produkteinkauf. In Hinblick auf Sicherheitsanforderungen ergibt sich eine zu hohe Abhängigkeit von den Herstellerangaben.

Es wird zu wenig auf die beiden wichtigsten Gefahrenquellen (Fahrlässigkeit/Irrtümer der Mitarbeiter) und technische Defekte (der Hard- und Software) reagiert.

Hier herrscht die etwas fatalistische Haltung, daß gegen diese Sicherheitsmängel kaum etwas effektiv unternommen werden kann.

Dieser Trend wird sich nach Ansicht der Experten durch die weitere Verbreitung von leistungsfähigen, aber unsicheren Workstationbetriebssystemen noch verstärken.

(B) AUF DIE NEUEN BEDROHUNGSBILDER OFFENER NETZE (INTERNET) WURDE RASCH REAGIERT.

Die laufende öffentliche Berichterstattung über Sicherheitsprobleme und „Hacker“ bei offenen Netzen führte ganz offensichtlich verstärkt zum Einsatz technischer (wirkungsvoller) Sicherheitsmaßnahmen.

Firewalls, Verschlüsselung und Virenprüfprogramme werden von einer großen Zahl von EDV-Anwendern eingesetzt.

(C) ES BESTEHT EIN ENORMES INTERESSE AN BERATUNGS- UND INFORMATIONSEINRICHTUNGEN.

Der Bereich IT-Sicherheit wird in Österrreich noch immer zu sehr als „Geheimwissenschaft“ betrieben. Besonders im Bereich der kleineren und mittleren Betriebe existiert nicht genügend personelle und finanzielle Kapazität, um laufend am letzten Stand der Sicherheitstechnik zu sein.

Es besteht daher der Wunsch nach unabhängigen Beratungsstellen.

Die Umfrage brachte aber auch eine klare Absage gegen verpflichtende oder überwachende Behörden. Von hoher Bedeutung sind Kompetenz- und Emergency-Zentren.

Die Kompetenzzentren könnten den Unternehmen in der Formulierung und Umsetzung ihrer Security Policy behilflich sein; die Emergency-Zentren sollten im Not- und Anlaßfall rasche Hilfestellung gewährleisten.

II. ERGEBNISSE IM ÜBERBLICK

- ***Die überwiegende Zahl der EDV-Anwender (75%) begrüßt die Standardisierung von IT-Sicherheitsmaßnahmen, nur eine Minderheit von 17% lehnt Aktivitäten in diesem Bereich ab.***

- *Österreichs EDV-Anwender sind bereit, Sicherheitsstandards zu übernehmen, diese einzuhalten, unabhängige nationale und internationale Serviceeinrichtungen zur Sicherheitsberatung zu konsultieren und für gute Sicherheitsprodukte (einfache Handhabbarkeit und Verständlichkeit) auch höhere Preise zu bezahlen.*

- *Die TN sind grundsätzlich aufgeschlossen gegenüber regulierenden (gesetzlichen) Maßnahmen im Bereich Sicherheitstechnik. Freiwillige Maßnahmen werden jedoch gegenüber Zwangsmaßnahmen bevorzugt. Diese freiwilligen Maßnahmen können durchaus auch verbindlichen Charakter haben.*

  Vier Maßnahmen, branchenspezifische „Codes of Conduct" (74%), technische Servicestelle (76%), ein nationales CERT (70%) und die regelmäßige Publikation von Prüfberichten und Übersichtskatalogen (72%,) erreichten eine Zustimmung von 70 Prozent und mehr.

  Es wird empfohlen diese ausdrücklich gewünschten Einrichtungen („nationales CERT" und „technische Servicestelle") rasch umzusetzen. Beide Maßnahmen könnten im Zusammenhang mit der durch die EU-Vorgaben notwendigen Novellierung des DSG realisiert werden.

- *Mehrheitlich abgelehnt wird eine Überwachungsbehörde, die EDV-Anwender auf Sicherheit „prüft" (65% Ablehnung, 15% Zustimmung).*

  Um jede Gefahr der Identifizierung von (erwünschten) Serviceeinrichtungen mit (unerwünschten) Überwachungseinrichtungen zu vermeiden, wird daher dringend empfohlen, die genannten Einrichtungen „nationales CERT" und „technische Servicestelle" behördenfern zu organisieren.

Hohe Zustimmung fand auch die Idee der steuerlichen Begünstigung von Sicherheitsprodukten (60% Zustimmung zu 18% Ablehnung). Angesichts der angespannten Budgetlage und auch in Hinblick auf eine mögliche Administration muß jedoch diese Idee skeptisch beurteilt werden.

- *Obwohl 98% der TN dem Grundsatzstatement „Fahrlässigkeit/Irrtümer von Mitarbeitern und technisch fehlerhafte Software stellen die größten Sicherheitsrisken dar“ zustimmten, konnten nur sehr mangelhafte Reaktionen darauf festgestellt werden. Besonders die Bereitschaft zur Sicherheitsschulung von Mitarbeitern und zum Einsatz von Analysewerkzeugen ist unterentwickelt.*

  Es wird empfohlen über unabhängige Beratungsstellen praxisnahe Sicherheitsinformationen für EDV-Endanwender anzubieten. Diese Beratungsstellen sollten zu IT-Sicherheits-Kompetenzzentren aufgewertet werden.

  Besonders im Bereich kleiner und mittlerer Firmen ist nicht zu erwarten, daß dortige Sicherheitsverantwortliche auf dem Stand der Technik bleiben können, da sie diese Aufgabe bestenfalls als Nebentätigkeit ausüben.

- *PC/Workstations (69%) und Netzwerkkomponenten (60%) gelten als DIE sicherheitsgefährdeten Anlagen. Nur 9% sehen besondere Gefährdungen im Mainframe-Bereich.*

- *Als besonders schwerwiegendes und weitgehend ungelöstes Sicherheitsproblem wurde der gesamte Softwarekomplex angesehen. Sowohl fehlerhafte Software, als auch programmtechnisch manipulierte Software werden als große Sicherheitsrisken angesehen.*

- *Im Zuge der Vernetzung werden auch externe Angriffe steigende Bedeutung erlangen.*

- *Die beiden Gefahrenbereiche "Höhere Gewalt" und Hardware-Defekte werden in der zukünftigen Sicherheitsdiskussion stark an Bedeutung verlieren.*

- *Interne Ansätze zur Sicherheitskontrolle werden gegenüber externen Prüfmaßnahmen eindeutig bevorzugt (85% gegenüber 7%).*

- ***Die gängige Meinung, daß Informationen über Sicherheitslücken bloß zu Verunsicherung und nicht zu konkreten Schutzmaßnahmen führen, konnte nicht bestätigt werden.***

- *Erfreulich ist der Trend „SW-Produkte mit ausgewiesenen Sicherheitsstandards“ einsetzen zu wollen. Hier ergeben sich enorme Chancen für österreichische Einrichtungen (SW-Entwicklung, Entwicklung von Zusatzprodukten, Prüf- und Zertifizierungsstellen).*

- *Erfreulich entwickelt sich das Bild im Zusammenhang mit Sicherheitsrisken bei offenen Netzwerken (z. B. INTERNET). Firewalls (68% Verbreitung), Datenverschlüsselung (50% Verbreitung) und Antivirenprogramme (89% Verbreitung) gehören zum Standardrepertoire im Zusammenhang mit offenen Netzwerkstrukturen.*

  Im Zusammenhang mit rechtlichen Regelungen, etwa einem eigenen Kryptographie-Gesetz, muß auf diese sich dramatisch veränderte Situation Rücksicht genommen werden. Ein Abweichen vom derzeitgen Status Quo (= Verschlüsseln ist allgemein erlaubt) ist nur in Hinblick auf eine zusätzliche Unterstützung jener sicherheitsbewußten Organisationen, die schon jetzt verschlüsseln, sinnvoll.

  Die Vielzahl an - zum Teil übertriebenen und/oder einseitigen - Presseberichten hat sicher ein gewisses Maß an Verunsicherung erzeugt, gleichzeitig aber die IT-Anwender motiviert, moderne Abwehrmaßnahmen zu setzen. Damit dürfte das Sicherheitsniveau der offenen Netze vielfach höher liegen, als meistens publiziert wird.

- *Neue Sicherheitsmaßnahmen werden bei der überwiegenden Zahl von TN (84%) aufgrund qualifizierter Ereignisse (Fachinformationen, Empfehlungen der Revision, Verdacht auf Datenverlust) und aufgrund von Standardsituationen (Neuinstallationen, Auftreten von Datenverlust) gesetzt. Damit kann von im wesentlichen akzeptablen Sicherheitsstrategien gesprochen werden.*

  Es wird empfohlen, weitere Anstrengungen zu unternehmen, sicherheitsrelevante Informationen direkt an die EDV-Anwender (Betreiber) heranzutragen (etwa durch geeignete Onlinedienste).

III. ERGEBNISSE DER UMFRAGE [IT-SEC97]

A. TECHNISCHE DATEN ZUR DURCHFÜHRUNG DER UMFRAGE

Die Umfrage erfolgte im Zeitraum vom 1.11.97 bis 5.12.97. Retournierte Fragebögen wurden bis 31.12.97 (Redaktionschluß) akzeptiert. 10 Tage vor dem offiziellen Ende der Umfrage wurde eine Teilgruppe der angeschriebenen Organisationen durch einen zweiten Brief an die Beantwortung erinnert. Es handelte sich dabei vornehmlich um Firmen. Bis Redaktionschluß wurden 427 Fragebögen retourniert, nach Redaktionschluß kamen noch rund 40 weitere Antworten, die nicht berücksichtigt werden konnten.

Die Umfrage erfolgte sowohl mittels eines klassischen Fragebogens in gedruckter Form als auch als WWW-Formular, das über Internet online ausfüllbar war.

B. DIE AUSWERTUNG

Insgesamt wurden 427 Fragebögen retourniert und ausgewertet (351 kamen per Post, 76 mittels WorldWideWeb).

Neben einer Komplett-Auswertung wurden folgende Zusatzauswertungen durchgeführt:

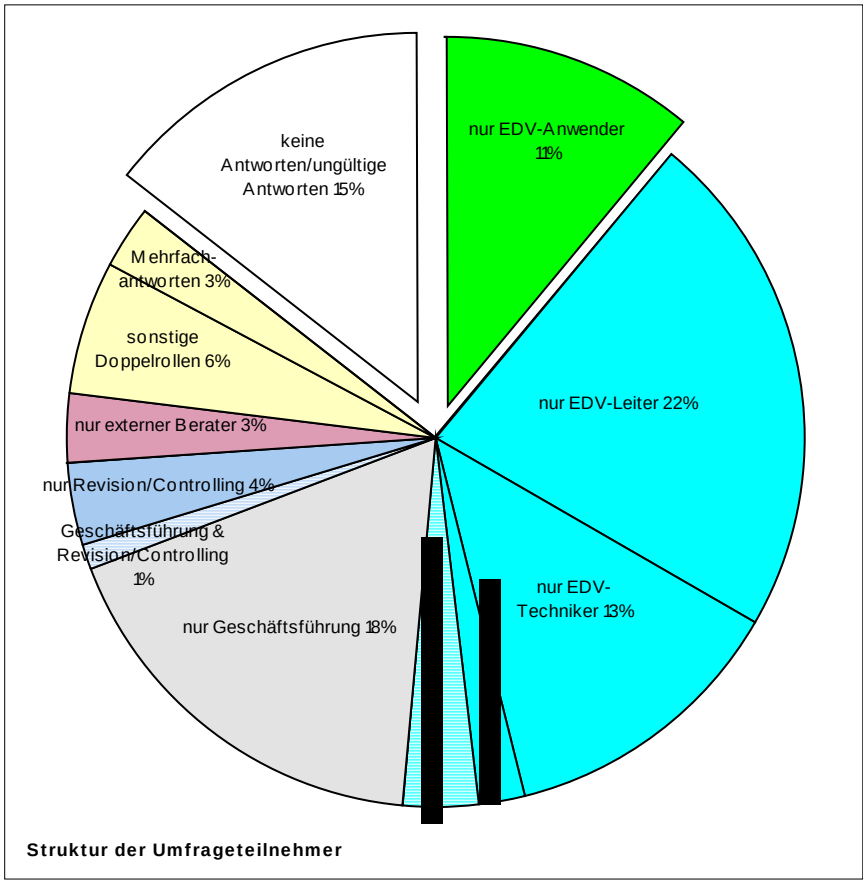
- Antworten von Unternehmen mit mehr als 5 MA (234 TN) (VAR I)
- Antworten von Unternehmen aus dem Bereich Gewerbe/Industrie (94 TN) (VAR II)
- Antworten von Unternehmen aus dem Dienstleistungsbereich (209 TN) (VAR III)
- Antworten von Unternehmen aus dem Bereich Gewerbe/Industrie mit mehr als 5 MA (71 TN) (VAR IV)
- Antworten von Unternehmen aus dem Dienstleistungsbereich mit mehr als 5 MA (111 TN) (VAR V)

Da auch die Möglichkeit bestand, den Fragebogen anonym zu retorunieren, konnte ein Teil der Fragebögen diesen Untergruppen nicht oder nicht eindeutig zugeordnet werden.

C. DIE TEILNEHMER

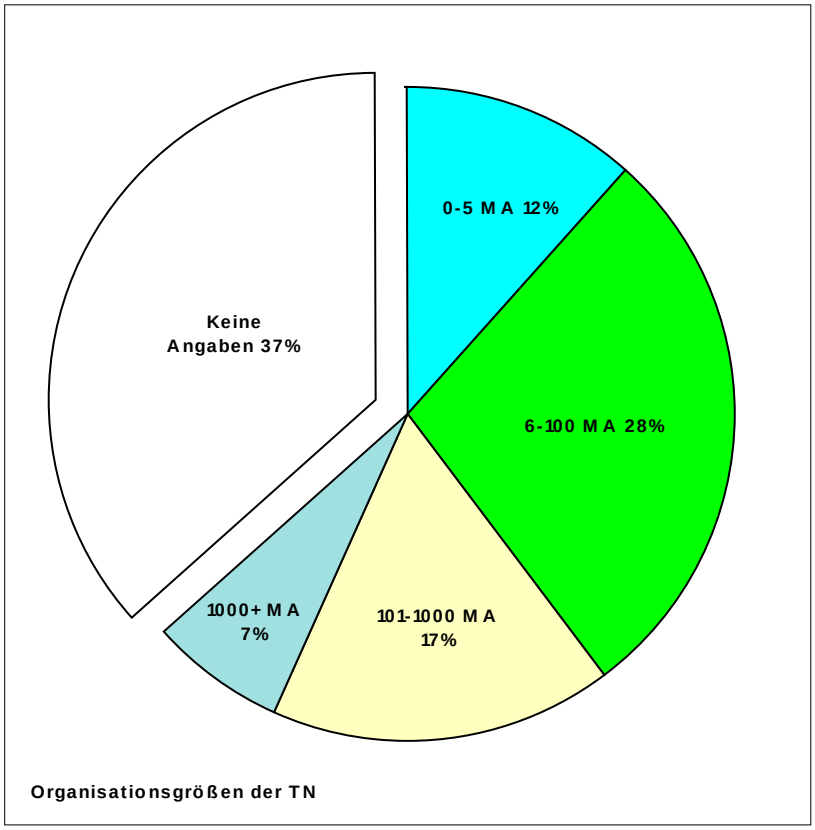
Es bestand die Möglichkeit, den Fragebogen anonym oder unter Angabe des Namens einzusenden. 59 TN machten von der anonymen Form der Teilnahme Gebrauch.

Bezüglich der innerbetrieblichen Verantwortlichkeit waren 22% der TN EDV-Leiter (insgesamt gaben 36% an, in der EDV-Abteilung tätig zu sein). 23% der TN stammten aus den Bereichen Geschäftsführung/Revision/Controlling. 4% der TN gaben als Funktionen EDV-Leitung + Geschäftsführung an. Mehrfachnennungen kamen von 9%, 11% waren sonstige EDV-Anwender. Keine oder keine gültigen Antworten kamen von 15% der TN.



Struktur der Umfrageteilnehmer

52% der TN gaben als Organisationsgröße 6 und mehr MA an, 24% eine Größe von mehr als 100 MA. Es konnte damit ein für Österreich typischer Querschnitt von Betriebsgrößen erzielt werden.



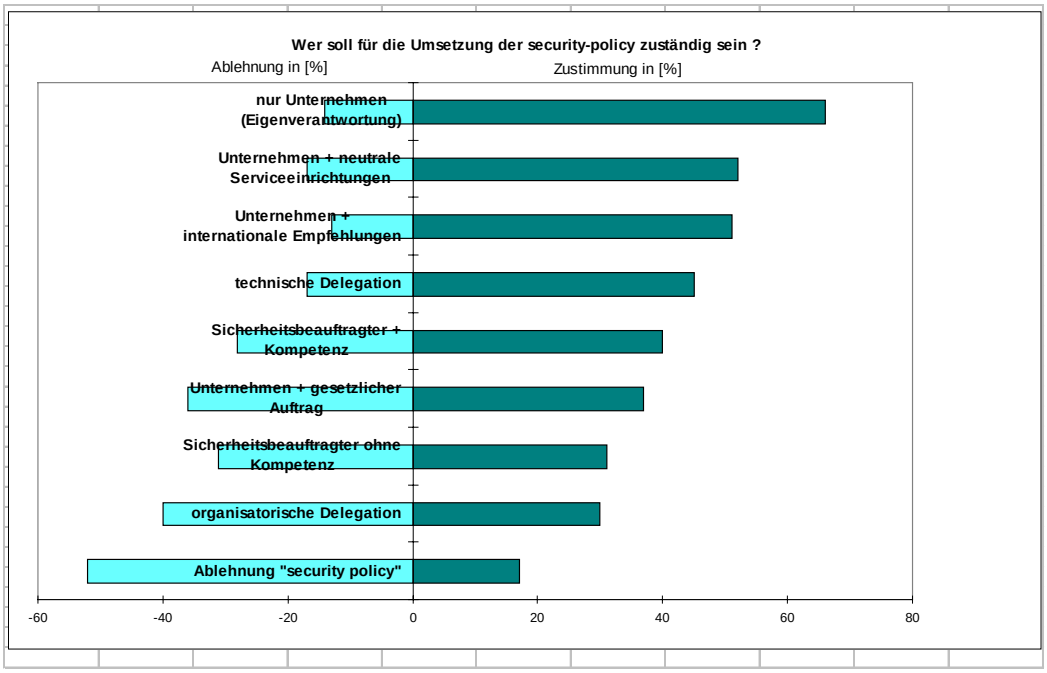
(1.) ÖSTERREICH EDV-ANWENDER WÜNSCHEN SICHERHEITSSTANDARDS

- **74%** der TN begrüßen Sicherheitsstandards, **18%** der TN lehnen Sicherheitsstandards ab, 8**%** beantworten diese Frage sowohl mit ja als auch nein.
- Die Zusatzfrage „Ja, weil damit die Auswahl und Beurteilung von Sicherheitsprodukten erleichtert wird“ wurde von 171 TN (= 55% der zustimmenden TN) positiv beantwortet.
- Als Argumente gegen eine Standardisierung wurden genannt: „Standards hinken der Zeit nach.“ (9 TN), „Standards erfüllen nicht individuelle Anforderungen.“ (14 TN), „Vielfalt ist der bessere Schutz.“ (14 TN) und „Standards sind zu umständlich.“ (3 TN) [Mehrfachnennungen waren möglich].

⇨ **Die Frage pro/contra IT-Sicherheitsstandards wurde eindeutig für Standards (rund 74%) beantwortet, wobei nur eine ganz kleine Gruppe (34 TN = 8%) keine eindeutige Meinung dazu hatte.**

(2.) ZWISCHEN PRAGMATISMUS UND RESERVIERTHEIT

Wer sollte für die Umsetzung einer unternehmensweiten Security Policy zuständig sein?



- Wenig überraschend erhielt die Aussage „Unternehmen sollten für Ihre Security Policy selbst verantwortlich sein“ die größte Zustimmung (66%). Angesichts der Tatsache, daß der Großteil österreichischer Unternehmen Klein- oder Mittelbetriebe sind, ist das jedoch eine problematische Einstellung.

  Aufgrund der rasch wachsenden Komplexität der IT-Systeme und der Abhängigkeit der Unternehmen von der EDV muß bezweifelt werden, daß dies ausreicht, eine Security Policy zu betreiben, die laufend „state of the art“ ist. Auch in anderen Studien wurde diese Position kritisch kommentiert.

- Je größer die Unternehmen sind, desto eher besteht die Bereitschaft, ihre Security Policy über externe Stellen absichern zu lassen (56% Zustimmung für die Inanspruchnahme neutraler Serviceeinrichtungen). Dieser Trend setzt sich bei Industrie/Gewerbebetrieben noch verstärkt fort. Die Bereitschaft neutralen Serviceeinrichtungen bzw. internationalen Empfehlungen zu folgen, liegt jeweils bei 57%.

⇨ **Das Ignorieren unternehmensweiter Sicherheitskonzepte ist eine absolute Minderheitsmeinung in Österreich. Bloß über den Weg zu einer Security Policy und die Sicherung derselben herrschen unterschiedliche Ansichten.**

⇨ **Unabhängige Beratungsstellen würden in Österreich sehr wohlwollend aufgenommen werden.**

(3.) HANDHABBARKEIT VON SICHERHEITSTECHNIK SCHLÄGT KOSTENFAKTOR

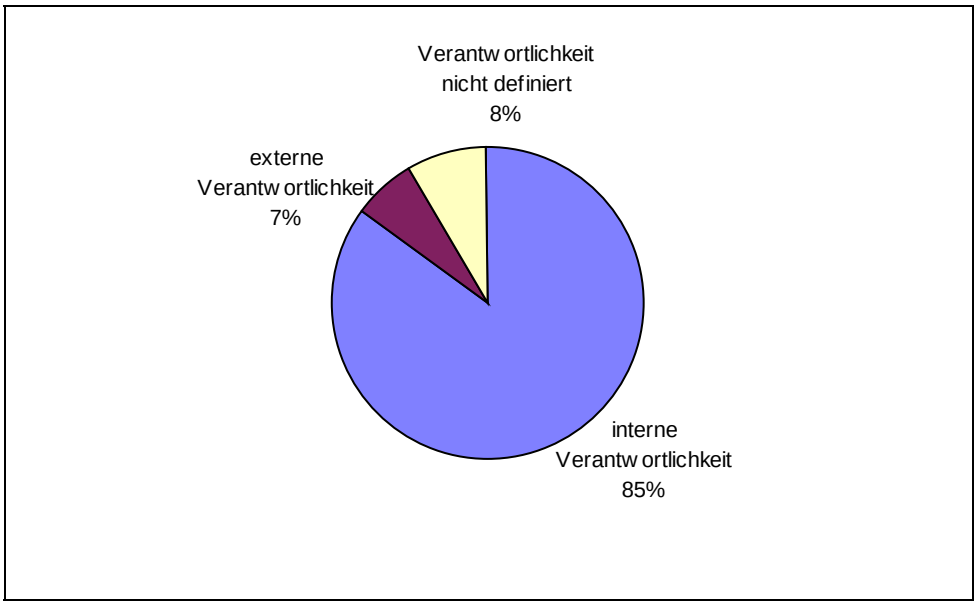
Das deutlichste Ergebnis war, daß „geringe Kosten“ für nicht einmal für die Hälfte der TN ein entscheidendes Kriterium bei der Beschaffung von Sicherheitstechnik darstellt (43%).

Das bei weitem wichtigste Kriterium für die Auswahl von Sicherheitsmaßnahmen stellte die „einfache Handhabung“ (83%) dar.

Auch „leichte Verständlichkeit“ (54%) wurde ebenfalls öfter als der Kostenfaktor genannt.

(4.) NICHT IN DIE KARTEN SCHAUEN LASSEN

Die weitaus überwiegende Zahl der TN bevorzugt interne Kontrollmaßnahmen (85%). Hingegen betreiben bloß 7% bei der Kontrollle der Sicherheitsmaßnahmen „outsourcing“. Dieser Wert wird sogar von der Anzahl der Organisationen übertroffen, die keine Zuständigkeit für die Sicherheitskontrolle zugeben (8%).



Graphik 4: Verantwortlichkeit bei der Kontrolle der Sicherheitsmaßnahmen