NOP World
United Business Media

Kontrolle der Zugriffsverwaltung und des Datenschutzes innerhalb Ihres Unternehmens

Weißbuch über
Zugriffsverwaltung und Datenschutz
in Verbindung mit Tivoli Software

Kontakt:

Liz Montgomery

Director

NOP Business

Ludgate House

245 Blackfriars Road

London, SE1 9UL

Großbritannien

Durchwahl: +44 (0)20 7890-9748

Fax: +44 (0)20 7890-9222

E-Mail: l.montgomery@nopworld.com

Inhalt

1. Zusammenfassung

Alle Befragten sind sich der wachsenden Komplexität ihrer Umgebungen und insbesondere der zunehmenden unbeabsichtigten Bloßlegung ihrer Systeme durch nachlässige Nutzer sehr bewusst. IT-Entscheider sind bestrebt, gleichzeitig sicherzustellen, dass ihre Systeme geschützt sind und die Benutzer dennoch nicht mit komplexen Zugriffssystemen überlastet werden. Sie erreichen dies heute entweder durch die Einführung neuer Authentifizierungsverfahren oder alternativ durch Synchronisierung. Eine Umstellung auf Einzelanmeldung (Single-Sign-On) wird von vielen derjenigen in Betracht gezogen, die dies bisher noch nicht implementiert haben.

IT-Entscheider müssen allerdings noch Herz und Verstand der Budgetverwalter und/oder des Vorstandes gewinnen, um sicherzustellen, dass Sicherheitsvorkehrungen getroffen werden, bevor ein Schaden eintritt. Die Einstellung „Das könnte uns nicht passieren“ scheint noch immer allzu weit verbreitet zu sein – oder aber führende Geschäftsentscheider sind sich einfach der potenziellen Kosten nicht bewusst. Jenen Befragten, die bereits größere Virusangriffe oder andere mit der Zugriffsverwaltung zusammenhängende Ausfälle erlebt haben, ist die Erlangung der erforderlichen Mittel gelungen – allerdings oftmals erst nach dem entsprechenden Vorfall.

Ein wesentliches Problem in diesem Zusammenhang scheint zu sein, dass die IT-Abteilung selbst ihr schlimmster Feind sein kann. Gesteigerte Sicherheit, so geben die Fachleute zu, geht mit der Wahrnehmung der Nutzer einher, dass die Systeme langsamer bzw. schwerfälliger sind. In ähnlicher Weise lassen auch zu viele Schauergeschichten die Entscheidungsträger abstumpfen – sie denken zum Teil, die IT-Abteilung schlage blinden Alarm.

Die Verfügbarkeit guter integrierter Tools zur Unterstützung der IT-Abteilung beim Management dieser Bedrohungen wird in Frage gestellt. Die Befragten

setzen alle möglichen Lösungen ein, und viele der größten Unternehmen entwickeln ihre eigenen Tools für das zentrale Bedrohungsmanagement und zur Erkennung von Eindringversuchen (Intrusion Detection).

Beim Datenschutz ergibt sich ein recht anderes Bild. Datenschutz ist im Wesentlichen für eine Schlüsselgruppe von Unternehmen von Interesse, die bereits aktiv mit großen Datenbanken, oftmals mit Kundeninformationen, arbeiten. Diesen Unternehmen stehen derzeit nur relativ wenige Tools für das Management von Datenschutzangelegenheiten zur Verfügung. Die Möglichkeit, Prüfungen und Informationen darüber bereitzustellen, welchen Verarbeitungen und Zugriffen derartige Daten unterlegen haben, könnte in Zukunft von wachsender Bedeutung sein, insbesondere bei Weiterentwicklung der EU-Gesetze. Die Notwendigkeit der Gesetzeskonformität ist mit Abstand der wichtigste Grund für die Einführung von IT-Tools zum Management von Datenschutzangelegenheiten, und hierbei an der Spitze der Entwicklung zu stehen, könnte auch einen gewissen Wettbewerbsvorteil bedeuten.

2. Hintergrund und Fragestellung

Tivoli Software, ein Unternehmen der IBM Software Gruppe, bietet Software an, die von Unternehmen aller Größen zur Unterstützung von Netzwerken, Systemen, Anwendungen und Business-to-Business-Commerce eingesetzt wird. Mit diesen Produkten und Dienstleistungen ermöglicht IBM es den Unternehmen, die Auswirkungen ihrer IT-Infrastruktur auf ihre Geschäftsprozesse zu managen und eine Rentabilität ihrer gesamten Technologie-Investitionen zu erzielen.

Hauptziel dieser Studie war es, Tivoli die neu auftauchenden IT-Managementfragen rund um web-basierte Anwendungen verstehen zu helfen, wobei das besondere Augenmerk größeren Unternehmen in Europa galt. Spezielle Zielsetzung war, die Wahrnehmungen bzw. Einschätzungen von Kunden bezüglich der Verfügbarkeit von E-Business zu verstehen, unter besonderer Berücksichtigung der folgenden Aspekte:

- *Bekanntheit*
- *Bedürfnisse*
- *Herausforderungen*
- *derzeitiger und künftiger Einsatz*

In dieser Reihe liegen insgesamt vier Berichte vor. Drei dieser Berichte behandeln verschiedene Themen unter der übergreifenden Fragestellung „Management der Auswirkungen auf Geschäftsprozesse“:

- *Performance und Verfügbarkeit*
- *Geschäftskontinuität und Datenspeicherung*

Der vorliegende dritte Bericht konzentriert sich speziell auf Fragen rund um die Zugriffsverwaltung und den Datenschutz.

3. Methodik

Die Daten in diesem Weißbuch beruhen auf der Befragung **Verfügbarkeit von E-Business**, die im Auftrag von Tivoli Software durchgeführt wurde.

In dieser Befragung ging es u. a. um Aspekte des IT-Managements rund um web-basierte Anwendungen sowie um die Einschätzungen von Kunden zur Verfügbarkeit von E-Business, insbesondere in Bezug auf Bekanntheit, Bedürfnisse, Herausforderungen sowie derzeitigen und künftigen Einsatz.

Die Studie wurde in zwei Phasen durchgeführt, wobei eine Kombination von qualitativem und quantitativem Feedback stattfand, um ein umfassendes Verständnis der von den Daten aufgezeigten grundlegenden Themen zu erlangen. Zunächst wurden hierzu 16 persönliche Interviews in vier Ländern durchgeführt (je vier Interviews in Frankreich, Deutschland, Italien und Großbritannien), um die neu entstehenden Themen ausführlich zu explorieren und sicherzustellen, dass in der anschließenden quantitativen Befragung alle entscheidenden Bereiche abgedeckt werden. Die Interviews dauerten im Durchschnitt eine Stunde und wurden von muttersprachlichen Marktforschungsfachleuten von NOP durchgeführt. Diese Phase war auf gewinnorientierte Unternehmen mit mehr als 1.000 Mitarbeitern beschränkt.

Die zweite Phase der Studie, ihrerseits quantitativer Natur, sorgte für solide Daten zur zuverlässigen Messung des derzeitigen Verhaltens und der aktuellen Einstellungen gegenüber web-basierten Anwendungen. Die Interviews wurden telefonisch durchgeführt und dauerten jeweils ca. 30 Minuten. Die endgültige Aufschlüsselung des Samples ist im Folgenden dargestellt:

Land	**Anzahl der Interviews**
Großbritannien	70
Frankreich	70
Deutschland	70
Italien	50
Insgesamt	**260**

Das Sample für diese Phase war ebenfalls auf größere Unternehmen mit mehr als 1.000 Mitarbeitern beschränkt. Innerhalb dieser Gruppe waren die Interviews recht gleichmäßig auf Unternehmen mit 1.000 bis 2.999 Mitarbeitern (43 %) und Unternehmen mit mehr als 3.000 Mitarbeitern (57 %) verteilt. Die Teilnehmer kamen aus einem repräsentativen Spektrum von Branchen, ausgenommen staatliche und nicht auf Gewinn gerichtete Organisationen.

Die Befragten mussten für die Infrastruktur und Systemleistung speziell hinsichtlich web-basierter Anwendungen zuständig sein. Interessanterweise handelte es sich hierbei oft nicht um den Leiter der IT-Abteilung oder den IT-Manager, sondern um eine wichtige leitende Führungskraft in recht großen IT-Teams, die in der Regel dem Leiter der IT-Abteilung direkt unterstellt war.

4. Ergebnisse der Studie

4.1 Einleitung

Im gegenwärtigen Geschäftsumfeld implementieren immer mehr Unternehmen technologische Systeme, die ihren Mitarbeitern, Kunden, Lieferanten und anderen Dritten einen gemeinsamen Zugriff auf die Informationsressourcen des Unternehmens ermöglichen. Diese Systeme werden heutzutage typischerweise mit Hilfe web-basierter Technologien erstellt, die den Vorteil relativer niedriger Entwicklungskosten, möglichen Zugriffs von verschiedenen Plattformen und den Nutzern vertrauter Schnittstellen bieten. Einhergehend mit dieser Zunahme des vernetzten Informationszugriffs ergeben sich jedoch wichtige Zugriffsverwaltungs- und Datenschutzfragen, die bei Nichtbeachtung durch die Unternehmen deren geschäftliches Vorankommen bedrohen können.

Obwohl es große Medienaufmerksamkeit für Fragen rund um den kundenorientierten E-Commerce über Internet gegeben hat, werden Unternehmen sich erst in jüngster Zeit der neuen technischen und politischen Fragen bzw. Probleme rund um die Zugriffsverwaltung und den Datenschutz am Arbeitsplatz bewusst.

Dieses Weißbuch verfolgt mehrere Zielsetzungen:

- Beschreibung der Zuständigen für die Entwicklung und Durchsetzung der Sicherheits- und Datenschutzpolitik innerhalb von Unternehmen;
- Ermittlung der neu entstehenden Probleme im Zusammenhang mit Zugriffsverwaltung und Datenschutz für die Unternehmen von heute;
- Verständnis der Gründe dafür, dass einige Unternehmen ihre eigenen Lösungen für die aufgezeigten Probleme entwickeln;

- Untersuchung der Reaktionen auf einige mögliche Lösungen für diese Probleme, um den Unternehmen bei der Auswahl der zu implementierenden Lösung eine fundierte Entscheidung zu ermöglichen.

4.2 Entwicklung und Durchsetzung von Richtlinien

4.2.1 Definition von „Sicherheit“

Um über die Zuständigkeit für Sicherheit und die Entwicklung der Sicherheitsrichtlinien innerhalb eines Unternehmens sprechen zu können, ist es zunächst wichtig zu definieren, was man unter dem Begriff „**Sicherheit**“ versteht. Im Allgemeinen könnte „**Sicherheit**“ beschrieben werden als „**Freiheit von Risiko oder Gefahr**“. Im Kontext der Informatik sollte Sicherheit jedoch definiert werden als „**die Verhinderung von bzw. den Schutz vor Zugriffen auf Informationen durch unberechtigte Empfänger**“ und als „**die Verhinderung von bzw. den Schutz vor absichtlicher, aber unberechtigter Zerstörung oder Veränderung dieser Informationen**“.

Computersicherheit umfasst drei wichtige Bereiche, mit denen sich alle Unternehmen befassen müssen:

- **Vertraulichkeit**: Gewährleistung, dass keine unberechtigten Nutzer auf Informationen zugreifen.
- **Integrität**: Gewährleistung, dass keine unberechtigten Personen Informationen in einer Weise verändern, die von berechtigten Nutzern nicht erkannt wird.
- **Authentifizierung**: Gewährleistung, dass die Nutzer jene Personen sind, die sie vorgeben zu sein.

4.2.2 Zuständigkeit für die Entwicklung von Sicherheitsrichtlinien

Die Ergebnisse der Studie „Verfügbarkeit von E-Business“ zeigen, dass die Zuständigkeit für die Entwicklung von Sicherheitsrichtlinien hauptsächlich in der Verantwortlichkeit der IT-Abteilung liegt (66 %).

Andere Abteilungen haben den Befragten zufolge ebenfalls Zuständigkeit für diese Aufgabe, u. a. die Sicherheitsabteilung (13 %) und der zentrale Geschäftsbetrieb (10 %). Sicherheitsabteilungen sind übrigens in den Finanz- und Unternehmensdienstleistungssektoren weitaus stärker verbreitet als in allen anderen untersuchten Branchen.

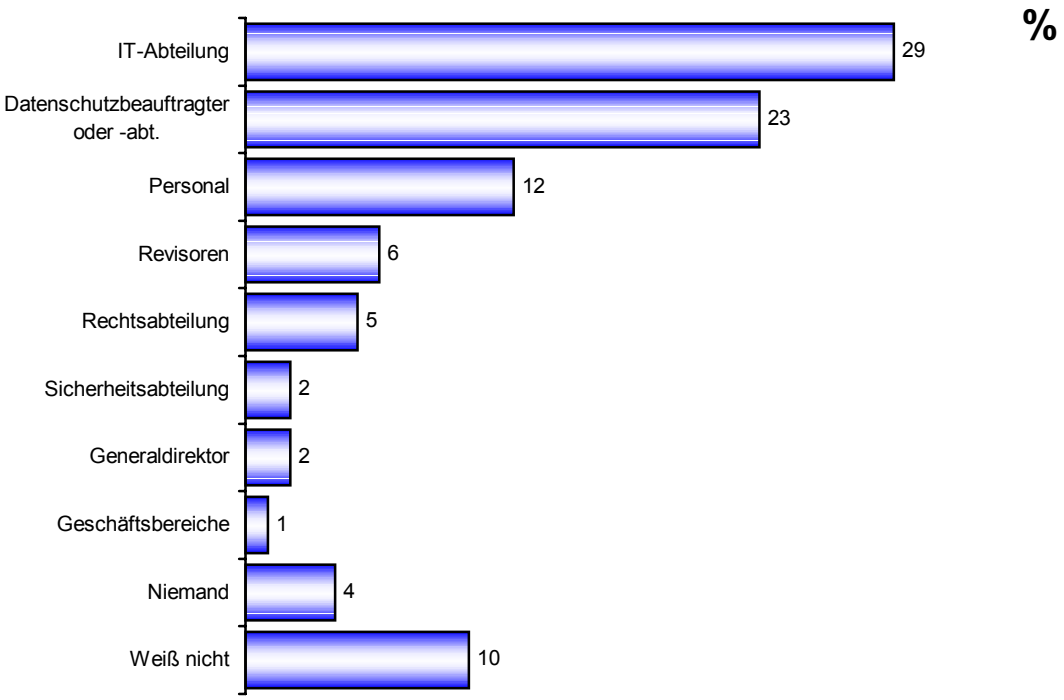
4.2.2 Zuständigkeit für die Durchsetzung von Sicherheit

Die Zuständigkeit für die Durchsetzung der Sicherheit liegt ebenfalls hauptsächlich in der Verantwortlichkeit der IT-Abteilung (68 %). Auch hier werden außerdem wieder die Abteilungen Sicherheit (25 %) und zentraler Geschäftsbetrieb (9 %) als für diese Aufgabe zuständig genannt.

4.2.2 Zuständigkeit für den Datenschutz

Die Zuständigkeit für den Datenschutz liegt zwar häufig auch noch im Bereich der IT-Abteilung, doch hier zeigt sich ein sehr viel breiteres Spektrum von zuständigen Abteilungen. In Italien beispielsweise fällt der Datenschutz – in Widerspiegelung der Bedeutung der Datenschutzgesetze in jenem Land – häufig in die Zuständigkeit des Generaldirektors, und auch die Revisions- und Personalabteilungen spielen dort eine Rolle. In 4 % der interviewten Unternehmen liegt der Datenschutz den Befragten zufolge allerdings überhaupt nicht in der Verantwortlichkeit einer bestimmten Person oder Abteilung.

F. Wer ist zuständig für den Datenschutz?



Basis: Alle Befragten (260)

Die Antwort auf diese Frage schwankt sehr stark in Abhängigkeit von der Menge der vertraulichen bzw. personenbezogenen Informationen, die ein Unternehmen halten muss, sei es über seine Mitarbeiter oder seine Kunden. Einzelhandels- und Transportunternehmen sowie einige Firmen in der Finanz- und Unternehmensdienstleitungsbranche sind, wie zu erwarten, in dieser Beziehung höher organisiert.

4.3 Probleme

Die IT-Entscheider haben verschiedene Schlüsselprobleme aufgezeigt:

- Externe Bedrohungen
- Böswillige Bedrohungen aus dem Innern des Unternehmens heraus
- Unbeabsichtigte Bedrohungen durch Handlungen von Mitarbeitern

All dies vor dem Hintergrund der Schwierigkeit, Finanzmittel zu erlangen.

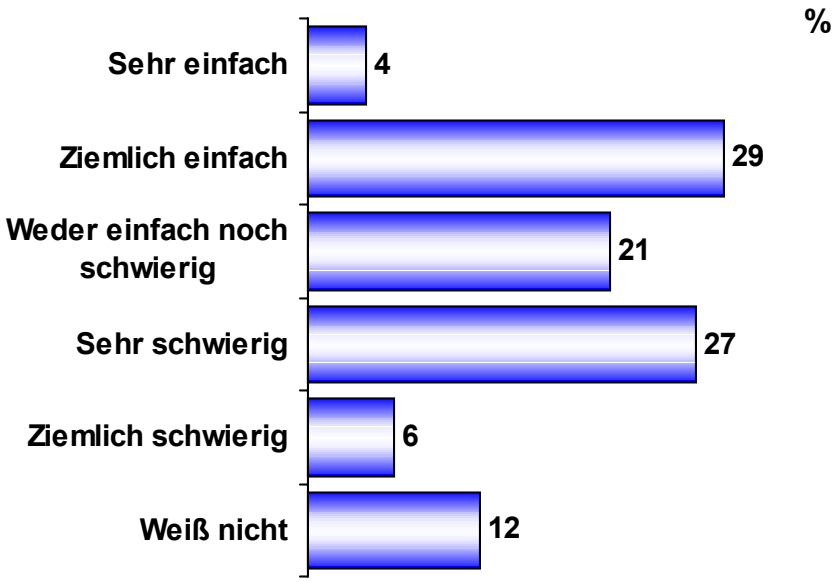
Im Fall des Datenschutzes haben wir speziell untersucht, ob die Unternehmen Datenschutzmaßnahmen nur als lästige Pflicht ansehen – als etwas, das getan werden muss, um den gesetzlichen Bestimmungen Genüge zu leisten – oder ob der Datenschutz ein Potenzial für einen wirtschaftlichen Vorteil oder sogar den Aufbau von Kundenbeziehungen darstellt. Es zeigt sich, dass die Einführung noch immer hauptsächlich auf die erforderliche Einhaltung von Gesetzen zurückzuführen ist anstatt auf geschäftliche Notwendigkeiten oder Kundenforderungen.

4.3.1 Bedrohungen

Erkennen „echter" Bedrohungen

Es ist für Unternehmen von größter Wichtigkeit, erkennen zu können, welche Bedrohungen „echt" sind. In diesem Zusammenhang wurden die Teilnehmer der Studie gefragt, wie einfach bzw. schwierig es sei, echte Bedrohungen aus der Menge der Warnungen zu erkennen, die von den verschiedenen Produkten, die sie zur Zugriffsverwaltung und -überwachung einsetzen, generiert werden. Die folgende Abbildung verdeutlicht die Ergebnisverteilung:

F. Wie einfach bzw. schwierig ist es, aus der Menge der Warnungen, die von den Produkten zur Zugriffsverwaltung und -überwachung generiert werden, echte Bedrohungen zu erkennen?



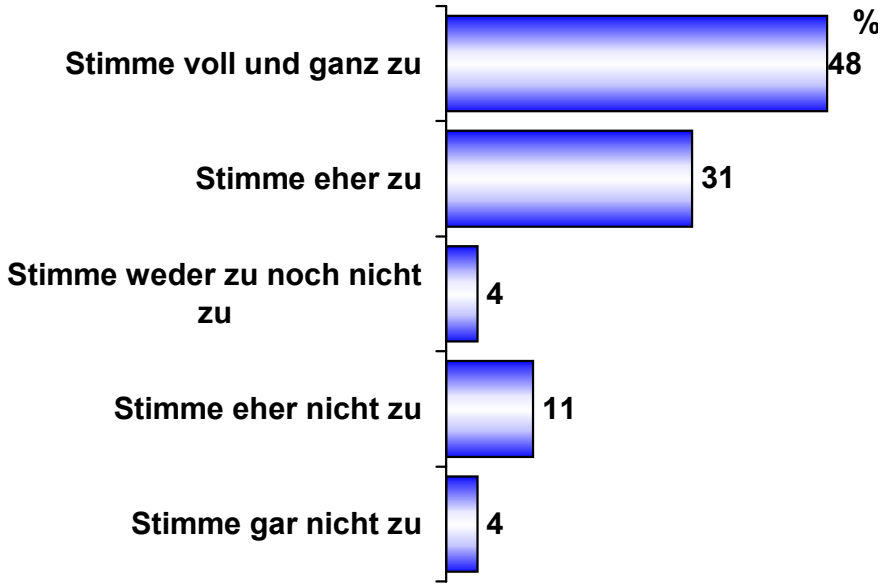
Basis: Alle Befragten mit Zuständigkeit für Sicherheit oder Authentifizierungsverwaltung (226)

Aus der vorstehenden Abbildung ist klar ersichtlich, dass die Aufgabe der eindeutigen Erkennung von Bedrohungen ein „*grauer*“ Bereich ist. Dies wird auch von der Tatsache unterstrichen, dass etwas mehr als ein Viertel der Befragten angibt, dass dies entweder „**Ziemlich einfach**“ oder „**Ziemlich schwierig**“ sei, und 12 % mit „**Weiß nicht**“ antwortet.

4.3.2 Mitarbeiter – die größte Bedrohung für Ihr Unternehmen

„Alternative“ Hacker, jugendliche Virusschreiber und sog. „Script Kiddies“ aus unterschiedlichen Teilen der Erde können zwar die Sicherheit von Unternehmen bedrohen, doch die Studie legt nahe, dass die größte Bedrohung wahrscheinlich eine interne Person ist. Ebenso wie andere jüngst veröffentlichte Untersuchungen zeigt auch diese Studie, dass fast die Hälfte aller Befragten voll und ganz zustimmt, dass die größte Gefahr für den Schutz von Informationen interner Natur ist und nicht von externen Quellen wie Viren oder Hackern ausgeht.

F. Nachlässige Mitarbeiter sind eine größere Bedrohung für den Datenschutz als Hacker.



Basis: Alle Befragten (260)

Weitere 31 % stimmen eher zu, dass ihre Mitarbeiter eine größere Gefahr darstellen als externe Bedrohungen. Darüber hinaus glaubt fast ein Viertel der Befragten mit Zuständigkeit für Sicherheit bzw. für die Verwaltung der Authentifizierungsverfahren, dass ihre Nutzer „**Nicht sehr sorgsam**“ in Bezug auf die Einhaltung von Zugriffskontrollregeln sind.

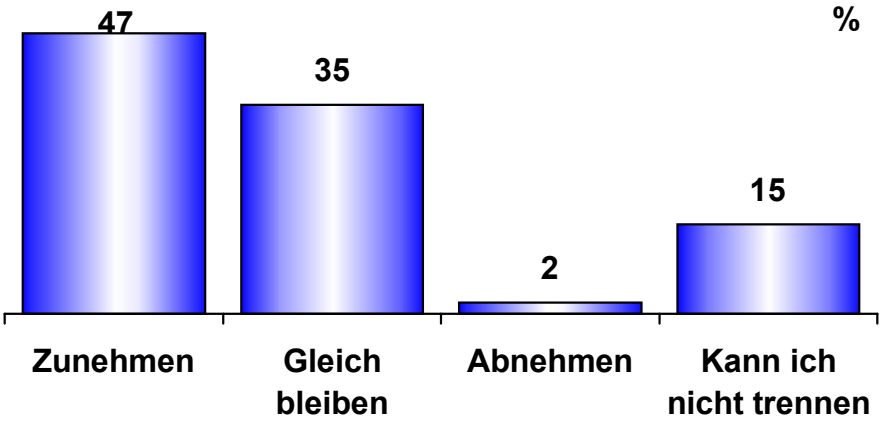
Das Ergebnis von all dem ist, dass sehr viel IT-Zeit für das Management dieser Bedrohungen aufgewendet wird. Schon allein die Zeit für die Verwaltung der Authentifizierung, einschließlich Rücksetzung von Passwörtern, stellt für die IT-Abteilung eine recht starke Arbeitsbelastung von 1–2 Tagen pro Woche dar.

Von den Herausforderungen, denen sich Unternehmen in Zukunft gewachsen zeigen müssen, halten viele Befragte insbesondere die Schaffung von mehr Zugriffskanälen, Remote-Zugriff und Zugriff für Dritte für jene Bereiche, die in Bezug auf Sicherheit und Datenschutz Besorgnis erregend sind.

4.3.3 Erlangung von Finanzmitteln

Ein Thema, das sich durch die gesamte Studie zieht, ist die Schwierigkeit, die erforderlichen Finanzmittel für die Gewährleistung der Geschäftskontinuität zu bekommen. Bei der Erlangung des erforderlichen Budgets für die Sicherstellung der Zugriffsverwaltung und des Datenschutzes durch höhere Sicherheit sieht es nicht anders aus.

F. Wie wird sich der Anteil des IT-Budgets, der für Sicherheit aufgewendet wird, in den nächsten 12 Monaten verändern?



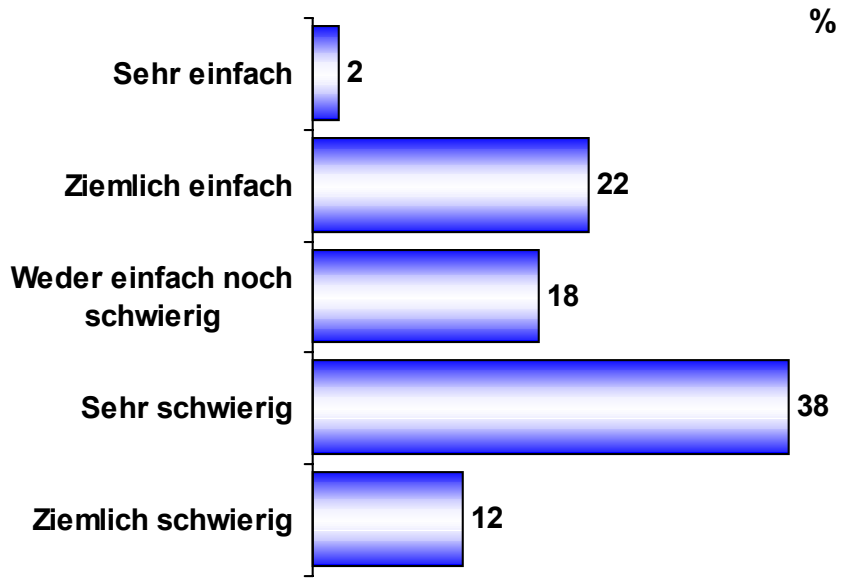
Basis: Alle Befragten mit Zuständigkeit für Sicherheit oder Authentifizierungsverwaltung (226)

Obwohl 47 % angeben, dass der Anteil ihres IT-Budgets, den sie für Sicherheit aufwenden, in den nächsten 12 Monaten zunehmen wird, sagen doch viele, dass Finanzmittel oft erst zur Verfügung gestellt werden, nachdem ein Sicherheitsausfall eingetreten ist. Dies spiegelt auch die Ergebnisse der qualitativen Studie wider, in der die Befragten häufig die Einstellung des Vorstandes beklagten, das Risiko sei zu gering, und dass Maßnahmen erst ergriffen werden, wenn der Schaden bereits passiert ist. Selbst einige der Personen, mit denen wir gesprochen haben, vertraten die Ansicht, „*in unserem Unternehmen gibt es nichts Interessantes zum Hineinhacken*“ – ohne Rücksicht auf den potenziellen Scha-

den und die Ausfallzeit, die von einer externen oder internen Person, die einen Groll hegt, verursacht werden könnte.

Die folgende Abbildung veranschaulicht die Schwierigkeit, der sich Befragte gegenübersehen, wenn sie versuchen, die geschäftlichen Entscheidungsträger davon zu überzeugen, in Software für die interne oder externe Zugriffsverwaltung und Zugriffskontrolle zu investieren.

F. Wie einfach ist es, die geschäftlichen Entscheidungsträger zu überzeugen, Gelder für Software für die interne oder externe Zugriffsverwaltung und -kontrolle zur Verfügung zu stellen?



Basis: Alle Befragten mit Zuständigkeit für Sicherheit oder Authentifizierungsverwaltung (226)

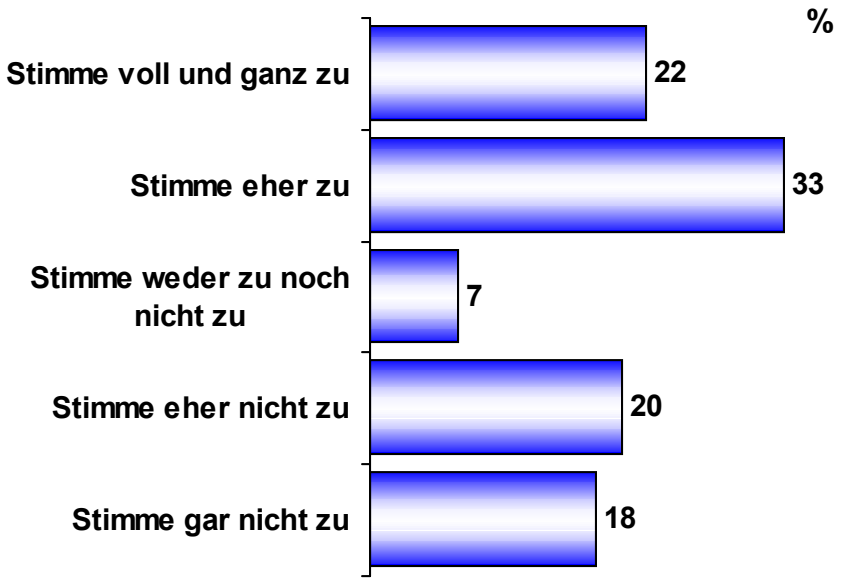
Die in diesem Diagramm dargestellten Ergebnisse spiegeln auch die Resonanz der qualitativen Studie wider, in der viele Befragte hervorhoben, dass ihre Unternehmen in derartigen Situationen nur reaktiv sind.

Darüber hinaus verdeutlichen im Rahmen der qualitativen Befragung geäußerte Ansichten, dass die Geschäftsführung oft andere Aufgaben für wichtiger erachtet als den Schutz der internen Daten bzw. Anwendungen. So wurde berichtet, dass

es einfacher ist, Gelder für Maßnahmen zu erlangen, die für Effizienz, Benutzerkomfort, schnellen Zugriff oder sogar physische Sicherheit (Diebstahl, Überschwemmung) sorgen. Zugriffsverwaltungstools dagegen behindern in den Augen dieser Nicht-IT-Entscheider teilweise die unmittelbare Effizienz bzw. den direkten Benutzerkomfort, hieß es.

Dies wird auch durch die unten stehende Abbildung bestätigt, für die die Befragten gebeten wurden zu bewerten, wie ernst interne Entscheidungsträger ihrer Ansicht nach die Sicherheit nehmen.

F. Interne Entscheidungsträger nehmen die Sicherheit nicht ernst genug.



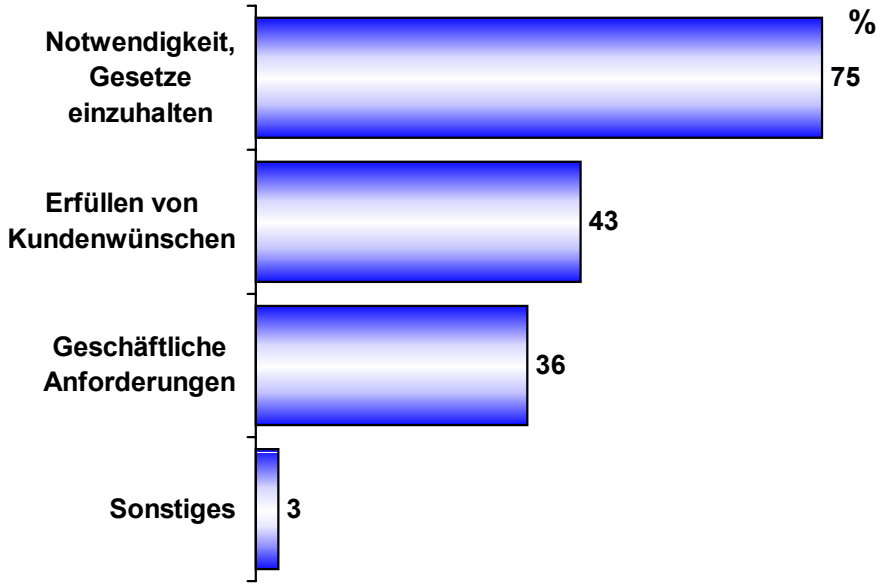
Basis: Alle Befragten (260)

4.3.4 Datenschutzangelegenheiten

Nur eine Minderheit von Unternehmen setzt derzeit spezielle IT-Lösungen zum Management ihrer Datenschutzangelegenheiten ein, doch der Anteil der hieran interessierten Unternehmen ist im Steigen begriffen. Für die Mehrzahl der Firmen liegt der treibende Grund dafür, diesbezüglich etwas zu unternehmen, in der Notwendigkeit, Gesetze einzuhalten. Die Möglichkeit, sich hierdurch einen

wirtschaftlichen Vorteil – oder sogar Kundennachfrage – zu sichern, ist deutlich weniger wichtig.

F. Was ist/wäre der treibende Grund für den Einsatz von IT-Tools für das Management der Einhaltung von Datenschutzgesetzen?



Basis: Alle Befragten (260)

4.4 Vorhandene und in Erwägung gezogene Zugriffsverwaltungs- und Datenschutzmanagementlösungen

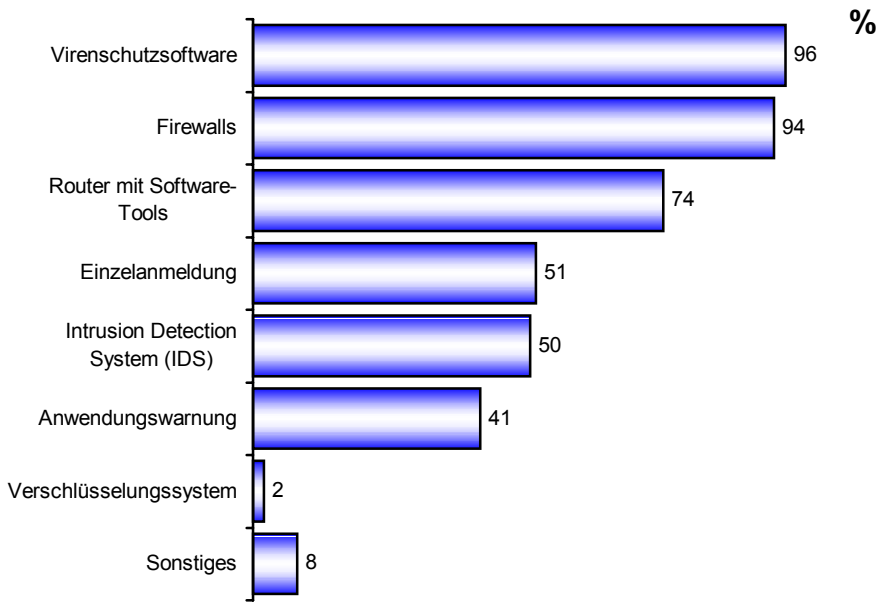
Diese großen europäischen gewinnorientierten Unternehmen haben ein breites Spektrum von Lösungen für das Zugriffs- und Bedrohungsmanagement implementiert, mit Programmen von Drittunternehmen, intern entwickelten Lösungen und auch Freeware oder Shareware. Viele Befragte scheinen zu denken, dass sie Lösungen implementiert haben, und sie haben anscheinend Spaß an der technischen Herausforderung, derartige Lösungen zusammenzubauen. Sie anerkennen allerdings auch, dass der Grad der Bedrohung stetig zunimmt und dass es schwieriger wird, „echte“ Gefahren von willkürlichen bzw. harmlosen Bedrohungen zu unterscheiden.

Nur wenige Unternehmen verfügen über Lösungen für das Management von Informationen im Kontext von Datenschutz, auch wenn dies für einige Unternehmen, die mit sehr großen, hauptsächlich kundenbasierten Datenbanken arbeiten, von starkem Interesse ist.

4.4.1 Hauptlösungen für Sicherheitsmanagement und Zugriffsverwaltung

Die Unternehmen nutzen derzeit ein breites Spektrum von Lösungen für das Sicherheitsmanagement und die Zugriffsverwaltung. Fast alle Befragten haben Virenschutzsoftware und Firewalls implementiert, und annähernd drei Viertel verfügen über Router mit speziellen Sicherheitssoftwaretools.

F. Was sind die Hauptlösungen, die Sie derzeit für das Sicherheitsmanagement und die Zugriffsverwaltung nutzen?



Basis: Alle Befragten mit Zuständigkeit für Sicherheit oder Authentifizierungsverwaltung (226)

Darüber hinaus nutzt knapp über die Hälfte Einzelanmeldungen (Single-Sign-On). Weiterhin verfügt die Hälfte über irgendeine Art von System zur Erkennung von Eindringversuchen (Intrusion Detection System).

4.4.2 Eingesetzte Produkte für Sicherheitsmanagement und Zugriffsverwaltung

Es werden vorrangig führende Netzwerkhardware-, Firewall- und Virenschutzmarken eingesetzt, was die oben bei **4.4.1** angegebenen Hauptlösungen widerspiegelt, d. h. Cisco, Checkpoint (Firewall1), Symantec/Norton und in geringerem Umfang Network Associates/McAfee. Darüber hinaus wurde aber auch eine Vielzahl anderer Produkte genannt, die in den Unternehmen zum Einsatz kommt. Hierzu gehören auch Freeware und Shareware.

4.4.3 Zentrale Verwaltung von Warnungen

Mehr als zwei Drittel der Befragten mit Zuständigkeit für Sicherheit bzw. für die Verwaltung der Authentifizierungsverfahren gibt an, dass sie in der Lage sind, Warnungen zentral zu verwalten. Bei Unternehmen mit mehr als 100 IT-Mitarbeitern glauben sogar 80 % der Unternehmen, über eine zentrale Verwaltung zu verfügen.

Fast drei Viertel jener Befragten, die über die Möglichkeit einer zentralen Warnungsverwaltung verfügen, hat ihre Lösung von einem Drittunternehmen bezogen.

Die Studie zeigt allerdings auch, dass bei den Unternehmen mit 3.000 oder mehr Mitarbeitern fast ein Drittel seine eigenen Lösungen entwickelt. Ein guter Teil nutzt zudem auch Freeware, Shareware oder Open-Source-Software, oftmals von Universitäten. SNORT, ein Open-Source-Programm zur Erkennung von Eindringversuchen in Netzwerke, ist eines der in diesem Zusammenhang genannten Beispiele. Diese Software kümmert sich jedoch nur um eine bestimmte Gruppe von Warnungen, und so dient ein kompetentes zentrales Verwaltungssystem dazu, alle Informationen von Firewalls, Virenschutz und Intrusion Detection zusammenzuführen und daraus aussagekräftige Daten zu generieren.

In den quantitativen Gesprächen stellten wir fest, dass die Befragten häufig die Ansicht vertreten, dass serienmäßig hergestellte Softwarepakete nicht ausreichend ausgefeilt sind, um den Anforderungen ihrer komplexen Umgebungen gerecht zu werden, und dass es ihnen eindeutig Spaß macht, Softwaretools zu schreiben, die eine Art „Armaturenbrett" bzw. Monitor bieten, der Testalgorithmen für die Suche nach bestimmten Verhalten integriert. Einige Befragte sind auch der Ansicht, dass kommerzielle Software immer hinter den Hackern und den vielen neuartigen Formen von Bedrohung hinterherhinken wird, die sich ständig „in der freien Wildbahn" entwickeln.

4.4.4 Authentifizierung & Zugriffskontrolle

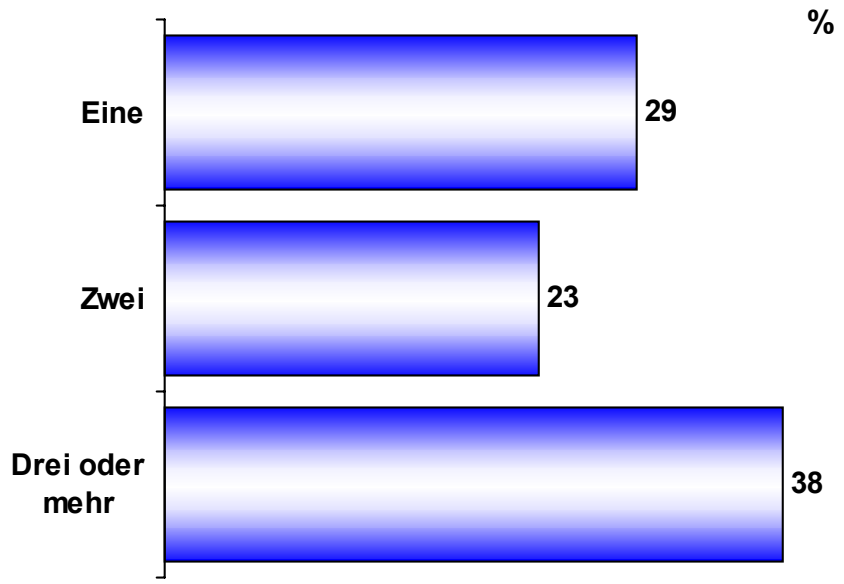
Wie bereits oben erwähnt, glauben viele der für die Zugriffskontrolle Zuständigen, dass die Benutzer die vorgegebenen Richtlinien nicht immer genau einhalten. Die Verfahren für den Informationszugriff sind deshalb immer sicherheitsbewusster geworden. Der Vorgang zur Identifikation einer Person, häufig auf der Grundlage eines Benutzernamens und eines Kennworts, wird als Authentifizierung bezeichnet. In Sicherheitssystemen ist dies zu unterscheiden von der Autorisierung. Hierbei handelt es sich um den Vorgang, bei dem eine Person auf der Grundlage ihrer Identität Zugriff auf bestimmte Systemobjekte erhält. Die Authentifizierung dagegen stellt lediglich sicher, dass die Person diejenige ist, der sie vorgibt zu sein, sagt aber nichts über die Zugriffsrechte dieser Person aus.

Die **„Zugriffskontrolle"** kann man als die Mechanismen für die Genehmigung oder Beschränkung von Zugang zu einem Computernetzwerk beschreiben. Über die Zugriffskontrolle wird der Benutzerzugriff gemanagt, indem eine Authentifizierung der Identität des jeweiligen Benutzers bzw. seiner Zugehörigkeit zu einer vordefinierten Gruppe verlangt wird. Die Zugriffskontrolle wird typischerweise von Systemadministratoren genutzt, um den Zugriff auf Anwendungen, Datenbanken und andere Netzwerkressourcen zu steuern.

4.4.5 Anmeldungen (Sign-Ons)

Die Studie zeigt, dass die typische Zahl von Anmeldungen, über die ein Benutzer zu Authentifizierungszwecken verfügt, mindestens drei oder mehr beträgt. Dieses Verhalten war besonders offensichtlich in Italien und Deutschland und könnte auf die Datenschutzgesetze in diesen beiden Ländern zurückzuführen sein, die sehr viel strenger sind als die britische Gesetzgebung.

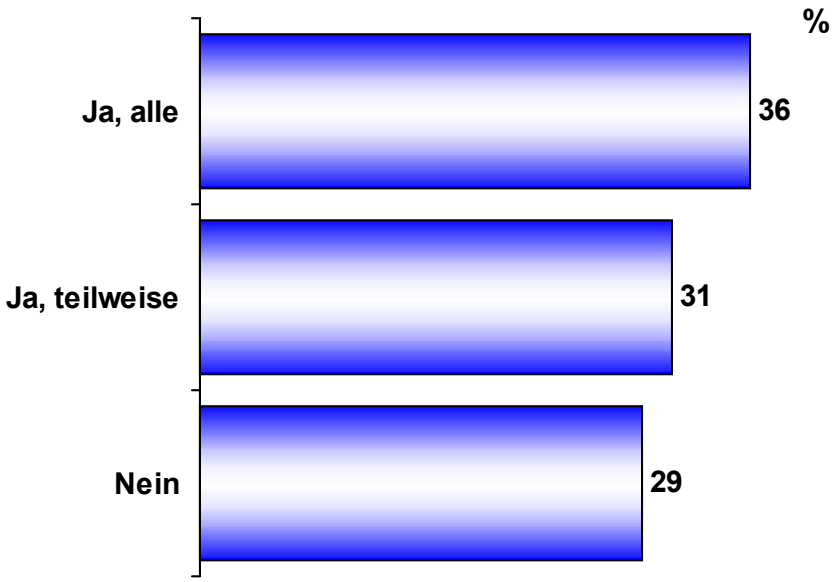
F. Wie viele Anmeldungen hat ein typischer Benutzer in Bezug auf die Authentifizierung?



Basis: Alle Befragten mit Zuständigkeit für Sicherheit oder Authentifizierungsverwaltung (226)

Allerdings sind bei über einem Drittel jener Benutzer mit mehr als einer Anmeldung die Anmeldungen transparent oder synchronisiert. Deutschland ist sehr viel sicherheitsbewusster als andere europäische Länder in der Studie.

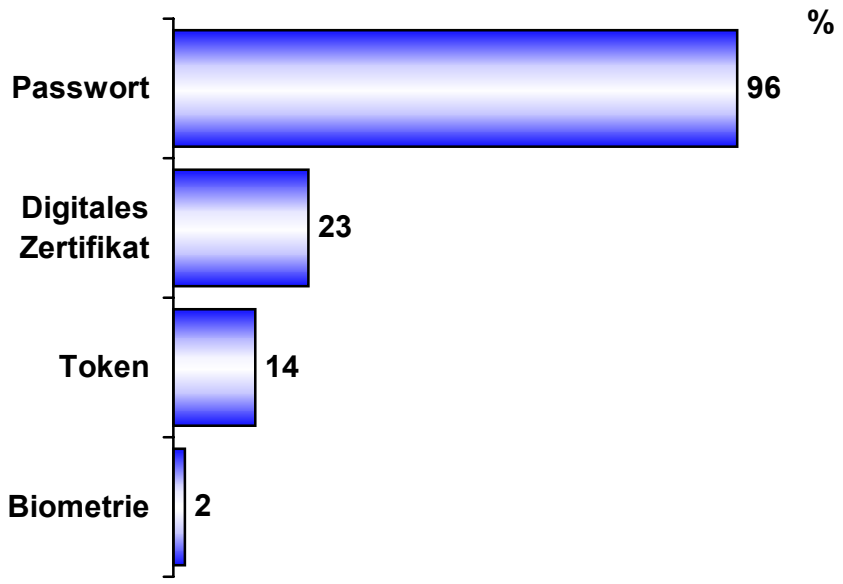
F. Sind diese Anmeldungen für die Benutzer transparent oder synchronisiert?



Basis: Alle Befragten, bei denen die Benutzer mehr als eine Anmeldung haben (137)

In Bezug auf die heute am weitesten verbreiteten Anmeldearten zeigt sich, dass fast alle Unternehmen Passwörter nutzen. Die meisten Unternehmen setzen zusätzlich noch eine andere Art von Mechanismus ein, was auf eine gewisse Annahme von digitalen Zertifikaten und Token hindeutet. Darüber hinaus kommt in einem kleinen Prozentsatz der befragten Unternehmen auch Biometrie zum Einsatz. Biometrie bezeichnet Authentifizierungstechniken, die auf messbaren körperlichen Eigenschaften beruhen, die automatisch überprüft werden können. Hierzu gehören zum Beispiel eine Computeranalyse von Fingerabdrücken oder Sprache. Obwohl dieser Bereich noch in den Kinderschuhen steckt, sind doch viele Befragte der Ansicht, dass Biometrie bei künftigen Computern und insbesondere bei E-Commerce eine entscheidende Rolle spielen wird.

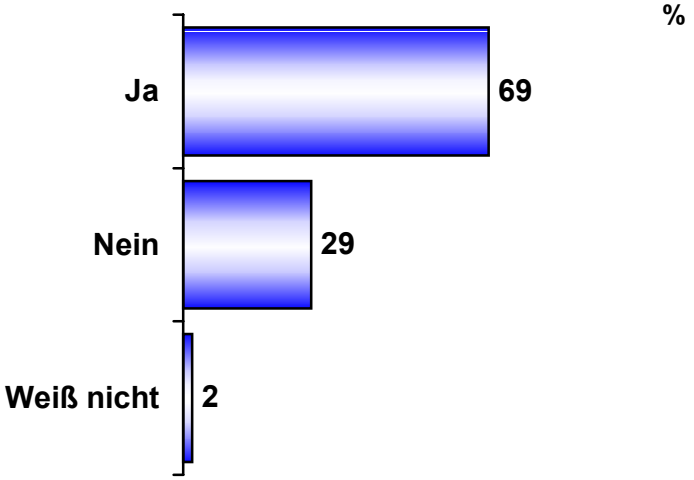
F. Was für eine Art von Anmeldung wird genutzt?



Basis: Alle Befragten mit Zuständigkeit für Sicherheit oder Authentifizierungsverwaltung (226)

Vom Sicherheitsstandpunkt aus gesehen ist es zumindest beruhigend, dass über zwei Drittel jener Befragten, die derzeit keine synchronisierten Anmeldungen haben, angibt, dass sie schon ein Single-Sign-On bzw. eine einzige Zugriffskontrolle für das ganze System in Betracht gezogen haben.

F. Haben Sie schon in Betracht gezogen, ein Single-Sign-On bzw. eine einzige Zugriffskontrolle für das ganze System bereitzustellen?



Basis: Alle Befragten ohne synchronisierte Anmeldungen (87)