Anwender im Wettlauf gegen Viren und Hacker

Ergebnisse der silicon.de-Umfrage "IT-Sicherheit 2002"

Security-Experten müssen an vielen Fronten kämpfen

Die Sicherheit - also die Verfügbarkeit, Vertraulichkeit und Integrität - seiner Daten, Übertragungswege und Anlagen mögen für den IT-Manager nicht das primäre Ziel seiner Tätigkeit darstellen, aber ohne diese Faktoren sind alle Bemühungen um betriebswirtschaftliche Effizienz und Rationalisierung von vorneherein aussichtslos. Das Streben nach größtmöglicher Sicherheit nimmt daher für den Verantwortlichen im Unternehmen einen prominenten Platz in seiner Agenda ein. Diese Aufgabe ist um so brisanter, je stärker sein Unternehmen im Internet präsent ist und je engmaschiger es mit Kunden und Lieferanten vernetzt ist.

Die Bedrohung in der Realität ...

Von allen Gefahrenquellen für die IT-Sicherheit halten Computerviren die Sicherheitswächter am stärksten in Atem. Drei von vier Unternehmen hatten im vergangenen Jahr mindestens einmal einen Virus im Haus. Diese Art von Störenfrieden rangiert damit weit vor allen anderen Quellen des Ärgers für den Sicherheitsfachmann. Wer allerdings glaubt, mit einer Antivirensoftware sei das Problem elegant aus der Welt zu schaffen, liegt zumindest nicht zu 100 Prozent richtig: Bekanntlich erkennt diese Software Viren auch nicht immer. Selbst dann nicht, wenn sie optimal über Mail- und andere Server, Arbeitsplatzrechner und Internetzugänge verteilt ist und regelmäßig aktualisiert wird. Und selbst die perfekte Antivirensoftware hat unangenehme Nebenwirkungen: "Weil diese Software immer komplexere Checks durchführen muss, geht sie mit zunehmender Zahl der Virensignaturen allmählich an die Performance", warnt Jürgen Gulbins, IT-Consultant und Sicherheitsspezialist. Außerdem dauere der Start-up der Rechner länger, das koste produktive Arbeitszeit. Insofern sind aufmerksame und geschulte Mitarbeiter im Kampf gegen die Schädlinge enorm wichtig.

Daten sind das A und O der betrieblichen IT, sie sind für das Unternehmen wertvoller als die Software oder die Rechner, auf denen sie abgelegt sind. Daher gilt deren Verlust als größter anzunehmender Unfall in einem Datenzentrum. Aber in der Praxis

ist der Datenverlust, resultiere er nun aus einem Versagen der Technik oder aus menschlichen Unzulänglichkeiten, eine wesentlich seltenere Erscheinung als der Virenbefall. Mit "nur" 23,3 Prozent der Nennungen rangiert er weit abgeschlagen auf dem zweiten Platz in der "Hitliste" der populärsten Sicherheitsprobleme.

Quelle: silicon.de-Studie IT-Security 2002

Auf den vorderen Rängen der real erlebten Bedrohungen rangieren auch der unerlaubte Zugriff auf Netzressourcen und der Befall mit Trojanern. Bemerkenswert: Mit betrügerischen 0190-Dialern hatte eine signifikante Minderheit unter unseren Lesern zu kämpfen - ein Hinweis darauf, dass noch immer einige User von ihrem Firmencomputer aus im Internet auf anrüchigen Seiten surfen. Diese ärgerliche Erscheinung ist allerdings auf Kleinbetriebe und Zweigstellen mit Modem- oder ISDN-Zugang beschränkt. Mit zunehmender Verbreitung von breitbandigen Internetzugängen wie xDSL oder Standleitungen wird sich das Problem der 0190-Dialer erledigen, weil Dialer damit generell entfallen. Die Surfmoral der Mitarbeiter wird dadurch allerdings nicht besser - dazu bedarf es einer entsprechenden Regelung zwischen Arbeitgeber und Arbeitnehmer.

... und in den Köpfen

Die einsame Spitzenstellung des Virenthemas hat sich im Bewusstsein der Befragten nachhaltig niedergeschlagen. Auf die Frage, welche Faktoren die größte Gefahr für die Sicherheit der IT darstellten, setzen die Herren über Bits und Bytes fast einhellig die Viren auf Platz eins ihrer Prioritätenliste.

An zweiter Stelle der subjektiv empfundenen Gefährdungen für die IT-Sicherheit rangiert die Angst vor dem unberechtigten Zugang. Dagegen helfen Zugangskontrollen und Passwörter, die wiederum bestimmten Regeln für ihren regelmäßigen Austausch unterliegen. Das scheint einigermaßen zu klappen, denn in der Hierarchie der realen Gefahren nimmt der Zugang ohne die entsprechenden Rechte nur eine vergleichsweise untergeordnete Stellung ein.

Das Einschleusen von Trojanern, Datenverlust, Datendiebstahl und der Verlust der Systemintegrität - etwa durch technische Fehler - zaubern jedoch vielen IT-Leitern und Administratoren Sorgenfalten auf die Stirn.

Die Sicherheitsverantwortlichen, so eine wichtige Erkenntnis der Umfrage, sehen ihre Aufgabe nicht nur in der Beherrschung technischer Hilfsmittel. Die menschlichen und organisatorischen Aspekte des Themas rangieren ebenso weit vorne. Fast vier von fünf Befragten räumten "weichen" Maßnahmen wie der Heranbildung eines Sicherheitsbewusstseins bei den Mitarbeitern den gleichen Rang ein wie die eher technisch zu verstehenden Sicherung des Netzwerks.

Das sieht auch der Meta-Group-Sicherheitsexperte Carsten Casper so: "Organisatorische Maßnahmen und das Etablieren von Prozessen zur Sicherung der Infrastruktur gehören auf der Tagesordnung ganz nach oben".

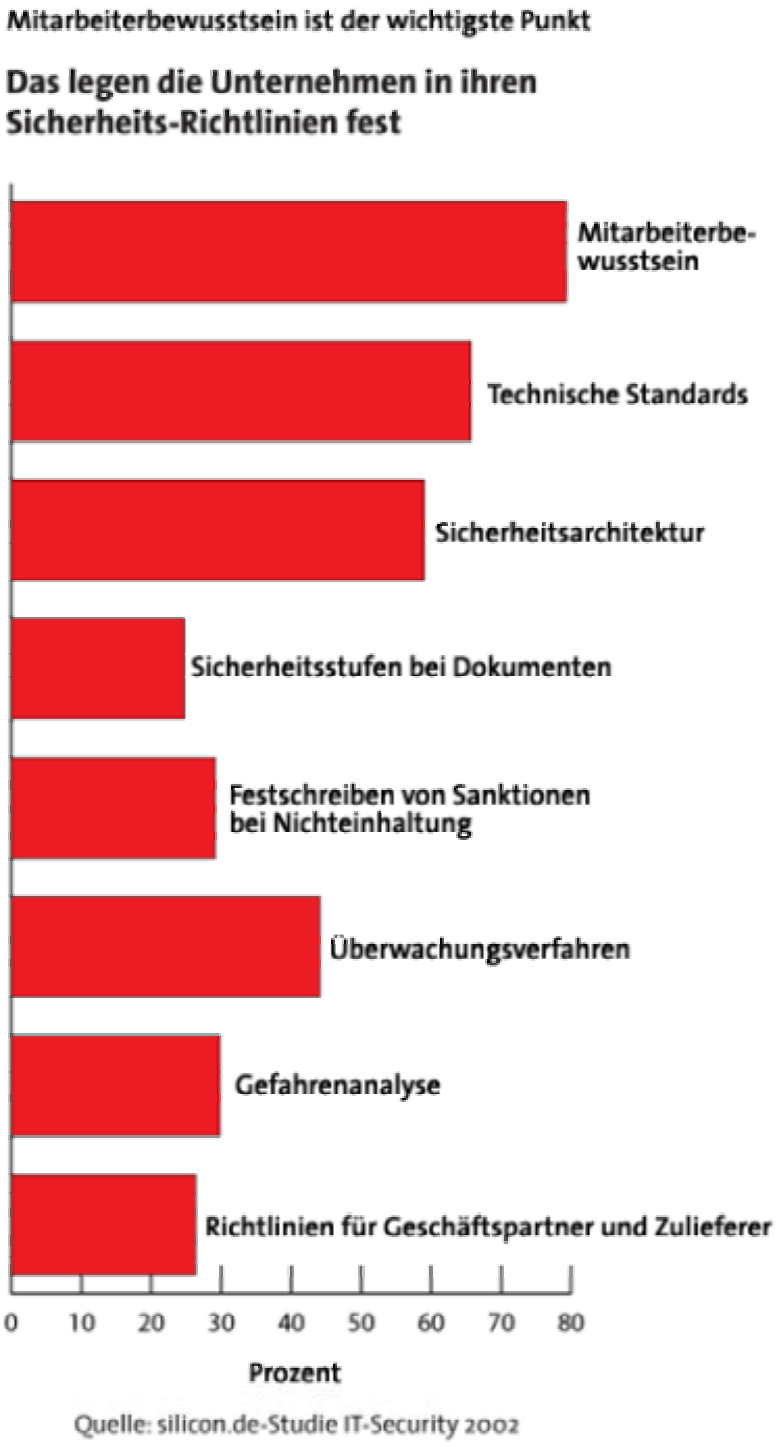
Auch dass die IT-Sicherheit in immerhin fast 30 Prozent der befragten Unternehmen mittlerweile Chefsache ist, begrüßt Casper. Trotzdem sei noch eine Menge Verbesserungspotenzial da. "Die weichen Faktoren werden noch zu wenig genannt", bedauert er.

Strategische Richtlinien gefordert

Eine der vornehmsten Aufgaben des Managements sei die Erarbeitung von Richtlinien für die IT-Sicherheit, so Casper. In diesem Prozess scheinen die Unternehmen noch nicht sehr weit gekommen zu sein: Nur in jedem fünften Betrieb existiert ein umfassendes schriftliches Regelwerk für den Umgang mit IT-Ressourcen. Solche Richtlinien sollten beispielsweise die private Nutzung von Rechnern und den Umgang mit fremder Software regeln, ebenso wie sie festlegen sollten, was die Mitarbeiter im Internet tun dürfen und was nicht.

Fast doppelt häufig wie durch ein umfassendes Regelwerk wird die Sicherheitsfrage durch eine Reihe unzusammenhängender Anweisungen geregelt, die aber immerhin in schriftlicher Form vorliegen. In mehr als 25 Prozent der Betriebe gibt es dazu sogar lediglich mündliche Vorgaben.

"Leider noch zu viel Stückwerk", kritisiert Casper, "es wäre wichtig, dass die Sicherheitsrichtlinien eine umfassende Strategie reflektieren und daher aus einem Guss sind".



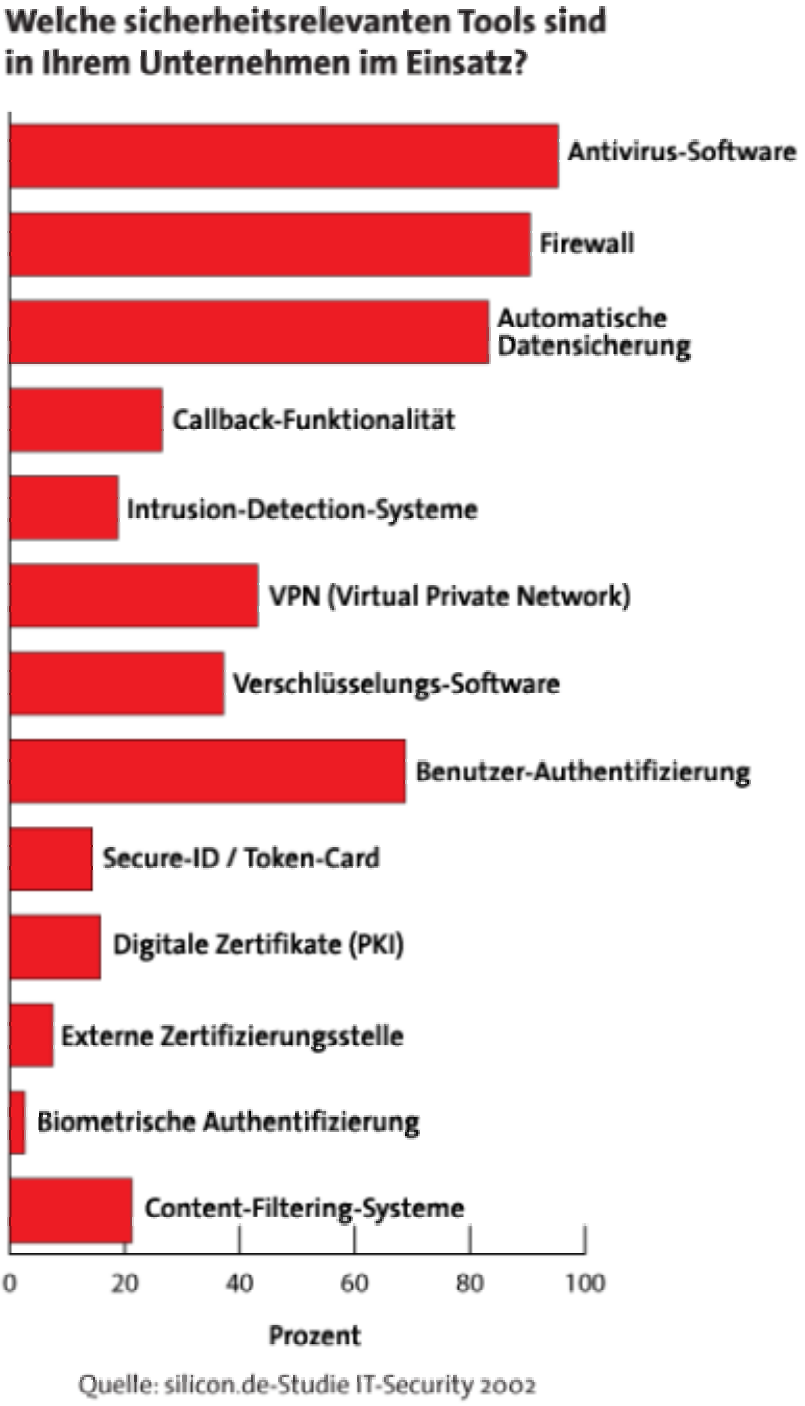
Sind schriftliche oder mündliche Richtlinien vorhanden, so steht der Faktor Mensch an erster Stelle: In fast 80 Prozent der Fälle enthalten die Richtlinien Anleitungen, die unmittelbar an das Mitarbeiterbewusstsein gerichtet sind. Immerhin in 30 Prozent der Fälle sehen die Regeln Sanktionen disziplinarischer oder personeller Art für Verstöße vor; ebenso häufig enthalten sie eine Gefahrenanalyse. Allerdings ist nicht zu

übersehen, dass im Maßnahmenkatalog der Unternehmen technische Gesichtspunkte wie Standards, Überwachungsverfahren oder Dokumenten-Klassifizierung wieder den breitesten Raum einnehmen.

Technische Maßnahmen

Die sicherheitstechnische Praxis spiegelt die subjektiv empfundene Bedrohungslage wider: Bei mehr als 95 Prozent der Befragten versieht eine Antivirensoftware ihren Dienst. Mithin verzichtet nicht einmal jeder zwanzigste User auf dieses Hilfsmittel im Abwehrkampf gegen die digitalen Quälgeister. Auch Firewalls sind aus den Betrieben nicht mehr wegzudenken; neun von zehn Anwendern setzen dieses Instrument gegen unerwünschten virtuellen Besuch ein.

Auch die automatische Datensicherung halten die meisten Anwender, über 80 Prozent, für unentbehrlich. Damit reduzieren die Anwender die Gefahr eines Datenverlustes doch erheblich. Die bereits weiter oben besprochene Feststellung, dass sich immerhin mehr als jeder fünfte Betrieb im Berichtszeitraum mit diesem Problem konfrontiert sah, ändert daran nichts: Die Umfrage forscht nicht danach, ob der einmal eingetretene Datenverlust noch zu beheben war, etwa durch Verwendung von Backup-Daten.

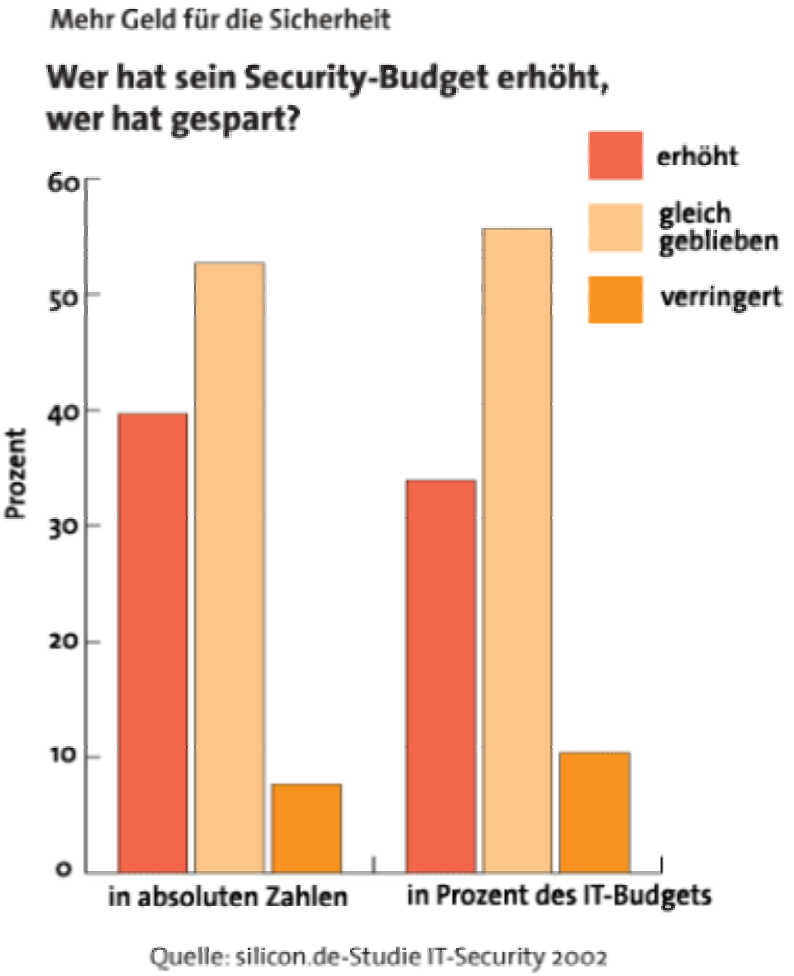


Die Digitale Signatur wird von vielen Experten als wesentliches Element für die Sicherheitsarchitektur der Unternehmen gepriesen. Von einer Akzeptanz dieser Technik auf breiter Front kann indessen nicht die Rede sein. Unsere Umfrage zeigt, dass sie lediglich eine recht kleine Minderheit der Anwender nutzt und davon auch nur jeder zweite Betrieb auf die Dienste externer Zertifizierungsstellen zurückgreift. Eine nähere Analyse des Zahlenwerks macht deutlich, dass die digitale Signatur und

entsprechende Zertifizierungsservices in Klein- und Mittelbetrieben mit weniger als 500 Mitarbeiter besonders selten anzutreffen sind - ein Hinweis darauf, dass diese Techniken noch zu komplex sind und eine aufwändige Infrastruktur erfordern. Der Rückzug der Deutschen Post aus diesem Geschäft vor wenigen Wochen passt zu dem Bild einer Technik, die an den Bedürfnissen breiter Schichten vorbei entwickelt wurde.

Uneinheitliche Neigung zu Sicherheitsinvestitionen

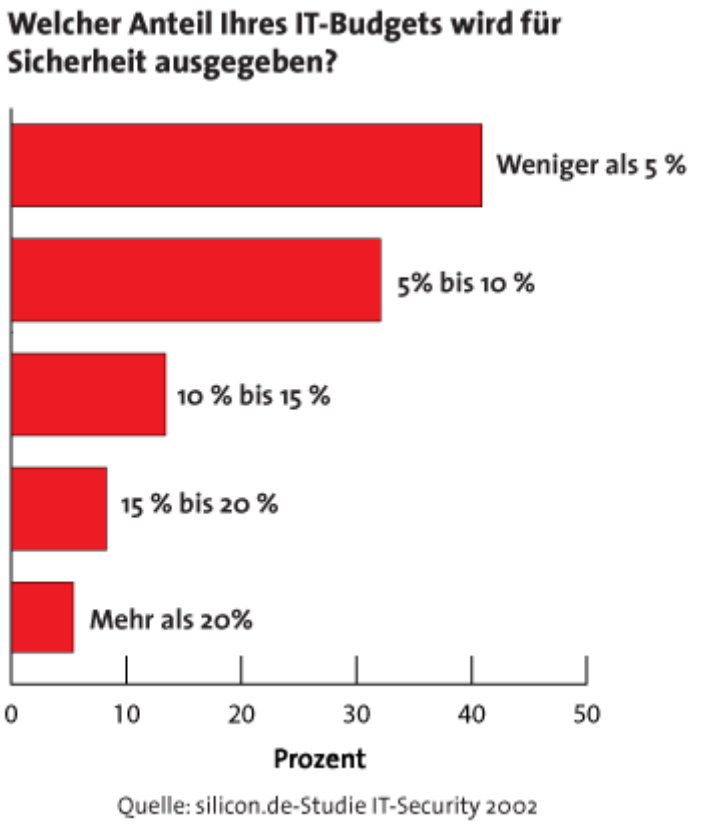
Wie teuer darf die Sicherheit sein? In dieser Frage gehen die Auffassungen der Anwender auseinander. Unsere Umfrage registriert insgesamt einen Trend zu höheren Ausgaben, doch dieser ist schwach und nicht einheitlich über alle Betriebsgrößen und Branchen ausgeprägt. Dass die IT-Budgets in diesem Krisenjahr insgesamt eher niedriger ausgefallen sind als in den Vorjahren, dürfte sich herumgesprochen haben. Etwa jeder dritte Anwender versuchte gegenzusteuern, indem er den für die Sicherheit vorgesehenen Anteil ihres Gesamtetats erhöhte. Dem steht eine Minderheit von rund 10 Prozent gegenüber, die den Sicherheitsanteil verringerte. Die große Mehrheit (über 50 Prozent) beließen diesen Anteil unverändert.



Legt man bei der gleichen Frage die absolute Höhe der Ausgaben zugrunde, so zeigt sich ein leicht verändertes Bild: Fast 40 Prozent der User haben in diesem Jahr nach eigenem Bekunden mehr Geld für die Sicherheit als im vergangenen Jahr ausgegeben beziehungsweise eingeplant, das Häuflein der Sparer schmilzt auf knapp acht Prozent.

Die größten Investitionen in die IT-Sicherheit tätigten, wenig überraschend, Unternehmen aus der Kreditbranche und aus dem Dienstleistungswesen. Jeweils sieben Prozent der User aus diesen beiden Bereichen spendieren mehr als 20 Prozent des Gesamt-IT-Etats für die Security. Beim verarbeitenden Gewerbe machte diese sicherheitsbewusste Gruppe nur fünf Prozent aus, im öffentlichen Sektor zieht der Sparkurs von Bund, Ländern und Gemeinden Bremsspuren: Nur 2,4 Prozent der Befragten aus diesem Sektor gaben an, mehr als 20 Prozent des IT-Etats in die Sicherheit zu investieren.

Die insgesamt größte Gruppe der Anwender (41 Prozent) lässt weniger als fünf Prozent des IT-Gesamthaushalts in die Sicherheit fließen. Ein knappes Drittel der Befragten spendiert der Sicherheit zwischen fünf und zehn Prozent des Etats. (Grafik)



Die erhobenen Daten legen den Schluss nahe, dass sich in der deutschen IT-Sicherheitslandschaft Änderungen nur graduell und allmählich vollziehen. Die Änderungen gegenüber der letzten Erhebung von vor einem Jahr sind nur geringfügig. Positiv ist allerdings festzustellen, dass auch die angesichts schrumpfender IT-Budgets zu erwarteten Kürzungen weitgehend ausgeblieben sind oder die Unternehmen ihre Security-Investitionen sogar leicht erhöht haben.

Zur Studie

Die Umfrage wurde im Mai 2002 unter den Lesern von silicon.de durchgeführt. Insgesamt wurden 483 vollständig ausgefüllte Fragebögen abgegeben. 20 Prozent der Anwender kamen aus Kleinbetrieben mit bis zu 19 Mitarbeitern, 22 Prozent der

Teilnehmer verfügen über 20 bis 99 Arbeitsplätze. Die Gruppe der mittelständischen Unternehmen mit 100 bis 499 Mitarbeitern stellt mit knapp 30 Prozent der Teilnehmer die größte Gruppe. In die nächste Größenklasse mit 500 bis 4999 Beschäftigen fallen 18,6 Prozent der Teilnehemer, während Großunternehmen mit über 5000 Arbeitsplätzen zu 9,7 Prozent beteiligt waren.

Hinsichtlich ihrer fachlichen Zuordnung kommen die größten Teilnehmergruppen mit jeweils mehr als 20 Prozent aus der verarbeitenden Industrie, Dienstleistungsgewerbe und IT- beziehungsweise TK-Industrie. Die restlichen Teilnehmer ordneten sich zu wechselnden Anteilen dem Handel, der Öffentlichen Hand, dem Kreditwesen, dem Gesundheitsbereich und den Medien zu.

Rund 13 Prozent der Befragten sind in der Geschäftsleitung tätig, 40 Prozent sind für den IT-Einsatz im Unternehmen verantwortlich. Weitere 12 Prozent managen eine Abteilung im betrieb, 21 Prozent sind IT-Experten. Der Rest entfällt auf betriebswirtschaftlcihe Funktionen und "sonstige Tätigkeiten".

Ziel der Umfrage war es, den Status Quo der Bedrohungsszenarien, der Sicherheitsstrategien des und Ausgabeverhaltens in der deutschen Wirtschaft zu dokumentieren.

Christoph Hammerschmidt