INFORMATIONSSICHERHEIT IN SCHWEIZER UNTERNEHMEN

Eine Umfragestudie über Bedrohungen, Risikomanagement und Kooperationsformen

Zürich, August 2006

CSS
An ETH Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Kontakt:
Center for Security Studies
Seilergraben 45-49
ETH Zentrum / SEI
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch

Inhaltsverzeichnis

Abbildungsverzeichnis

Vorwort

Internetkriminalität gibt es, seit der Computer Feder und Papier vom Schreibtisch verdrängt hat. Seitdem Computer global vernetzt wurden, hat sich die Internetkriminalität stark ausgebreitet. Trotzdem wird die volle Dimension der damit verbundenen Bedrohung noch nicht wahrgenommen; sie versteckt sich teilweise noch immer hinter einem leicht verklärten Bild von etwas Virtuellem und Fiktivem.

Der Schweizerische Bundesrat hat die Bedeutung dieser Problematik erkannt und bereits zwei Mal einem breiten Bedürfnis entsprochen: Einmal, als er die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)[1] einrichtete, ein zweites Mal mit der Schaffung der Melde- und Analysestelle Informationssicherung (MELANI)[2]. Damit wurden zweckmässige und effiziente Strukturen geschaffen, um die Gesellschaft wirksam vor den genannten Bedrohungen zu schützen. Was jedoch noch fehlte, war eine umfassende Auslegeordnung über den Stand des Schutzes sowie der Bedrohungslage aus Sicht der Schweizer Wirtschaft. In anderen Ländern, allen voran in den Vereinigten Staaten, sind solche Studien auf nationaler Ebene in der Form des CSI/FBI Computer Crime and Security Survey[3] schon seit langem verfügbar. So enthält der Jahresbericht 2005 breit abgestützte Fakten wie zum Beispiel, dass über die Hälfte der befragten US-Betriebe im Laufe des Jahres Opfer einer Informatikattacke wurden oder dass 95 Prozent von ihnen eine Beschädigung ihrer Website erlitten. Noch wichtiger aber ist die Feststellung, dass die Kosten pro Informatikattacke zwischen 2004 und 2005 sprunghaft angestiegen sind, nämlich von durchschnittlich rund 51'000 US-Dollar auf rund 300'000 US-Dollar.

Solche Daten dienen nicht nur der Sensibilisierung der Öffentlichkeit. Sie ermöglichen den Unternehmen auch Vergleiche zu ziehen, erlittene Vorfälle in einen grösseren Kontext zu stellen, die Effizienz der getroffenen Massnahmen besser beurteilen zu können und letztlich auch eigenen Handlungsbedarf zu erkennen. Mit der praktischen Umsetzung der schweizweiten Studie wurde die Forschungsstelle für Sicherheitspolitik der ETH Zürich[4] betraut.

Die Ergebnisse bestätigen zum einen bekannte Tendenzen, überraschen zum anderen jedoch auch mit unerwarteten Fakten. Sachverständige werden diesen Bericht ohne Zweifel schätzen; seine leichte Verständlichkeit wird ihn aber auch für alle interessant machen, die sich mit Informationssicherheit befassen – einer Problematik also, der man sich auf Dauer nicht mehr entziehen kann.

Mauro Vignati
MELANI-Analytiker, Projektleiter

1 http://www.scoci.ch.
2 http://www.melani.admin.ch.
3 Computer Security Institute(CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005).
4 http://www.css.ethz.ch.

Die wichtigsten Resultate im Überblick

Eine deutliche Mehrheit der befragten Unternehmen (72%) hat im Jahr 2005 mindestens einen Vorfall in der Informationssicherheit festgestellt.
Am stärksten verbreitet sind Viren, Würmer, Trojanische Pferde und Spyware. Eine relativ häufig festgestellte Bedrohung ist auch der konventionelle Diebstahl von Laptops oder anderer Hardware. Seltener sind gezielte Angriffe auf die Verfügbarkeit, Hacking, Datendiebstahl oder Verunstaltung der Homepage.

Grossfirmen mit mehr als 250 Mitarbeitern und Unternehmen, die über das Internet ein- oder verkaufen, haben ein erhöhtes Risiko eines Vorfalles.
Vor allem gezielte Angriffe richten sich sehr viel häufiger gegen Grossfirmen und Unternehmen, die E-Commerce betreiben.

Fast alle Firmen wenden technische und organisatorische Schutz-massnahmen an.
Von den technischen Massnahmen werden vor allem die Antiviren-Programme und Firewalls in fast allen Unternehmen benutzt. Von den organisatorischen Massnahmen ist das Backup-Management am stärksten verbreitet. Aufwändigere technische und organisatorische Massnahmen (wie z.B. Krisenorganisationen) werden vor allem in Grossfirmen und in Unternehmen der Informatikbranche angewendet.

Die Unternehmen haben wenig finanzielle und personelle Mittel für die Informationssicherheit zur Verfügung.
Nur in wenigen der befragten Firmen (32%) ist zudem ein ausgebildeter Informatiker für die Informationssicherheit verantwortlich.

Viele Firmen lagern ihre Risiken im Bereich der Informationssicherheit aus.
Besonders bei mittleren Firmen ist das Outsourcing beliebt. Häufig werden mögliche Schäden durch Probleme mit der Informationssicherheit auch versichert.

Viele Unternehmen würden eine verstärkte Kooperation untereinander begrüssen.
Die Mehrheit ist dabei der Meinung, dass für die Zusammenarbeit neue Organisationen geschaffen werden müssten. Bei einer möglichen Kooperation gilt es zu beachten, dass die Bedürfnisse der verschiedenen Unternehmen sehr unterschiedlich sind.

1 Einleitung

Die Informations- und Kommunikationstechnologien (IKT) prägen den Alltag der meisten Schweizer Firmen und Behörden. Sie ermöglichen ein vernetztes Arbeiten und vereinfachen die Kommunikation. Mit der Anwendung der neuen Technologien entstanden aber auch neue Probleme. Während man in den 1980er Jahren noch über die Existenz von Computer-Viren diskutierte, sind diese heute weltweit verbreitet und nur noch eine von zahlreichen möglichen Bedrohungen für die Informationssicherheit.

Die zunehmende Abhängigkeit von den Informations- und Kommunikationstechnologien in den verschiedensten Tätigkeitsfeldern sowie die zuweilen beobachtete Sorglosigkeit bei ihrer Nutzung erhöhen die Gefahr von IKT-Pannen, welche das reibungslose Funktionieren von Geschäftsprozessen in der Wirtschaft bedrohen. Ein Ausfall der IKT käme der Schweiz volkswirtschaftlich sehr teuer zu stehen. Eine Studie des Computer Engineering and Networks Laboratory (TIK) der ETH Zürich hat ergeben, dass der wirtschaftliche Schaden eines einwöchigen Internet-Blackout in der Schweiz bei 5,83 Milliarden Franken liegen würde. Die Studie verdeutlicht die Abhängigkeit einer modernen Gesellschaft wie der Eidgenossenschaft von Informatik und Internet. 48 Prozent der 3,6 Millionen Arbeitsplätze in der Schweiz sind auf die IKT angewiesen.[5]

Angesichts dieser Situation ergreifen die Unternehmen verschiedene Massnahmen – je nach Sicherheitsbedürfnis und den Mitteln, die sie zur Verfügung haben. Diese können von technischen über organisatorische Schutzmassnahmen bis hin zur allgemeinen Sensibilisierung der Mitarbeiter reichen.

Das Ziel dieser Studie ist es, einen Überblick über die Bedrohungen der Schweizer Wirtschaft im Bereich der Informationssicherheit zu erhalten, und zu erfahren, wie Unternehmen und Behörden mit diesen umgehen. Zusätzlich soll untersucht werden, ob in diesem Bereich eine Kooperation zwischen den Firmen denkbar ist und wie die Unternehmen beim Schutz ihrer IKT vom Staat unterstützt werden könnten.

1.1 Methode der Studie

Um einen möglichst breiten Überblick zu gewinnen, wurde eine schriftliche Umfrage bei Firmen und Behörden aus allen Grössenkategorien, aus allen Landesteilen und aus allen Branchen des zweiten und dritten Sektors (industrieller Sektor und Dienstleistungssektor) durchgeführt. Insgesamt wurden 4916 Firmen und Behörden per E-Mail oder brieflich angeschrieben.[6] Um den administrativen Aufwand so klein wie möglich zu halten, wurde der Fragebogen nicht physisch verschickt, sondern war über den versandten Link mittels Passwort auf dem Internet aufrufbar. Der Fragebogen bestand aus 36 Fragen und war während vier Wochen (15.03.2006-13.04.2006) für die Teilnehmer der Studie zugänglich.[7] Während dieser Zeit wurde der Fragebogen 562 mal ausgefüllt. Die Rücklaufquote beträgt somit 11.45%, was im üblichen Bereich für ähnliche Umfragen liegt.[8]

5 Dübendorfer, Thomas, Arno Wagner und Bernhard Plattner, *An Economic Model for Large-Scale Internet Attacks* (Studie des Computer Engineering and Networks Laboratory der ETH Zürich, 2004), S. 4.

6 Zur Auswahl und Zusammensetzung der Stichprobe siehe Anhang 1.

7 Der Fragebogen und Details zur Erhebungsmethode befinden sich im Anhang 5.

8 Für eine detaillierte Auswertung des Rücklaufes siehe Anhang 2.

1.2 Forschungsstand und Vergleichsstudien

Die meisten bisherigen Studien im Bereich der Sicherheit der IKT setzten sich ausschliesslich mit den technischen Aspekten auseinander oder sind als Handlungsempfehlungen für die Verantwortlichen in den Unternehmen gedacht. Bestandesaufnahmen über die Informationssicherheit in Schweizer Firmen gibt es noch nicht. Hilfreich für diese Studie war jedoch die Untersuchung „Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz" der Task Force KMU aus dem Jahr 2002[9], da es bei der Analyse der Informationssicherheit wichtig ist zu wissen, welchen Stellenwert die Informatik in den unterschiedlichen Firmen hat.

In anderen Ländern wurden teilweise bereits umfassende Analysen über die Informationssicherheit in den Unternehmen durchgeführt. Deshalb sollen die Ergebnisse jeweils mit den internationalen Studien verglichen werden. Vor allem der „FBI Computer Crime Survey 2005"[10], die Studie „Hi-Tech Crime: The Impact on UK Business 2005" der britischen National Hi-Tech Crime Unit[11], sowie der Bericht „Die Lage der IT-Sicherheit in Deutschland 2005" des deutschen Bundesamtes für Sicherheit in der Informatik (BSI) sind wichtige Quellen für Vergleichsdaten.[12]

1.3 Terminologie

In diesem Abschnitt folgt die Definition der in vorliegender Studie häufig verwendeten Begriffe.

Informationssicherheit
Informationssicherheit soll die unautorisierte Informations- bzw. Datenveränderung oder -gewinnung verhindern. Die Realisierung einer möglichst hohen Informationssicherheit wird durch einen Prozess gewährleistet, der neben (system)technischen auch betriebliche und organisatorische Massnahmen zum Schutz der Informationen umfasst.

Schutzziele in der Informationssicherheit
Authentizität: Unter Authentizität eines Objekts (z.B. Daten, Systeme, Server etc.) bzw. Subjektes (User) wird die Echtheit ihrer Identität verstanden, wobei diese anhand eindeutiger Eigenschaften überprüfbar sein muss.
Integrität der Daten: Datenintegrität ist gewährleistet, wenn es Subjekten und Objekten nicht möglich ist, die zu schützenden Daten unautorisiert zu verändern.
Vertraulichkeit: Ein System gewährleistet Vertraulichkeit, wenn es jegliche unautorisierte Informationsgewinnung, auch während des Datentransports, verhindert.
Verfügbarkeit: Ein System gilt dann als verfügbar, wenn authentifizierte und autorisierte Subjekte in der Ausübung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.

9 Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Studie im Auftrag des Staatssekretariates für Wirtschaft, Bern, 2002).

10 Computer Security Institute(CSI)/Federal Bureau of Investigation (FBI), 2005 Computer Crime and Security Survey (2005). http://www.gocsi.com.

11 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005). http://www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf.

12 Bundesamt für Sicherheit für Sicherheit in der Informationstechnik (BSI), *Die Lage der IT-Sicherheit in Deutschland 2005* (Juli 2005). http://www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf.

Verwundbarkeit
Unter Verwundbarkeit wird eine Schwachstelle im System verstanden, welche die oben definierten Schutzziele gefährden kann. Verwundbarkeiten können gegenüber physischen Gefahren (Feuer, Wasser, Erdbeben, Blitzschlag, Stromausfall), unsachgemässer Nutzung oder beispielsweise auch gegenüber Malware bestehen.

Bedrohung
Eine Bedrohung des Systems liegt dann vor, wenn eine oder mehrere Verwundbarkeiten bestehen, welche die oben definierten Schutzziele verletzen könnten.

Risiko
Das Risiko bezeichnet die Wahrscheinlichkeit (oder relative Häufigkeit), mit der eine Bedrohung zu einem Schadensereignis führt sowie die mit dem Schaden einhergehenden Kosten. Damit ist das Risiko auch abhängig von der Höhe der zu schützenden Werte.

Angriff / Vorfall
Ein Angriff bezeichnet einen nicht autorisierten Zugriff oder Zugriffsversuch auf ein System. Unterschieden wird in passive Angriffe (unautorisierte Informationsgewinnung, Verlust der Vertraulichkeit) und aktive Angriffe (unautorisierte Modifikation von Daten, Verlust der Integrität oder Verfügbarkeit).[13]

In dieser Studie wird allerdings meist allgemeiner von Vorfällen gesprochen, damit deutlich wird, dass auch Fehlmanipulationen ohne böse Absicht zu Problemen mit der Informationssicherheit führen können.

13 Die Definitionen sind vereinfacht und zusammengefasst übernommen aus: Eckert, Claudia, *IT-Sicherheit: Konzepte – Verfahren – Protokolle* (3. überarb. und erw. Auflage, München und Oldenbourg 2004), S. 4-17.

2 Häufigkeit der Vorfälle

In diesem ersten Teil der Analyse wird die Häufigkeit der Vorfälle, die Bedrohung der Informationssicherheit durch die Mitarbeiter der Unternehmen sowie das Risiko eines Vorfalls nach Art der Unternehmen und Form der Bedrohung untersucht. Zunächst muss aber erläutert werden, welche Bedrohungen für die Informationssicherheit berücksichtigt werden und wie diese definiert sind. Die Ausführungen zu den einzelnen Bedrohungen werden kurz gehalten, da sich genauere Informationen leicht im Internet und in der Literatur finden lassen.[14]

2.1 Bedrohungen der Informationssicherheit

Die Firmen wurden zu den wichtigsten bekannten Bedrohungen für die Informationssicherheit befragt. Grundsätzlich kann die Vertraulichkeit, die Verfügbarkeit sowie die Integrität der Daten bedroht sein. In der Befragung wurde Spam (auch Junk-Mails genannt), also die unerwünschte Werbung über E-Mail, nicht untersucht. Diese E-Mails können zwar sehr lästig sein, stellen jedoch in der Regel keine direkte Bedrohung für die Informationssicherheit dar.

2.1.1 Beschreibung der untersuchten Bedrohungen

Viren, Spyware, Würmer und Trojanische Pferde (allgemeine Malware)
Ein *Virus* besteht aus Programmanweisungen, die dem Rechner die auszuführenden Aktionen vorgeben. Um sich weiterzuverbreiten, nistet sich der Virus in einem "Wirtprogramm" ein. Das "Wirtprogramm" kann eine Anwendung (z.B. heruntergeladene Software) oder ein Dokument (z.B. eine Word-Datei, Excel-Datei) sein. Beim Ausführen der Anwendung oder beim Öffnen des Dokuments wird der Virus aktiviert, so dass der Rechner dazu gebracht wird, schädliche Aktionen auszuführen. Viren gelangen häufig über Anhänge in E-Mails oder über infizierte Dateien, die vom Internet heruntergeladen werden, auf den Rechner. Einmal aktiviert, können sie sich auch per E-Mail an Kontakte im Adressbuch weiterversenden. Weitere Verbreitungswege sind externe Datenträger (z.B. CD-ROM, USB Memory Stick, usw.).

Spyware soll ohne Wissen des Benutzers Informationen sammeln und diese an eine vordefinierte Adresse übermitteln. Welche Informationen ausgelesen werden, hängt dabei von der jeweiligen Spyware ab und kann von Surfgewohnheiten über Systemeinstellungen bis hin zu Passwörtern oder vertraulichen Dokumenten gehen.

Würmer bestehen, wie Viren, aus Programmanweisungen, die dem Rechner die auszuführenden Aktionen vorgeben. Im Gegensatz zu Viren benötigen Würmer zur Verbreitung jedoch kein Wirtprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten. Mögliches Ziel für einen Wurm sind Rechner, die Sicherheitslücken oder Konfigurationsfehler aufweisen und in irgendeiner Form mit anderen Rechnern (z.B. über das Internet, das lokale Netzwerk, usw.) verbunden sind.

Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder

14 Infos auf: http://www.melani.admin.ch/gefahren-schutz/gefahren/index.html?lang=de. In der Literatur finden sich zahlreiche Übersichtswerke zur Informationssicherheit. Ausführlich dazu: Bidgoli, Hossein et.al. (eds.), *Handbook of Information Security Volume 3* (Hoboken, 2006).

Datei tarnen. Häufig sind Trojanische Pferde Programme, die im Internet heruntergeladen werden. Jedoch auch bei Musikstücken oder Filmen kann es sich um Trojanische Pferde handeln. Diese nutzen Sicherheitslücken in den jeweiligen Abspielprogrammen (z.B. Media Player), um sich unbemerkt auf dem System zu installieren. Häufig werden Trojanische Pferde ebenfalls über Anhänge in E-Mails verbreitet. Sie dienen meist der Spionage vertraulicher Daten, der vollständigen Übernahme des Rechners oder zum Spamversand über den infizierten Rechner.

Angriffe auf die Verfügbarkeit (Denial of Service, DoS)

Angriffe auf die Verfügbarkeit haben zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. Eine populäre Variante von DoS Attacken im IT-Bereich ist das Senden sehr vieler Anfragen an einen Rechner/Dienst. Durch die vielen Anfragen wird der Rechner/Dienst so überlastet, dass er für die Antworten sehr viel Zeit benötigt oder gar ganz ausfällt.

Die Angriffe kommen häufig von verschiedenen Rechnern, die zuvor mittels Malware manipuliert worden sind. Man spricht dann von Distributed (verteilten) Denial of Service-Attacken (DDoS). Effektiv sind diese Angriffe vor allem gegen Firmen, die über das Internet Geschäfte abwickeln wollen. Sie treten häufig zusammen mit Erpressungen auf.

Weil viele Rechner unbemerkt mit Malware infiziert sind und darum von Hackern missbraucht werden können, steigt auch die Bedrohung durch DDoS-Angriffen. Wenn mehrere manipulierte Computer nämlich zu einem Netz (sogenannte Bot-Netze) zusammengeschlossen werden, lassen sich leicht DDoS-Angriffe durchführen. Experten warnen deshalb vor einer möglichen Zunahme dieser Angriffe.

Eindringen in das System (Hacking) und Datendiebstahl

Hacking ist kein genau definierter Begriff. Häufig wird er für alle Arten von unerwünschten Manipulationen an fremden Computern gebraucht. Hier soll Hacking das unerlaubte Eindringen in das Informatiksystem eines Unternehmens bezeichnen. Dies gelingt oft über den gezielten Einsatz von Spionageprogrammen (Spyware, Trojanische Pferde). Hacker können im System, in welches sie eingedrungen sind, Daten lesen, ändern oder löschen. Den grössten Schaden verursachen kriminell motivierte Hacker, die einem Unternehmen Daten stehlen. Vertrauliche Daten von Kunden oder neu entwickelte Ideen, von denen das wirtschaftliche Überleben der Unternehmen abhängt, sind oft Ziele solcher Angriffe. Ein Datendiebstahl kann deshalb sehr ernste Folgen für eine Firma haben. Diese Art von Angriffen ist meist nur schwer zu erkennen.

Verunstaltung der Homepage (Defacement)

Die Verunstaltung von einzelnen oder mehreren (Mass Defacement) Homepages geschieht über Sicherheitslücken in den Webservern. Der Inhalt und das Design der Homepages werden dann von den Angreifern verändert. Teilweise sind diese Angriffe politisch motiviert und werden von sogenannten „Hacktivisten“ ausgeführt, um einen politischen Protest zu platzieren. Oft werden die Homepages aber auch von „Script-Kiddies“ zum Spass verunstaltet. Je nachdem, wie wichtig die Homepage für die Geschäftstätigkeit eines Unternehmens ist, reichen die Folgen solcher Angriffe von Imageschaden bis zu erheblichen finanziellen Verlusten.

Missbrauch der Wireless-Netzwerke

Die Wireless Local Area Networks (WLAN) bieten einen drahtlosen und unkomplizierten Zugang zum Internet. Sie sind aber vielfach ungenügend geschützt. Über diese mangelhaft

geschützten Zugänge können Angreifer die Verbindung für verschieden Zwecke missbrauchen. Problematisch ist vor allem, dass der Missbrauch der Wireless-Netzwerke meist spät oder gar nicht bemerkt wird.

Konventioneller Diebstahl von Laptops und anderem Informatikmaterial
Bei allen neuen Formen der Bedrohung darf nicht vergessen werden, dass das Informatikmaterial auch auf konventionelle Art gestohlen werden kann. Neben dem Verlust des Materialwerts kann es dabei zu grossen zusätzlichen Schäden kommen, wenn beispielsweise auf einem entwendeten Laptop sensible Daten gespeichert worden sind.

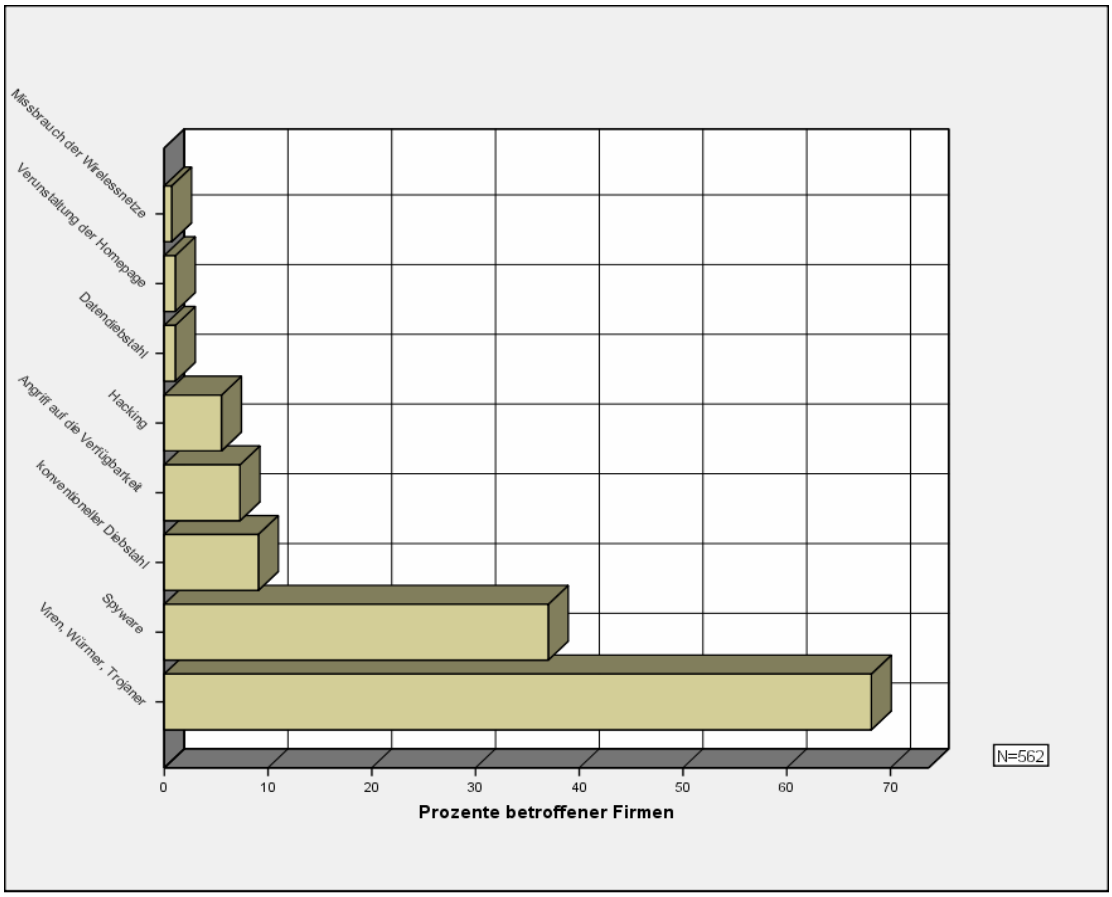
2.1.2 Häufigkeit der Vorfälle

In der Befragung wurde erhoben, ob die Unternehmen im Jahr 2005 von den beschriebenen Bedrohungen betroffen wurden. Die Auswertungen zeigen, dass Vorfälle in der Informationssicherheit häufig vorkommen. 72% der Firmen, welche an der Umfrage teilgenommen haben, geben an, dass mindestens eine der oben skizzierten Bedrohungen zu einem Vorfall in ihrer Informationsinfrastruktur geführt hat. Es muss aber beachtet werden, dass die Teilnehmer der Umfrage kein proportionales Abbild der Realität repräsentieren. Beispielsweise sind 15% der Teilnehmer der Umfrage Grossunternehmen mit mehr als 250 Mitarbeitern, während in der Realität nur 0.4% aller Firmen eine solche Grösse erreichen. Zusätzlich sind unter den befragten Firmen auch einige Branchen stärker vertreten als in der Wirklichkeit.[15] Wegen dieser unproportionalen Zusammensetzung der befragten Firmen, darf von den Aussagen über den Durchschnitt der Teilnehmer der Umfrage nicht direkt auf den Durchschnitt aller Schweizer Unternehmen aus dem zweiten und dritten Sektor geschlossen werden. Weil aber dennoch Schätzungen über die reale Häufigkeit der Vorfälle gemacht werden sollen, wird das statistische Verfahren der Gewichtung angewendet. Dabei wird die Realität simuliert, indem die Angaben der Firmen verschieden bewertet werden.[16] Wenn nun dieses Verfahren eingesetzt wird, lässt sich der Anteil der Schweizer Unternehmen, die im Jahr 2005 mindestens einen der beschriebenen Vorfälle bemerkt haben, auf 63% schätzen.

Weil die verschiedenen Bedrohungen sehr unterschiedliche Konsequenzen haben, ist es wichtig zu wissen, wie oft die einzelnen Vorfälle vorkommen. In Abbildung 1 wird ersichtlich, welche Vorfälle wie viele der befragten Firmen und Behörden betroffen haben.

15 Zum Rücklauf nach Grössenklassen und Branchen siehe Anhang 2.
16 Alle Daten werden mit einem Gewichtungsfaktor multipliziert. Mehr Informationen zum Verfahren der Gewichtung finden sich im Anhang 3.

Abbildung 1 Häufigkeit der Vorfälle



Es wird deutlich, dass Malware (Viren, Würmer, Trojanische Pferde und Spyware) klar am stärksten verbreitet ist. Gleich an dritter Stelle folgt der konventionelle Diebstahl von Informatikmaterial. Die technisch aufwändigeren, aber in ihren Konsequenzen auch gravierenderen Angriffe werden sehr viel seltener entdeckt.

2.1.3 Die Bedrohung durch eigene Mitarbeiter

Kenntnisse über die Häufigkeit der Vorfälle helfen, das Risiko für die Unternehmen besser abschätzen zu können. Dazu ist es aber auch wichtig zu wissen, wo die Vorfälle ihren Ursprung haben. Insbesondere interessiert die Frage, für wie viele Vorfälle die eigenen Mitarbeiter verantwortlich sind.

Mitarbeiter können aus verschiedenen Gründen die Informationssicherheit ihrer Unternehmen gefährden. Einerseits ist es oft ihr Fehlverhalten, welches das Eindringen von Malware oder auch gezielte Angriffe erst möglich machen, andererseits können sie selbst die Urheber eines Angriffs sein – zum Beispiel aus Gründen der Bereicherung oder der Rache an Vorgesetzten. Viele Experten schätzen, dass die Mitarbeiter für einen hohen Anteil der Vorfälle direkt verantwortlich sind.[17] Auch die britische Studie „Hi-Tech Crime: The Impact on UK

17 In einem Bericht von Gartner wird gar davon ausgegangen, dass 70% der Missbräuche der Informatik durch die Mitarbeiter betrieben werden. Gartner Research, *Enterprises and Employees: The Growth of Distrust* (2005). Zusammenfassung der Resultate auf: http://www.csoonline.com/analyst/report3317.html. Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik geht von einem hohen Anteil an Innentätern aus: Bundesamt für IT-Sicherheit, *Die Lage der IT-Sicherheit in Deutschland 2005* (Juli 2005), S. 29.

Business 2005“ ergab einen hohen Anteil an Innentätern. 37% der registrierten Vorfälle in britischen Unternehmen können gemäss dieser Studie auf bewusste Manipulationen durch unehrliche oder unzufriedene Mitarbeiter zurückgeführt werden.[18] In vorliegender Studie ist das nur bei 10% der befragten Firmen der Fall, womit der Prozentsatz deutlich tiefer liegt als erwartet. Es darf jedoch kein direkter Vergleich mit der britischen Studie gemacht werden, da bei dieser teilweise andere Bedrohungen untersucht worden sind und nur Firmen mit mehr als 100 Mitarbeitern teilgenommen haben.

Dennoch kann festgehalten werden, dass die Vorfälle, die direkt auf einen Mitarbeiter zurückgeführt werden können, in der Schweiz eher selten sind. Absichtlich fügen die Mitarbeiter der Firma nur in Ausnahmefällen Schäden zu. Die Bedrohung der Informationssicherheit durch unabsichtliches Fehlverhalten dürfte wesentlich grösser sein.

2.1.4 Die Häufigkeiten der Vorfälle im internationalen Vergleich

Wie sind nun die erhobenen Häufigkeiten der Vorfälle im Vergleich mit ausländischen Studien zu bewerten? In der breit angelegten Umfrage „Computer Crime Survey 2005“ des FBI gaben 87% der Teilnehmer an, einen Vorfall festgestellt zu haben. Es wurden dabei aber nur Firmen mit mehr als fünf Vollzeitstellen berücksichtigt. Für den Vergleich müssen also alle Kleinstfirmen mit weniger als fünf Mitarbeitern aussortiert werden. Von allen Firmen und Behörden in der Schweiz mit mehr als fünf Mitarbeitern haben 79% einen Vorfall festgestellt. Dies liegt etwas unter dem Wert der FBI-Studie, was sich aber auf den Umstand zurückführen lässt, dass die Vorfälle in der FBI-Studie etwas umfassender definiert sind. So zählt in dieser Studie beispielsweise auch das Entdecken von pornographischem Material zu den Vorfällen.

Auch die bereits zitierte britische Studie „Hi-Tech Crime: The Impact on UK Business 2005“ zeigt, dass die Schweiz ähnliche Probleme hinsichtlich der Informationssicherheit hat wie andere Länder. In dieser Umfrage unter Grossfirmen mit mehr als 100 Mitarbeitern ergab sich, dass 89% im Jahr 2004 einen Vorfall festgestellt haben. Wenn nur die Angaben der Firmen mit mehr als 100 Angestellten berücksichtigt werden, sind auch in der Schweiz 85% betroffen.

Auch was die Art der Vorfälle betrifft, entsprechen die Ergebnisse ungefähr jenen der internationalen Studien. Die FBI-Studie ergab ebenfalls, dass Viren und Spyware das mit Abstand häufigste Problem sind, dass konventioneller Diebstahl recht oft vorkommt und dass gezielte Angriffe eher selten sind.

Man kann also sagen, dass die Schweizer Unternehmen weder mehr noch weniger Vorfälle feststellen als die Unternehmen anderer Länder. Wegen der globalen Vernetzung betreffen eben auch die Bedrohungen für die Informationssicherheit die Unternehmen aus allen Ländern in ähnlichem Ausmass.

18 The National Hi-Tech Crime Unit (nhctu), *Hi-Tech Crime, The Impact on UK Business 2005* (2005), S.20.

2.2 Das Risiko eines Vorfalls nach Art der Firma

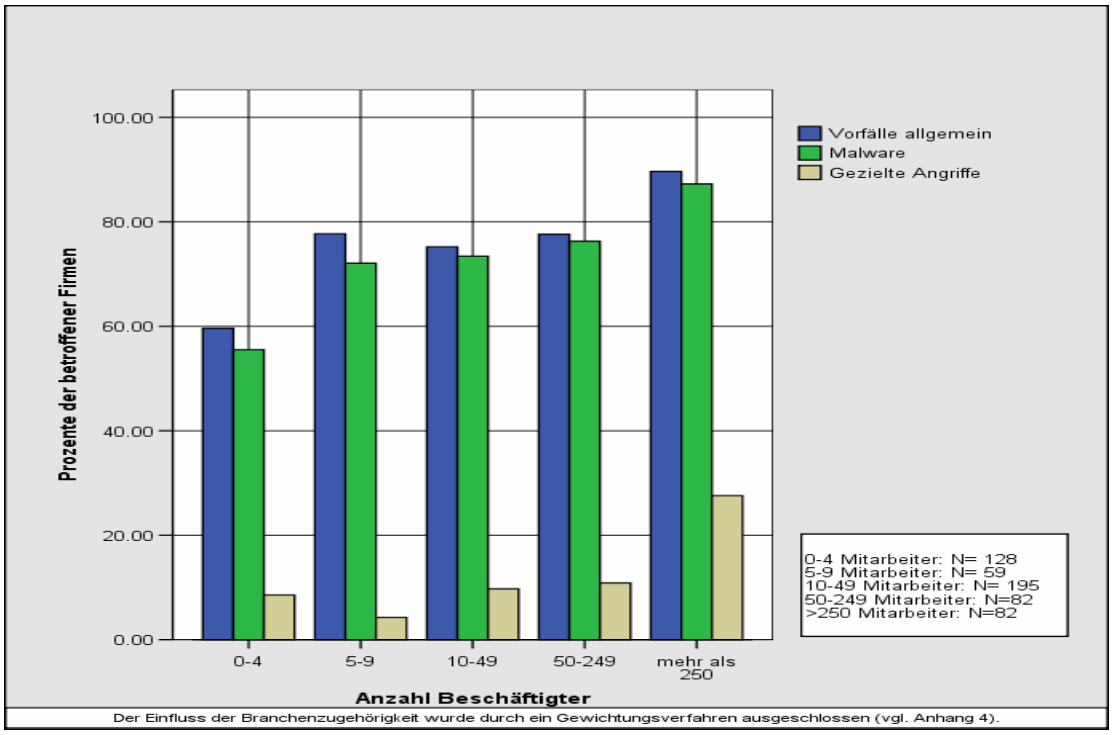
Während die Staatszugehörigkeit der Unternehmen also keinen entscheidenden Einfluss auf das Risiko eines Vorfalls hat, kann vermutet werden, dass die Grösse und das Tätigkeitsfeld einer Firma die Wahrscheinlichkeit von Malware und gezielten Angriffen beeinflussen. Im Folgenden geht es darum, zu untersuchen, welche Art von Firmen besonders häufig von Vorfällen betroffen ist.

2.2.1 Das Risiko nach Unternehmensgrösse

In der Studie der KMU Taskforce zur Verbreitung der Informatik und des Internets in den Unternehmen wurde nachgewiesen, dass zwischen der Unternehmensgrösse und der Nutzung der Informatik ein Zusammenhang besteht. Je grösser ein Unternehmen ist, desto wichtiger werden die Informatik- und Internettechnologien.[19] Mit der intensiveren Nutzung dieser Mittel steigt aber auch das Risiko von Vorfällen. Je mehr Mitarbeiter beispielsweise E-Mails verschicken und empfangen, desto grösser ist die Wahrscheinlichkeit, dass Viren in das Firmennetzwerk eindringen können. Zudem sind die grösseren Firmen attraktiver für gezielte Angriffe. Der Aufwand, der für einen gezielten Angriff nötig ist, lohnt sich für die Hacker nämlich nur, wenn die angegriffene Firma genügend Umsatz macht oder über genügend grosse Vermögenswerte verfügt, die in der einen oder anderen Form angegriffen respektive entwendet werden können. Bei grösseren Unternehmen ist natürlich jeweils mehr Geld zu holen als bei kleineren.

Abbildung 2 zeigt, wie die Wahrscheinlichkeit eines Vorfalls mit der Grösse der Unternehmen steigt.

Abbildung 2 Risiko von Vorfällen nach Grössenklassen



19 Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 199 zur Entwicklung erster geschäftskritischer Anwendungen* (Bern 2002), S. 19.

Es ist klar ersichtlich, dass die Kleinstunternehmen mit weniger als fünf Mitarbeitern insgesamt am wenigsten Vorfälle festgestellt haben. Die kleinen und mittleren Unternehmen (5-9, 10-49 und 50-249 Mitarbeiter) bilden eine recht homogene Gruppe. Sie haben zwar deutlich mehr Probleme mit Malware, stellen aber nicht signifikant mehr gezielte Angriffe fest als die Kleinstunternehmen. Gezielte Angriffe betreffen hauptsächlich Grossfirmen mit mehr als 250 Mitarbeitern. Von diesen haben 28% einen solchen Angriff festgestellt. Auch Malware betrifft Grossfirmen häufiger als kleine und mittlere Firmen.

Damit entsprechen die Ergebnisse ungefähr den Erwartungen. Der Unterschied zwischen Kleinstunternehmen und Grossfirmen ist sehr deutlich. Etwas überraschend ist vielleicht, dass es zwischen kleinen Unternehmen von 5-9 Mitarbeitern und mittleren Firmen bis zu 249 Mitarbeitern kaum Unterschiede gibt.

2.2.2 Das Risiko nach Geschäftstätigkeit

Um die Firmen nach ihrer Tätigkeit zu unterscheiden, wird gewöhnlich auf die Branchenzugehörigkeit[20] zurückgegriffen. Es wird angenommen, dass die Firmen der gleichen Branche ihre Geschäfte ähnlich abwickeln. Auch in dieser Studie sollen nun die unterschiedlichen Risiken der Branchen untersucht werden.

Wie die Unternehmensgrösse hat auch die Branchenzugehörigkeit einen Einfluss darauf, wie wichtig die Informatik- und Internettechnologien in einem Unternehmen sind.[21] Ebenso ist zu vermuten, dass nicht alle Branchen das gleiche Risiko eines gezielten Angriffes haben, weil gezielte Angriffe eher in Branchen erwartet werden, in denen hohe Umsätze erzielt werden, oder in Branchen, die über Vermögenswerte verfügen, die mit Hilfe von IKT gestützten Angriffen antastbar sind. Die Vermutung ist also, dass beispielsweise die Unternehmen der Finanzbranche und der Informatikbranche, welche die Informatik stark nutzen und hohe Umsätze generieren, häufiger Vorfälle feststellen als Firmen aus der Baubranche oder dem Gastgewerbe.

Die Auswertung der Umfrage bestätigt diese Vermutung aber nicht. Zwar registrieren Unternehmen aus der Informatikbranche besonders häufig Vorfälle, aber gleichzeitig verzeichnen die Finanzdienstleistungsunternehmen ähnlich wenige Vorfälle wie die Firmen aus dem Gastgewerbe.[22] Möglicherweise entsprechen die Ergebnisse deshalb nicht den Erwartungen, weil die einzelnen Brachen sich unterschiedlich gut schützen.[23]

Vermutlich ist aber die Unterscheidung nach Branchen auch nicht besonders gut geeignet, um von der Geschäftstätigkeit auf das Risiko eines Vorfalls zu schliessen. Innerhalb der Branchen können die Informatik- und Internettechnologien eine sehr unterschiedliche Rolle spielen. Ein geeignetes Kriterium der Geschäftstätigkeit, welches einen Einfluss auf das Risiko haben könnte, muss darum stärkeren Bezug zur Nutzung der Informatik- und Internettechnologien aufweisen. Ein solches Kriterium ist der Ein- und Verkauf über das Internet.

20 Es wird zwischen 12 Branchen unterschieden. Für Details zur Einteilung nach Branchen siehe Anhang 1.

21 Die Ergebnisse der Umfrage korrespondieren diesbezüglich mit den Resultaten der Studie der Task Force KMU. Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Bern, 2002), S. 20.

22 Wenn die Ergebnisse nach Grösse gewichtet werden, ergibt sich, dass 71% der Firmen aus der Finanzbranche und 73% der Unternehmen aus dem Gastgewerbe einen Vorfall festgestellt haben. Am höchsten ist der Anteil der Unternehmen, die einen Vorfall festgestellt haben, bei den unternehmensbezogenen Dienstleistungsbetrieben (86%), am tiefsten bei jenen aus der Handelsbranche (61%).

23 Auf das Thema Risikomanagement wird im nächsten Kapitel detaillierter eingegangen.

Das sogenannte E-Commerce ist für die Schweizer Unternehmen sehr wichtig geworden. 77% der befragten Firmen geben an, über das Internet Produkte oder Dienstleistungen einzukaufen.[24] Deutlich weniger, nämlich 19%, verkaufen über ihre Homepage Produkte oder Dienstleistungen.[25] Es ist nun anzunehmen, dass Firmen, welche E-Commerce betreiben, eher einen Vorfall feststellen, wobei vor allem eine Zunahme der gezielten Angriffe erwartet wird.

Abbildung 3 Risiko von Vorfällen nach Geschäftstätigkeit mittels E-Commerce

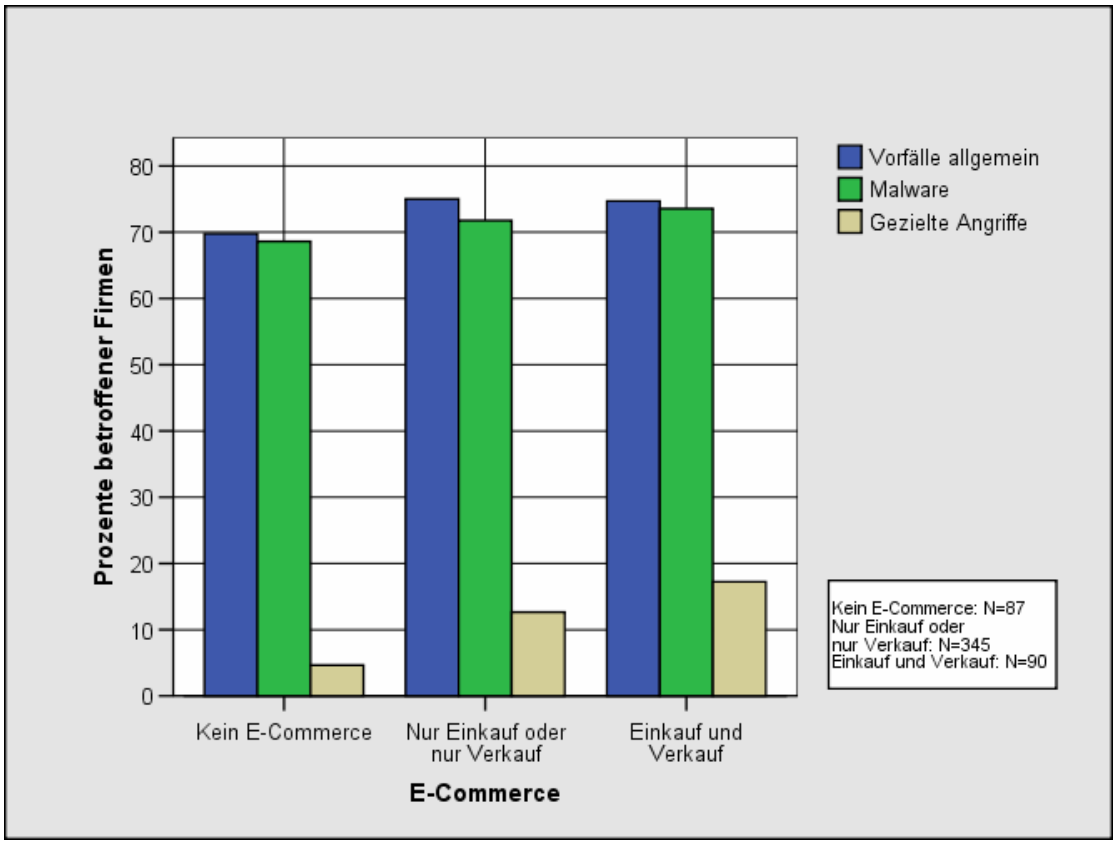


Abbildung 3 bestätigt diese Vermutung klar. Firmen, die E-Commerce betreiben, haben ein deutlich höheres Risiko eines gezielten Angriffes. 12% der Firmen, die mit Hilfe des Internets entweder verkaufen oder einkaufen, und gar 17% jener, die beides tun, haben einen gezielten Angriff festgestellt. Die Häufigkeit von allgemeiner, nicht gezielt eingesetzter Malware nimmt gleichzeitig nur schwach zu. Firmen ohne E-Commerce registrieren zwar fast gleich viele Vorfälle, diese sind aber nur selten gezielte Angriffe (nur 5% dieser Firmen haben einen Angriff festgestellt).

Die Vermutung, dass die gezielten Angriffe bei Firmen mit E-Commerce zunehmen, trifft also zu. Um das Risiko von allgemeiner Malware einzuschätzen, ist es hingegen nicht wichtig, ob eine Firma über das Internet Geschäfte abwickelt oder nicht. Da generische, nicht für einen

24 Nach statistischer Gewichtung (vgl. Anhang 3) sind es immer noch 73%. Diese sehr hohe Zahl entspricht früheren Studien zum E-Commerce. Der Netzreport 2 (2001) gab den Anteil der Unternehmen, welche über das Internet einkaufen, auf 60% an. Die Studie der Task Force KMU eruierte für die KMUs hingegen nur einen Anteil von 29%. Angaben aus: Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Bern, 2002), S. 32.

25 14% sind es, wenn durch das Gewichtungsverfahren (vgl. Anhang 3) der Anteil unter allen Schweizer Firmen geschätzt wird.

spezifischen, individualisierten Einsatz programmierte Viren, Würmer, Trojanische Pferde und Spyware per se viel breiter gestreut sind und daher ungezielt verwundbare Systeme befallen, ohne in erster Linie auf die kommerziellen Tätigkeiten der Firmen zu zielen, ist Malware genauso wahrscheinlich bei Firmen, die das Internet nicht für die Abwicklung ihrer Geschäfte benutzen.

2.2.3 Fazit und weitere mögliche Einflüsse auf das Risiko

Es zeigt sich, dass gewisse Unternehmen ein grösseres Risiko eines Vorfalls betreffend die Informationssicherheit haben als andere. Die Grösse der Unternehmen und die Nutzung des Internets, um Geschäfte abzuwickeln, spielen dabei eine wichtige Rolle.

Neben der Grösse der Unternehmen und ihrer Geschäftstätigkeit können auch andere Faktoren wie die Art der Verbindung zum Internet, der Grad der technischen Innovationen oder die Bekanntheit der Firma das Risiko eines Vorfalls beeinflussen. Es wären also noch weitere ausführliche Analysen notwendig, um die Gefährdung der Informationssicherheit für die einzelnen Firmen voraussagen zu können.

Ob dies überhaupt möglich ist, bleibt fraglich. Bei den Analysen der Risiken nach Art der Firma darf nämlich auch nicht vergessen werden, dass die Firmen nur die Vorfälle angeben konnten, welche sie auch entdeckt haben. Gerade bei gezielten Angriffen kommt es aber häufig vor, dass diese lange Zeit unentdeckt bleiben.

Zudem muss beachtet werden, dass die Firmen unterschiedlich auf die Bedrohungen der Informationssicherheit reagieren. Technische und organisatorische Schutzmassnahmen können die Wahrscheinlichkeit eines Vorfalls senken, indem sie die Bedrohungen frühzeitig abwehren, beziehungsweise indem sie die bestehenden Verwundbarkeiten reduzieren, so dass trotz identischer Bedrohungslage das Risiko sinkt. Gleichzeitig führen bessere Schutzmassnahmen in Unternehmen auch dazu, dass Vorfälle eher entdeckt werden. Deshalb wird im folgenden Kapitel das Risikomanagement der Unternehmen genauer betrachtet.

3 Risikomanagement

So vielfältig die Bedrohungen der Informationssicherheit sind, so breit ist auch das Feld möglicher Gegenmassnahmen. Das Risikomanagement besteht aus technischen Massnahmen, beinhaltet aber auch strategische und organisatorische Fragen. Um den Überblick nicht zu verlieren, werden verschiedene Teilaspekte des Risikomanagements in diesem Kapitel separat untersucht.

Zuerst werden die technischen und organisatorischen Massnahmen und ihre Verbreitung in den Unternehmen untersucht. Dann wird der Frage nachgegangen, welche finanziellen und personellen Ressourcen die Firmen für das Risikomanagement im Bereich der Informationssicherheit einsetzen. Gerade weil die Firmen üblicherweise möglichst wenig Mittel für die Informationssicherheit aufwenden wollen, ist es interessant zu untersuchen, ob zwischen den verschiedenen Firmen signifikante Unterschiede feststellbar sind. Schliesslich wird im letzten Abschnitt analysiert, wie häufig die Schweizer Unternehmen die Aufgaben der Informationssicherheit an externe Spezialisten delegieren und ob sie versuchen, die Risiken durch Versicherungen abzudecken.

3.1 Technische und organisatorische Schutzmassnahmen

Für das Risikomanagement der Unternehmen ist es entscheidend, dass sie die für sie am besten geeigneten Massnahmen ergreifen. In diesem Kapitel wird nun analysiert, welche der verschiedenen Möglichkeiten von welchen Firmen am häufigsten angewendet werden. Dabei wird zur Wahrung der Übersicht zwischen technischen und organisatorischen Massnahmen unterschieden.

3.1.1 Definition der technischen Massnahmen

Bevor die Verbreitung der Massnahmen diskutiert werden kann, müssen diese kurz definiert werden, wobei für genauere Beschreibungen wiederum auf Informationen im Internet und in der Literatur verwiesen wird.[26]

Antiviren-Programme
Antiviren-Programme gehören zur Grundausstattung der technischen Massnahmen zum Schutz der Informatiksicherheit. Diese Programme spüren Malware auf, welche sich auf dem Computer festgesetzt hat und blockieren oder beseitigen diese. Damit dies gelingt, müssen jedoch die Muster der Malware bekannt sein. Weil ständig neue Viren und Würmer auftauchen ist es nötig, die Antiviren-Programme laufend zu aktualisieren.

Firewall
Das Ziel von Firewalls ist der Schutz der Computersysteme vor unerwünschten Eindringlingen und vor den Bedrohungen durch Malware. Zu diesem Zweck überwachen die Firewalls die ein- und ausgehenden Verbindungen. Dabei werden unerwünschte Verbindungen abgewiesen. In Unternehmen werden die Firewalls üblicherweise an den Schnittstellen zwischen dem Internet

26 http://www.melani.admin.ch/gefahren-schutz/gefahren/index.html?lang=de. Ausführlich beschrieben werden die Massnahmen in: Bidgoli, Hossein et al. (eds.) *Handbook of Information Security Volume 3* (Hoboken, 2006).

und dem eigenen Netzwerk eingesetzt und gehören ebenfalls zum Standard der technischen Massnahmen.

Encryption (Verschlüsselung)
Wenn heikle Informationen auf Computernetzwerken gespeichert werden, besteht immer ein Risiko, dass Unbefugte an die Informationen gelangen können. Die gleiche Bedrohung besteht bei der Kommunikation vertraulicher Daten (z.B. über E-Mail). Deswegen werden Verschlüsselungs-Programme eingesetzt. Die Daten werden dabei nach einem bestimmten Verschlüsselungsverfahren (Algorithmus) in einen „Geheimtext" umgewandelt und können nur von jemandem wieder entschlüsselt werden, der über den entsprechenden Schlüssel verfügt. Dies bedeutet für die Anwender einen Mehraufwand, der sich lohnt, wenn die Geheimhaltung der Information von zentraler Bedeutung ist.

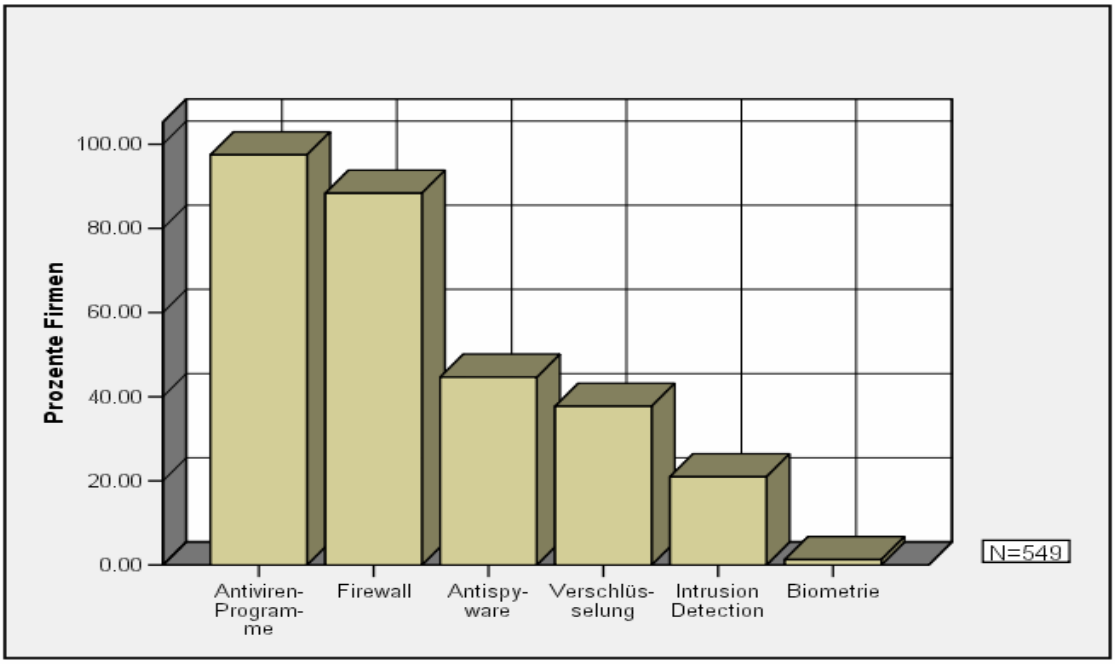
Intrusion Detection (Angriffserkennung)
Ein Intrusion Detection System (IDS) ist ein Programm, das die Aktivitäten auf einem Rechner oder auf Netzwerken überwacht, speichert und analysiert. Sobald Aktivitäten registriert werden, die einem typischen Angriffsmuster entsprechen, schlägt das System Alarm. Eine sinnvolle Anwendung von IDS setzt allerdings schon bedeutend mehr Kenntnisse voraus als dies bei Firewalls oder Antiviren-Programmen der Fall ist.

Biometrische Massnahmen
Diese Massnahmen können für die physische Zugangsbeschränkung zu Computern verwendet werden. Die Benutzer müssen sich beispielsweise durch Fingerabdruck, Gesichtserkennung oder Augenmerkmale authentifizieren. Die Verfahren sind meist relativ aufwändig.

3.1.2 Die Anwendung technischer Massnahmen

Abbildung 4 zeigt nun die Verbreitung der oben beschriebenen Massnahmen in den Schweizer Unternehmen.

Abbildung 4 Anwendung der technischen Schutzmassnahmen



Insgesamt schützen sich praktisch alle, nämlich 99.6% der Teilnehmer mit mindestens einer der möglichen technischen Massnahmen. Antiviren-Programme und Firewalls benutzen weit über 80% der Unternehmen.

Während also die meisten Firmen die elementaren technischen Sicherheitsmassnahmen ergriffen haben, werden aufwändigere Technologien wie Intrusion Detection und Biometrie viel seltener angewendet. Dieses Resultat überrascht wenig und entspricht auch ungefähr den Ergebnissen, welche die Erhebung des CSIs und des FBIs für die US-Firmen ergab.[27] Aus Kostengründen ist es nachvollziehbar, dass die Unternehmen solche technisch und auch finanziell anspruchsvolleren Massnahmen seltener einsetzen. Für einige Firmen sind diese auch nicht sinnvoll. Darum lohnt es sich genauer zu betrachten, bei welchen Firmen die aufwändigeren Massnahmen angewendet werden.

Es zeigt sich, dass vor allem Grossfirmen solche Massnahmen ergreifen. Verschlüsselungstechniken setzen beispielsweise 60% der Grossfirmen ein, während diese Technik nur 25% der Mikrounternehmen benutzen. Im Vergleich der verschiedenen Branchen wird deutlich, dass die aufwändigen technischen Massnahmen bei den Unternehmen aus der Informatik- und der Finanzbranche am stärksten verbreitet sind.[28] Diese Ergebnisse waren zu erwarten, da die grösseren Firmen und speziell jene aus der Finanzbranche stark auf eine sichere Informatikinfrastruktur angewiesen sind. Weil in der Informatikbranche viel Know-how vorhanden ist, überrascht es ebenfalls wenig, dass dort die Umsetzung von aufwändigen technischen Massnahmen stärker verbreitet ist.

3.1.3 Definition der organisatorischen Massnahmen

Neben den technischen Massnahmen können die Firmen ihre Informationssicherheit auch über die Anwendung von verschiedenen organisatorischen Massnahmen erhöhen. In der Umfrage wurden sie zu den wichtigsten derartigen Massnahmen befragt. Diese sollen hier kurz beschrieben werden.

Security Policy
Die Security Policy eines Unternehmens bildet das Grundkonzept der Informationssicherheit. Es werden Ziele gemäss dem Sicherheitsanspruch der Firma festgelegt, die Verantwortlichkeiten bestimmt und die zur Verfügung stehenden Mittel definiert. Klarheit in diesen Fragen bildet die Voraussetzung dafür, dass die verschiedenen Einheiten eines Unternehmens im Bereich der Informationssicherheit reibungslos zusammenarbeiten.

Vorfallsmanagement (Incident Response)
Beim Vorfallsmanagement geht es darum, sich auf einen möglichen Angriff auf die Informationssicherheit vorzubereiten. Dabei sollten sowohl technische als auch organisatorische und rechtliche Massnahmen berücksichtigt werden. Das Ziel eines solchen Managements ist, dass die Informatik nach einem Vorfall möglichst schnell wieder einsatzbereit ist.

27 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), S. 5.

28 63% der Firmen aus der Finanzbranche setzten Verschlüsselungstechnologien ein, 42% Intrusion Detection und 5% biometrische Massnahmen. Bei den Unternehmen aus der Informatikbranche benutzen 57% Verschlüsselungstechnologien, 41% Intrusion Detection und 5% biometrische Massnahmen. Damit sind diese Unternehmen klar führend in der Anwendung der aufwändigen Technologien.

Datensicherungs-Managemet (Backup)
Die Datensicherung dient zum Schutz von Datenverlusten aller Art. Dazu wird eine Kopie der Daten (Backup) erstellt und an einem sicheren Ort aufbewahrt. Bei der Ausarbeitung eines Datensicherungs-Management gilt es vor allem die Fragen zu klären, wie oft die Sicherung durchzuführen ist, wer dafür verantwortlich sein soll, welche Daten gespeichert werden (alle, nur die wichtigsten, nur die neuesten) und wie die Backup-Daten verwaltet werden.

Aktualisierung und Schliessen von Sicherheitslücken (Updates / Vulnerability Scan)
Die grosse Komplexität der Betriebssysteme und der möglichen Anwendungen hat zur Folge, dass immer wieder neue Sicherheitslücken entdeckt werden, die dann von Hackern oder Malware ausgenutzt werden. Deshalb ist es von entscheidender Bedeutung, dass Sicherheitslücken frühzeitig entdeckt und mittels so genannter Patches geschlossen werden. Entscheidend ist es, die Verantwortung für das Update-Management klar zu verteilen, so dass diese auch regelmässig durchgeführt werden.

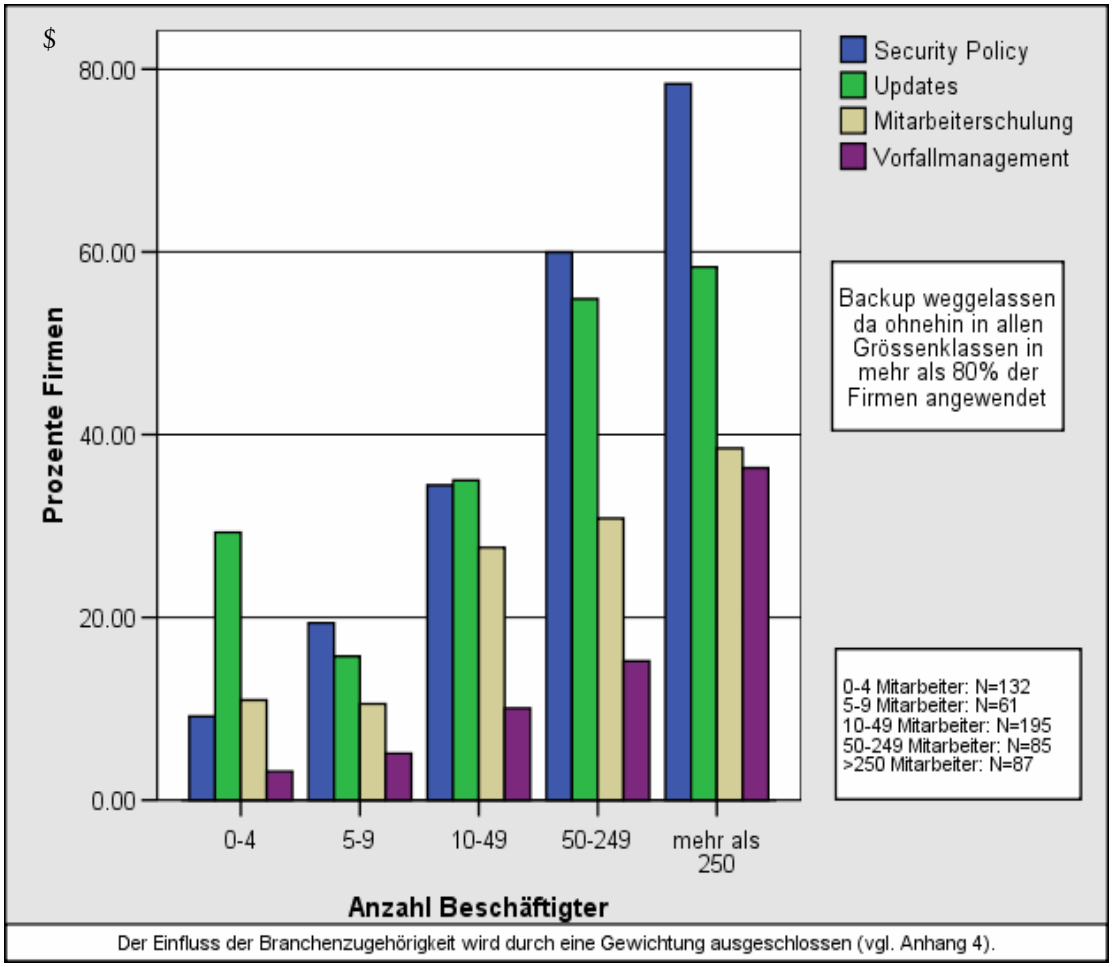
Mitarbeiterschulung
Eine regelmässige Weiterbildung der Mitarbeiter im Bereich der Informationssicherheit kann das Risiko von Vorfällen minimieren, indem Fehlverhalten korrigiert wird. Die Schulung kann durch externe oder interne Fachkräfte geschehen, kann sich aber auch auf regelmässige Informations-kampagnen beschränken.

3.1.4 Die Anwendung organisatorischer Massnahmen

Die Untersuchung zur Verbreitung der verschiedenen organisatorischen Massnahmen in den Schweizer Unternehmen zeigt, dass die Datensicherung das wichtigste Anliegen der Firmen ist. Fast alle, nämlich 91%, wenden ein Backup-Konzept an. Die übrigen Konzepte werden weniger häufig angewendet. Je 39% haben eine Security Policy respektive ein Update Management, 26% schulen ihre Mitarbeiter, und 13% haben ein Vorfallsmanagement.

Wieder soll überprüft werden, ob die organisatorischen Massnahmen von den verschiedenen Unternehmen unterschiedlich oft angewendet werden. In Abbildung 5 ist der Einfluss der Grösse der Firmen gut ersichtlich.

Abbildung 5 Anwendung der organisatorischen Massnahmen nach Grössenklassen



Es ist deutlich erkennbar, dass organisatorische Massnahmen bei grösseren Firmen sehr viel häufiger angewendet werden als bei kleineren und mittleren Unternehmen. In grösseren Firmen ist es auch wichtiger, die Verantwortlichkeiten klar zu regeln und klare Handlungsanweisungen für alle Mitarbeiter zu erstellen. Besonders das Vorfallmanagement steigt mit der Grösse der Unternehmen stark an. 36% der Grossfirmen haben ein solches Management. Dies zeigt, dass es im Vergleich zu den kleinen Firmen für die grossen Unternehmen viel wichtiger ist, dass die Informatik nach einem Vorfall möglichst rasch wieder einsetzbar ist. Dennoch verzichten relativ viele, nämlich 64% der antwortenden Grossfirmen, auf ein Vorfallsmanagement.

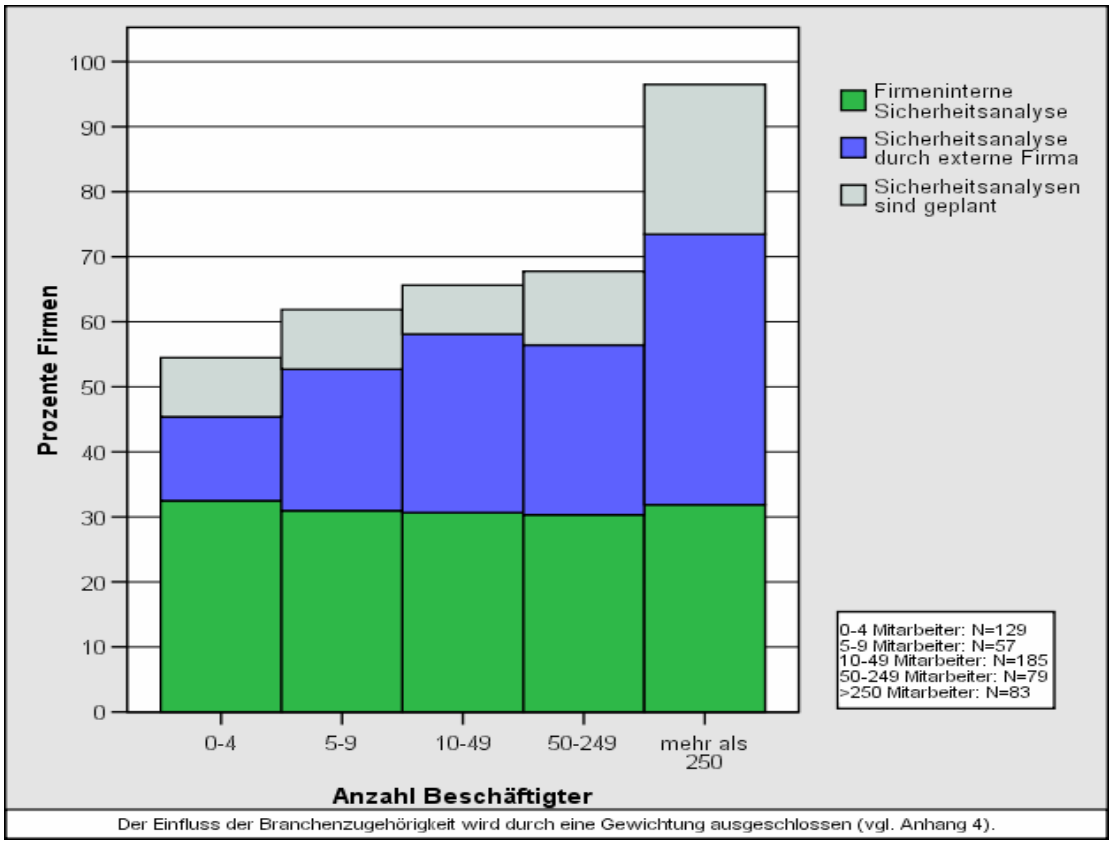
3.1.5 Die Überprüfung der getroffenen Massnahmen

Ein wichtiges Sicherheitskonzept, das hier separat untersucht werden soll, ist die ständige Überprüfung der getroffenen Massnahmen. Nur wer alle Massnahmen zur Bewahrung der Informationssicherheit regelmässig analysiert, stellt früh genug Schwachstellen fest und kann reagieren, bevor diese Schwachstellen zu Problemen führen. Von den befragten Unternehmen führen 56% solche Analysen regelmässig durch (32% firmenintern, 24% lassen ihre Sicherheit durch eine externe Firma prüfen). Weitere 11% der Befragten haben solche Sicherheitsanalysen

für die Zukunft geplant.[29] Ein Drittel der Firmen führt keine regelmässige Überprüfung durch und plant dies auch nicht.

Bei einer detaillierteren Betrachtung zeigt sich wiederum, dass es vor allem die Grossfirmen sind, welche konsequent ihre Sicherheit überprüfen. Wie in der Abbildung 6 dargestellt wird, führen 72% der Grossfirmen bereits Sicherheitsanalysen durch und weitere 13% davon geben an, solche zu planen.

Abbildung 6 Verbreitung der Sicherheitsanalysen nach Unternehmensgrösse



Der hohe Anteil an Grossfirmen, die Sicherheitsanalysen durchführen, hebt sich deutlich vom eher bescheidenen Anteil bei den mittleren Firmen ab. Erst die Grossfirmen haben offenbar die Wichtigkeit der ständigen Überprüfung der Sicherheitsmassnahmen erkannt oder verfügen über die dafür notwendigen Ressourcen.

Zum Vergleich dieser Werte kann auf die „Hi-Tech Crime"-Studie verwiesen werden. Diese Umfrage unter Britischen Firmen mit mehr als 100 Mitarbeitern hat ergeben, dass 33% keine Sicherheitsanalysen durchführen.[30] Die Grossfirmen verhalten sich also in der Schweiz bezüglich der Durchführung von Sicherheitsanalysen ähnlich wie in Grossbritannien (28% der Schweizer Grossfirmen analysieren ihre Sicherheit noch nicht).

29 Die Gewichtung dieser Resultate nach Grösse und Branche (vgl. Anhang 3) ergibt, dass der Anteil aller Schweizer Firmen, die eine Sicherheitsanalyse durchführen, auf 47% geschätzt werden kann. Weitere 8% planen eine Sicherheitsanalyse für die Zukunft.

30 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005), S. 29.

3.2 Der Aufwand der Unternehmen für die Informationssicherheit

Die beschriebenen Massnahmen sind teilweise mit beträchtlichen Kosten verbunden. Weil sich die Bedrohungen laufend verändern, müssen die Unternehmen die technischen und organisatorischen Massnahmen ständig neu anpassen. Zudem muss Personal zur Verfügung gestellt und geschult werden. Natürlich versuchen die Firmen, die Kosten für die Informationssicherheit möglichst gering zu halten. Deshalb ist der finanzielle Aufwand, den sie dafür betreiben, ein guter Indikator, um zu überprüfen, wie wichtig ihnen die Informationssicherheit ist. Das gleiche gilt auch für den personellen Aufwand, allerdings ist dabei nicht nur die Anzahl der Mitarbeiter zu berücksichtigen, sondern auch der Ausbildungsstand der Verantwortlichen für die Informationssicherheit.

3.2.1 Der finanzielle Aufwand für die Informationssicherheit

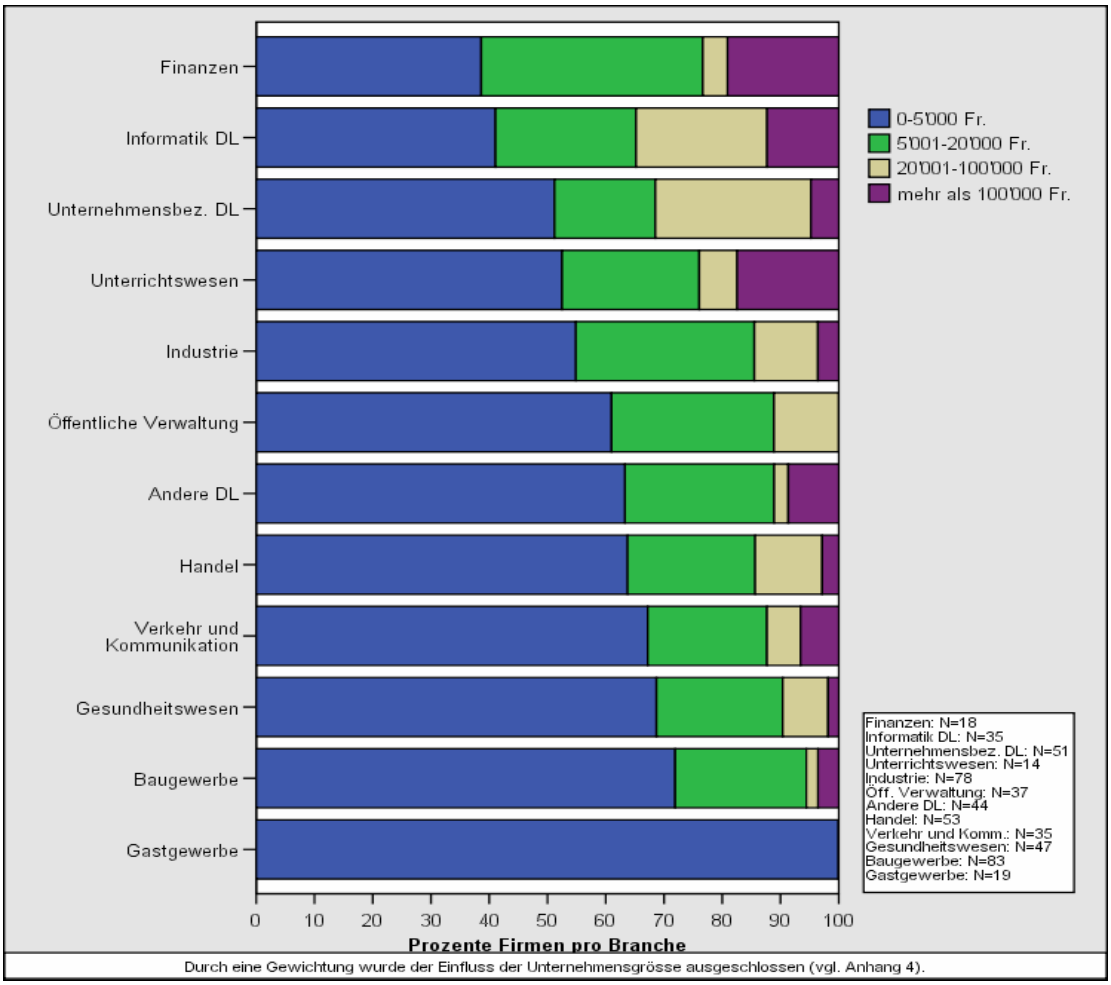
Weil es für die wenigsten Unternehmen möglich sein dürfte, die Kosten für die Informationssicherheit präzise zu beziffern, wurden diese in der Umfrage mit Hilfe von vier Kategorien (0-5'000 Fr.; 5'001-20'000 Fr.; 20'001-100'000 Fr.; mehr als 100'000 Fr.) erhoben. Die Auswertung ergibt, dass viele Unternehmen nur beschränkte finanzielle Mittel für die Gewährleistung der Informationssicherheit zur Verfügung haben. 62% der Firmen, welche sich zu ihren Ausgaben für die Informationssicherheit äusserten, gaben an, nicht mehr als 5'000 Fr. zu diesem Zweck aufzuwenden. Nur 5% geben mehr als 100'000 Fr. aus. Eine detailliertere Analyse soll nun zeigen, welche Firmen wie viel in das Risikomanagement investieren.

Wenig überraschend ist der starke Zusammenhang zwischen der Grösse eines Unternehmens und dem finanziellen Aufwand für die Informationssicherheit. Je grösser eine Firma ist, desto mehr investiert sie in das Risikomanagement.[31] Aufgrund ihrer grösseren Budgets stehen den grösseren Unternehmen mehr Mittel im Bereich der Informationssicherheit zur Verfügung. Ihr grösserer Aufwand ist aber sicher berechtigt, schliesslich wurde ja im vorhergehenden Kapitel festgestellt, dass die Grossfirmen bedeutend mehr Vorfälle zu bekämpfen haben, als die kleinen und mittleren Firmen.

Neben der Grösse der Unternehmen kann aber auch ihre Tätigkeit einen Einfluss auf das finanzielle Engagement für die Informationssicherheit haben. Bei der Untersuchung der Vorfallshäufigkeit nach Branchen wurde bereits die Vermutung geäussert, dass die Unternehmen aus der Finanzbranche nur deshalb gleich wenig Vorfälle registrieren wie Firmen aus dem Gastgewerbe, weil sie sich besser vor den Bedrohungen der Informationssicherheit schützen. Für Unternehmen aus der Finanzbrache ist die Sicherheit der Daten normalerweise von viel zentralerer Bedeutung als für Firmen aus dem Gastgewerbe. Abbildung 7 zeigt auf, wie viel Aufwand die Unternehmen der verschiedenen Branchen für die Informationssicherheit betreiben.

31 Die Stärke des Zusammenhanges zwischen der Grösse der Unternehmen und dem Aufwand für die Prävention kann mit dem Korrelationskoeffizient Gamma ausgedrückt werden. Gamma kann für positive Korrelationen (je grösser desto mehr) Werte zwischen 0 und 1 erreichen. Für den untersuchten Zusammenhang errechnet sich der hohe Wert von 0.791.

Abbildung 7 Finanzieller Aufwand für die Informatiksicherheit nach Branchen



Tatsächlich bestehen zwischen den Branchen beträchtliche Unterschiede. Die Unternehmen der oben erwähnten Branchen bilden dabei die Extreme: Im Gastgewerbe gibt keine Firma mehr als 5'000 Fr. für die Informationssicherheit aus, während 19% der Firmen aus der Finanzbranche mehr als 100'000 Fr. investieren. Allgemein lässt sich sagen, dass die Firmen jener Branchen, in welchen die Informatik als wenig wichtig erachtet wird, konsequenterweise auch weniger in die Informationssicherheit investieren.

3.2.2 Der Personalaufwand für die Informationssicherheit

In der Umfrage wurden den Unternehmen zwei Fragen zu ihrem Personal für die Informationssicherheit gestellt. Zunächst war der Personalaufwand in diesem Bereich nach Anzahl der Vollzeitstellen anzugeben,[32] dann wurde der Ausbildungsstand des Leiters des Teams erfragt, welches für die Informationssicherheit verantwortlich ist.

Die Antworten auf die Frage nach der Grösse des für die Informationssicherheit verantwortlichen Teams weisen darauf hin, dass in den meisten Unternehmen nur wenig Personal zu diesem Zweck angestellt ist. In 13% der Firmen, welche zu dieser Frage Angaben machten, kümmert sich keiner der Angestellten direkt um die Informationssicherheit. Weitere 60% geben an, dass sie dafür höchstens 100 Stellenprozente zur Verfügung haben. Knapp ein

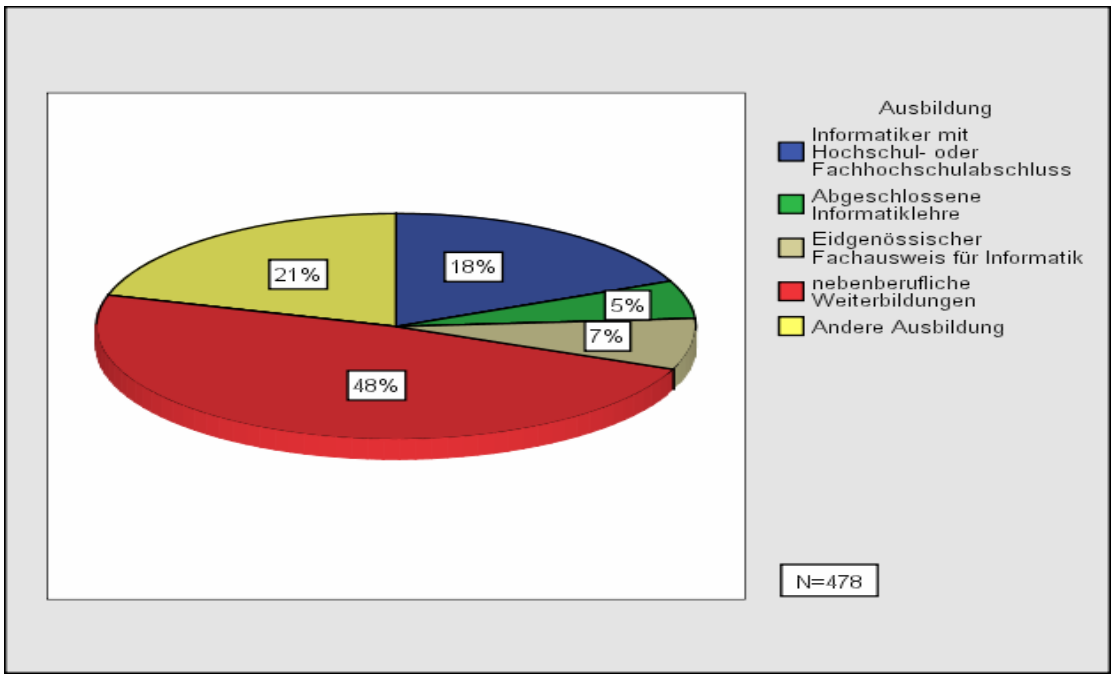
32 Wiederum wurden zur Vereinfachung Kategorien vorgegeben: keine Stelle; 0-1; 2-5; 6-10; mehr als 10 Stellen.

Viertel der Firmen (24%) beschäftigt kleine Teams von 2-5 Mitarbeitern, und nur sehr wenige (3%) stellen in diesem Bereich mehr als fünf Personen ein.[33] Die Informationssicherheit wird also in der Personalpolitik der Unternehmen nur selten als eigenständiger Aufgabenbereich definiert. Häufig dürften dafür die fehlenden finanziellen Mittel verantwortlich sein, teilweise ziehen die Firmen aber auch flexiblere Lösungen (externe Beratung, Outsourcing) einem festangestellten Team vor.

Parallel zu den aufgewendeten Mitteln steigt auch der Personalaufwand mit der Grösse der Unternehmen an.[34] Auch dies lässt sich darauf zurückführen, dass grössere Firmen über mehr personelle und finanzielle Ressourcen verfügen. Es ist aber nicht so, dass mehr finanzielle Mittel automatisch zu einem grösseren Personalaufwand führen. Die Untersuchung des Personalaufwandes nach Branchenzugehörigkeit zeigt nämlich, dass die Unternehmen der Finanzbranche zwar viel Geld in die Informationssicherheit investieren, aber gleichzeitig eher wenig Personal für diese Aufgabe anstellen.[35] Offensichtlich werden in einigen Branchen Outsourcing-Lösungen bevorzugt. Dies soll später genauer analysiert werden.

Zunächst gilt es noch, den Ausbildungsstand der Verantwortlichen für die Informationssicherheit zu untersuchen. Für einen wirksamen Schutz kann dies ebenso entscheidend sein wie die Grösse des Teams. Spezialisten sind aber teuer und weniger flexibel einsetzbar. Deshalb kann sich nicht jede Firma Spezialisten leisten.

Abbildung 8 Ausbildung der Verantwortlichen für die Informatiksicherheit



33 Bei einer Schätzung für alle Unternehmen in der Schweiz muss wieder berücksichtigt werden, dass Grossfirmen und einzelne Branchen unter den Teilnehmern der Umfrage überproportional vertreten sind. Wenn das Gewichtungsverfahren (vgl. Anhang 3) angewendet wird, ergeben sich folgende Schätzungen: In 22% der Unternehmen der Schweiz kümmert sich kein Angestellter um die Informatiksicherheit und in 68% höchstens ein Vollzeitangestellter.

34 Die Stärke des Zusammenhangs lässt sich wiederum mit dem Korrelationskoeffizienten Gamma ausdrücken (vgl. Fussnote 31). Gamma erreicht einen Wert von 0.588.

35 Wie in Abbildung 7 gezeigt, wenden die Unternehmen der Finanzbranche am meisten Geld für das Risikomanagement auf. Aber nicht einmal die Hälfte dieser Unternehmen hat mehr als zwei Personen angestellt, die sich um die Informationssicherheit kümmern.

Abbildung 8 verdeutlicht, dass in weniger als jeder dritten Firma ein ausgebildeter Informatiker für die Informationssicherheit verantwortlich ist. Bei detaillierterer Betrachtung wird klar, dass dieser Anteil in Wirklichkeit sogar noch tiefer liegen dürfte. In Grossfirmen und in Firmen aus der Informatikbranche sind nämlich viel häufiger ausgebildete Informatiker angestellt. Wenn berücksichtigt wird, dass es unter den teilnehmenden Firmen überproportional viele Grossunternehmen gibt, muss der Anteil von Informatikern, die in den Schweizer Unternehmen für die Informatiksicherheit verantwortlich sind, auf nur 15% geschätzt werden.[36]

Dieser geringe Anteil an formal qualifizierten Fachkräften kann dann zum Problem werden, wenn die Bedrohungen immer komplexer werden. Die Schweiz ist in dieser Hinsicht aber kein Sonderfall, auch die britische „Hi-Tech Crime"-Studie ergab, dass es in Bezug auf die Informationssicherheit an Arbeitskräften mit formalen Qualifikationen mangelt.[37]

Zusammenfassend lässt sich also über den Personalaufwand der Unternehmen im Bereich der Informationssicherheit sagen, dass die meisten Firmen für diese Aufgabe wenig Angestellte beschäftigen, und nur in einer Minderheit der Firmen die Hauptverantwortung dafür bei einem ausgebildeten Informatiker liegt.

3.3 Auslagerung des Risikos

Wie gezeigt wurde, gibt es Firmen, die zwar relativ grosse finanzielle Mittel in die Informationssicherheit investieren, gleichzeitig aber dafür nur wenig eigenes Personal anstellen. Offensichtlich beschäftigen diese Unternehmen dafür mehr externe Spezialisten, wodurch die Bedürfnisse im Bereich der Informationssicherheit flexibel abgedeckt werden können. Aber das Outsourcing hat nicht nur Vorteile. Weil der Schutz der Informatik in vielerlei Hinsicht eher ein Managementproblem als eine Frage von technischen Massnahmen ist, bleibt häufig ein wichtiger Teil der Aufgaben im Bereich der Informationssicherheit bei der Firma selbst. Zudem sind die Spezialisten von Outsourcing-Partnern meist relativ teuer.

Jede Firma muss deshalb abwägen, ob die Zusammenarbeit mit Outsourcing-Partnern oder eigene Sicherheitsteams für die Gewährleistung der Informationssicherheit die bessere Lösung sind. Weil für viele Unternehmen Outsourcing eine wichtige Ergänzung der eigenen Massnahmen darstellt, soll dessen Verbreitung im Folgenden untersucht werden. In einem zweiten Abschnitt wird dann thematisiert, ob die Unternehmen sich gegen allfällige Schäden eines Vorfalls versichern. Mit einer Versicherung kann das Risiko nämlich ebenfalls ausgelagert werden, da die möglichen finanziellen Schäden vom Versicherer getragen werden müssten.

3.3.1 Die Verbreitung der Zusammenarbeit mit Outsourcing-Partnern

Um zu erheben, wie wichtig Outsourcing im Bereich der Informationssicherheit in der Schweiz ist, wurden die Teilnehmer der Umfrage gefragt, wie viele Prozent der für die Informationssicherheit aufgewendeten Mittel für die Bezahlung der Outsourcing-Partner gebraucht werden.

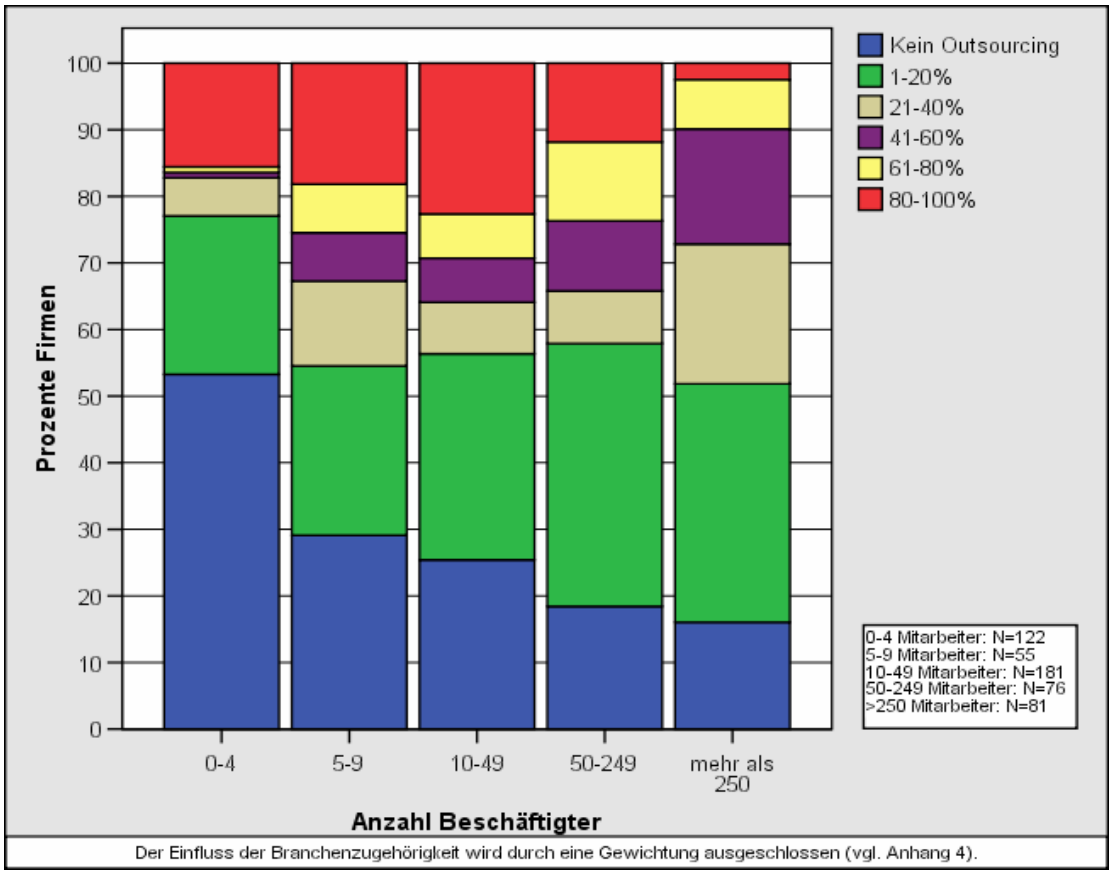
Von den befragten Firmen gaben 30% an, gar kein Outsourcing zu betreiben. Weitere 31% lagern höchstens 20% ihres Aufwandes für die Informationssicherheit aus. Mehr als die Hälfte der Firmen delegiert also nur einen kleinen Teil ihrer Informationssicherheit an Spezialisten, zugleich wenden aber auch 15% der Unternehmen mehr als 80% ihrer Mittel in diesem Bereich

36 Die Schätzung ergibt sich, wenn das Gewichtungsverfahren (vgl. Anhang 3) angewendet wird.

37 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005), S. 30.

für die Bezahlung von Outsourcing-Partnern auf. Die Unterschiede zwischen den Firmen sind sehr gross. Umso interessanter ist es zu untersuchen, welche Unternehmen Outsourcing Lösungen favorisieren. In Abbildung 9 ist die Verbreitung von Outsourcing nach Grössenklassen dargestellt.

Abbildung 9 Outsourcing nach Unternehmensgrösse



Die Mikrounternehmen mit weniger als fünf Mitarbeitern betreiben selten Outsourcing im grösseren Stil. Mehr als die Hälfte dieser Firmen kümmert sich ausschliesslich selbst um die Informationssicherheit. Vermutlich ist Outsourcing für diese Kleinstfirmen zu teuer. Ganz anders verhalten sich die kleinen und mittleren Firmen, welche einen hohen Anteil ihrer Informationssicherheit auslagern. Mehr als jede fünfte Firma mit 10-49 Mitarbeitern lagert mindestens 80% ihres Aufwandes für die Sicherheit ihrer Informatik aus. Diese mittleren Firmen sind teilweise stark auf die Informatik angewiesen, haben aber wenig eigene Möglichkeiten, deren Sicherheit zu gewährleisten. Die Grossfirmen hingegen arbeiten zwar häufig mit Outsourcing-Partnern zusammen, delegieren aber nur sehr selten mehr als 60% ihrer Informationssicherheit (nur 10% der Grossfirmen tun dies).

Der Blick auf die Verbreitung des Outsourcing nach Branchenzugehörigkeit bestätigt nun, dass die Unternehmen der Finanzbranche, welche zwar viel für die Informationssicherheit ausgeben, aber nur wenig Personal für diese Aufgabe beschäftigen, überdurchschnittlich viel Outsourcing betreiben. Nachvollziehbar ist, dass die Unternehmen aus der Informatikbranche

nur selten Outsourcing im Bereich der Informationssicherheit anstreben, da sie selbst genügend Know-how haben.[38]

Es liegen keine vergleichbaren internationalen Studien vor, die Rückschlüsse darauf ermöglichen würden, ob die Schweizer Unternehmen viel oder wenig Outsourcing betreiben. Im Vergleich mit der jährlichen „Computer Crime and Security Survey 2005" des FBI und des CSI ergibt sich zwar für die Schweiz ein deutlich höherer Anteil an Outsourcing. Aufgrund der speziellen Zusammensetzung der Teilnehmer der Befragung des FBI können die Ergebnisse aber nicht direkt verglichen werden.[39]

3.3.2 Die Abdeckung durch Versicherungen

Einen Spezialfall des Outsourcing bilden die Versicherungen. Dabei werden die allfälligen Kosten der Schäden durch Angriffe auf die Informationssicherheit ausgelagert. In der Schweiz werden seit dem Jahr 2000 Versicherungen zur Abdeckung von Internet-Risiken angeboten.[40] Die Ergebnisse der Umfrage zeigen, dass diese sich sehr schnell etabliert haben: 45% der Firmen, welche die Frage beantwortet haben, geben an, eine Versicherung gegen mögliche Schäden an der Informatikinfrastruktur zu besitzen. Aufgrund dieser Angaben lässt sich schätzen, dass ungefähr ein Drittel aller Firmen in der Schweiz eine solche Versicherung abgeschlossen hat.[41]

Am stärksten verbreitet sind Versicherungen bei den mittleren Unternehmen mit 50-249 Mitarbeitern, von denen 69% eine Versicherung zur Abdeckung dieser Risiken abgeschlossen haben. Bei den Mikrounternehmen ist der Anteil viel tiefer (29%), und auch die Grossunternehmen sind deutlich weniger oft versichert (54%). Am häufigsten versichern sich die öffentlichen Verwaltungen, gefolgt von den Firmen der Finanzbranche und den unternehmensbezogenen Dienstleistungsunternehmen.

Für die Firmen, welche sich nicht versichern, sind vor allem ökonomische Überlegungen ausschlaggebend. Mehr als die Hälfte (55%) gab an, dass sich eine Versicherung für sie nicht lohnen würde. Immerhin 29% haben schlicht nicht gewusst, dass solche Versicherungen angeboten werden. 15% gaben an, dass sie für Versicherungen keine Mittel zur Verfügung hätten, und weitere 8% (vor allem Grossfirmen) beurteilen die Angebote der Versicherungen als ungenügend.[42]

Auch bezüglich der Abdeckung des Risikos durch Versicherungen fehlen internationale Vergleichsdaten. Es kann aber auch ohne Vergleichsmöglichkeit festgestellt werden, dass die Abdeckung überraschend hoch ist. Obwohl erst seit wenigen Jahren Angebote in diesem Bereich bestehen, haben schon zahlreiche Firmen eine Versicherung abgeschlossen.

38 Nur 9% der Firmen aus der Informatikbranche wenden mehr als 40% ihrer Kosten im Bereich der Informationssicherheit für Outsourcing auf.

39 Computer Security Institute(CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), S. 9. Die Teilnehmer dieser FBI/CSI-Studie sind Mitglieder des Computer Security Institute (CSI). Deshalb kann davon ausgegangen werden, dass diese überdurchschnittlich viele eigene Anstrengungen im Bereich der Informationssicherheit unternehmen. Zudem sind in dieser Studie vor allem Grossfirmen befragt worden.

40 Haldemann, Lukas, V*ersicherung von Internet-Risiken* (Seminararbeit am Departement für Informatik der ETH Zürich, 2001), S. 5.

41 Diese Schätzung ergibt sich wiederum durch die Gewichtung der Daten aus der Umfrage nach Unternehmensgrösse und Branchenzugehörigkeit (vgl. Anhang 3).

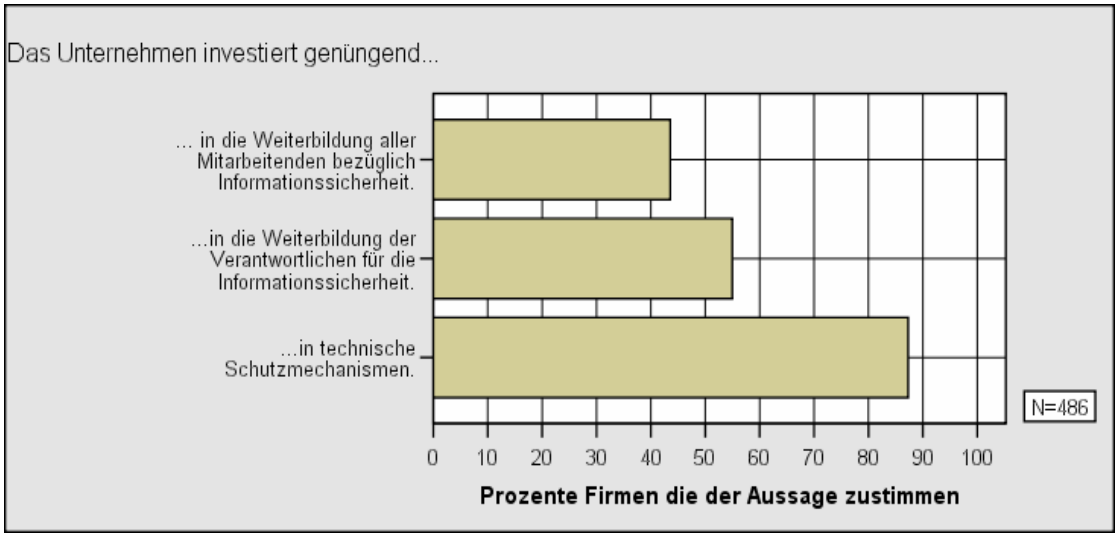
42 Es konnten mehrere Antworten gewählt werden.

3.4 Fazit zum Risikomanagement der Unternehmen

Das Risikomanagement kann sehr verschieden gestaltet werden. Die elementarsten Sicherheitsmassnahmen (Antiviren-Programme, Firewalls, Backups) wenden fast alle Firmen an. Einigen Unternehmen, vor allem den kleineren, genügen diese Vorkehrungen, andere haben ein grösseres Sicherheitsbedürfnis und decken dieses entweder selbst mit zusätzlichen technischen und organisatorischen Massnahmen ab, oder suchen sich Outsourcing-Partner. Da es viele Arten gibt, wie ein Risikomanagement implementiert werden kann und dies teils äusserst firmenspezifisch gestaltet wird, kann dessen Qualität nicht für die Gesamtheit der Unternehmen beurteilt werden. Es ist auch unmöglich, einen direkten Effekt der getroffenen Massnahmen auf die Vorfallswahrscheinlichkeit festzustellen. Dies lässt sich damit begründen, dass die Unternehmen, die mehr Massnahmen ergriffen haben, meist auch ein grösseres Risiko eines Vorfalls haben. Dazu kommt, dass Vorfälle teilweise nur dank der Schutzmassnahmen überhaupt entdeckt werden.

Die Unternehmen selbst scheinen zufrieden mit ihren Massnahmen. 87% sind mit der Aussage einverstanden, dass ihr Unternehmen genügend in die technischen Sicherheitsmassnahmen investiert. Wie Abbildung 10 zeigt, ist aber die Zufriedenheit mit der Ausbildung längst nicht gleich gross: Nur eine knappe Mehrheit ist zufrieden mit dem Engagement der Firmen bei der Ausbildung der Verantwortlichen für die Informationssicherheit, und gar eine Minderheit ist der Ansicht, dass in die Weiterbildung der allgemeinen Mitarbeiter genügend investiert wird.

Abbildung 10 Beurteilung der eigenen Investitionen in die Informationssicherheit



Natürlich sagt auch die Zufriedenheit der Firmen mit ihren eigenen Investitionen nur wenig über die tatsächliche Qualität des Risikomanagements aus. Es wird aber ersichtlich, dass viele Firmen erkannt haben, dass die Informationssicherheit nicht nur ein technisches Problem ist, sondern dass auch in die Ausbildung investiert werden muss.[43]

43 Die Ergebnisse entsprechen einer Umfrage der KPMG über die Zufriedenheit von ausgewählten CIOs (Chief Information Officers) mit der Informatiksicherheit in ihrem Unternehmen. Auch diese Umfrage ergab eine hohe Zufriedenheit für die technischen Massnahmen und eine tiefe Zufriedenheit beim Sicherheitsbewusstsein der End-Benutzer. KPMG, *IT-Management 2005* (Zürich und Genf, 2005), S. 26.

Auch wenn es also nicht möglich ist, die Qualität des Risikomanagements abschliessend zu beurteilen, so gilt es zum Schluss dieses Kapitels doch nochmals einige wichtige Punkte festzuhalten:
Die Schweizer Unternehmen lagern relativ häufig Teile ihrer Informationssicherheit aus (vor allem die mittleren Firmen). Ein Grund dafür ist, dass für die Informationssicherheit meist nur wenige Stellenprozente zur Verfügung stehen und die Mitarbeiter häufig keine ausgebildeten Informatiker sind. Besonders mittlere Firmen können sich bei weitem nicht alle nötigen Massnahmen leisten. Aufgrund der knappen Ressourcen und der Annahme, dass viele Verantwortliche auf Weiterbildungen angewiesen sind, ist es nun von Bedeutung, ob die Firmen an Kooperationen im Bereich der Informationssicherheit interessiert sind.

4 Externe Hilfe und Kooperation

In den bisherigen Kapiteln wurde deutlich, dass die Informationssicherheit für viele Unternehmen ein wichtiges Thema ist. Die meisten Firmen stellen immer wieder Vorfälle fest, welche die Sicherheit ihrer Informatik beeinträchtigen. Bei der Bewältigung dieser Vorfälle sind Unternehmen häufig auf externe Hilfe angewiesen. Zunächst soll deshalb geprüft werden, wie oft Firmen bei solchen Vorfällen externe Hilfe suchen und wo sie diese finden.

Nicht nur bei den Vorfällen selbst, sondern auch beim Risikomanagement stossen die Firmen oft an ihre Kapazitätsgrenzen. Ein effektiver und effizienter Schutz der Informatik ist teuer und muss ständig neu angepasst werden. Weil viele Firmen mit ähnlichen Problemen kämpfen, stellt sich die Frage, ob ein gegenseitiger Austausch nicht sinnvoll wäre. Darum wird auch die Frage untersucht, welche Firmen zu einer Zusammenarbeit bereit wären, wer diese koordinieren könnte und wie sie finanziert werden sollte. In diesem Zusammenhang wird dann auch die Rolle des Staates genauer betrachtet. Dabei steht die Frage im Vordergrund, welche Beiträge der Staat leisten könnte, um die Firmen in diesem Bereich zu unterstützen.

4.1 Externe Hilfe bei Vorfällen

Bereits bei der Untersuchung zum Anteil der Unternehmen mit Outsourcing-Partnern konnte festgestellt werden, dass die Schweizer Firmen im Bereich des Risikomanagements häufig auf Kompetenzen anderer Firmen angewiesen sind. Wenn nun ein Vorfall auftritt, der die Informationssicherheit bedroht, ist dies noch verstärkt der Fall. Es kann für Unternehmen aber auch problematisch sein, solche Hilfe anzufordern, weil eventuell Firmengeheimnisse an die Öffentlichkeit gelangen oder das Image des Unternehmens Schaden nehmen könnte. Es stellt sich deshalb die Frage, ob die Firmen bei Problemen mit der Informationssicherheit überhaupt externe Hilfe anfordern und wenn ja, bei wem.

Die Resultate der Befragung zeigen, dass 63% der Firmen, die einen für ihre Informationssicherheit relevanten Vorfall festgestellt haben, externe Hilfe beigezogen haben.[44] Die mittleren Firmen mit 10-49 Mitarbeitern fordern am häufigsten externe Hilfe an. Es bestätigt sich der Befund aus der Untersuchung zur Verbreitung von Outsourcing, dass die Firmen dieser Grössenklassen am stärksten auf fremde Unterstützung angewiesen sind. Ein Blick auf die Verteilung nach Branchen zeigt, dass die Teilnehmer aus der öffentlichen Verwaltung sehr oft externe Hilfe beiziehen (75%), während die Informatikunternehmen erwartungsgemäss seltener weitere Unterstützung benötigen (36%).

Von Interesse ist auch, wo die Firmen die nötige Hilfe finden. Die meisten Firmen wenden sich an ihre Outsourcing-Partner, den Hersteller ihrer Software oder den Internet Provider. Immerhin 40% geben aber auch an, dass sie sich mit Kollegen von anderen Firmen austauschen und 25% lassen sich über das Internet helfen.

44 Wiederum darf dieses Ergebnis nicht direkt auf die Gesamtheit aller Schweizer Unternehmen übertragen werden, da die Teilnehmer der Umfrage kein proportionales Abbild aller Firmen sind. Mit Hilfe des Verfahrens der Gewichtung (Anhang 3) kann aber geschätzt werden, dass ungefähr die Hälfte (47%) der Schweizer Firmen, die von einem solchen Vorfall betroffen waren, externe Hilfe in Anspruch nimmt.

Es zeigt sich also, dass Firmen nicht immer bezahlte Hilfe bei Experten suchen, sondern dass sie auch ein Interesse an gegenseitigem Austausch haben. Deshalb soll nun untersucht werden, wie die Kooperation unter den Firmen gestaltet werden könnte.

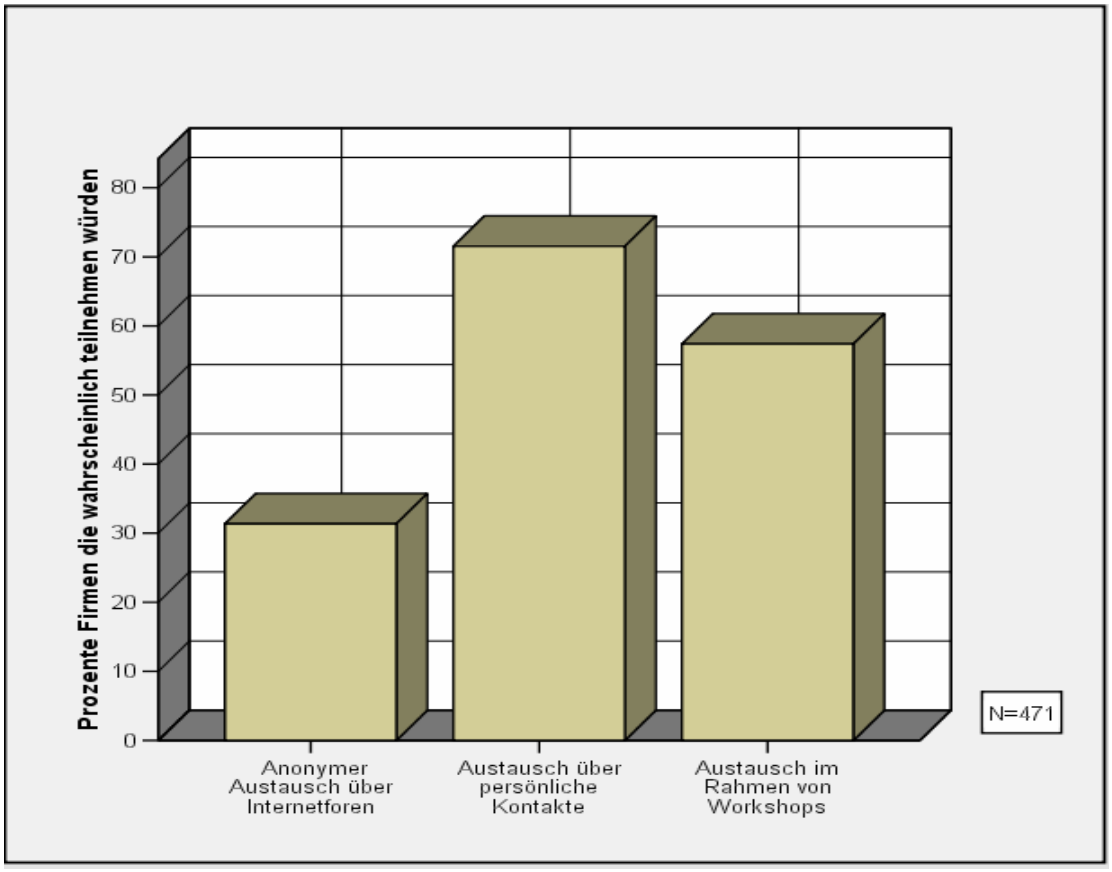
4.2 Kooperation zwischen den Unternehmen

Um zu erfahren, welche Zusammenarbeit für die Unternehmen sinnvoll sein könnte, müssen verschiedene Fragen geklärt werden. Zunächst muss abgeklärt werden, an welchen Formen der Kooperation die Firmen teilnehmen würden. Dann stellt sich aber auch die Frage, wer die Zusammenarbeit koordinieren könnte und schliesslich wird untersucht, ob die Bereitschaft vorhanden ist, für die Kooperation auch finanzielle Mittel aufzuwenden.

4.2.1 Mögliche Kooperationsformen

Damit klar wird, zu welcher Zusammenarbeit die Firmen bereit sind, wurden die Teilnehmer der Untersuchung gefragt, an welcher Form der Kooperation sie teilnehmen würden. Zur Auswahl standen der anonyme Austausch über Internetforen, der Austausch über persönliche Kontakte und der Austausch im Rahmen von Workshops. Abbildung 11 stellt die Ergebnisse dieser Frage dar.

Abbildung 11 Teilnahmebereitschaft nach Kooperationsformen



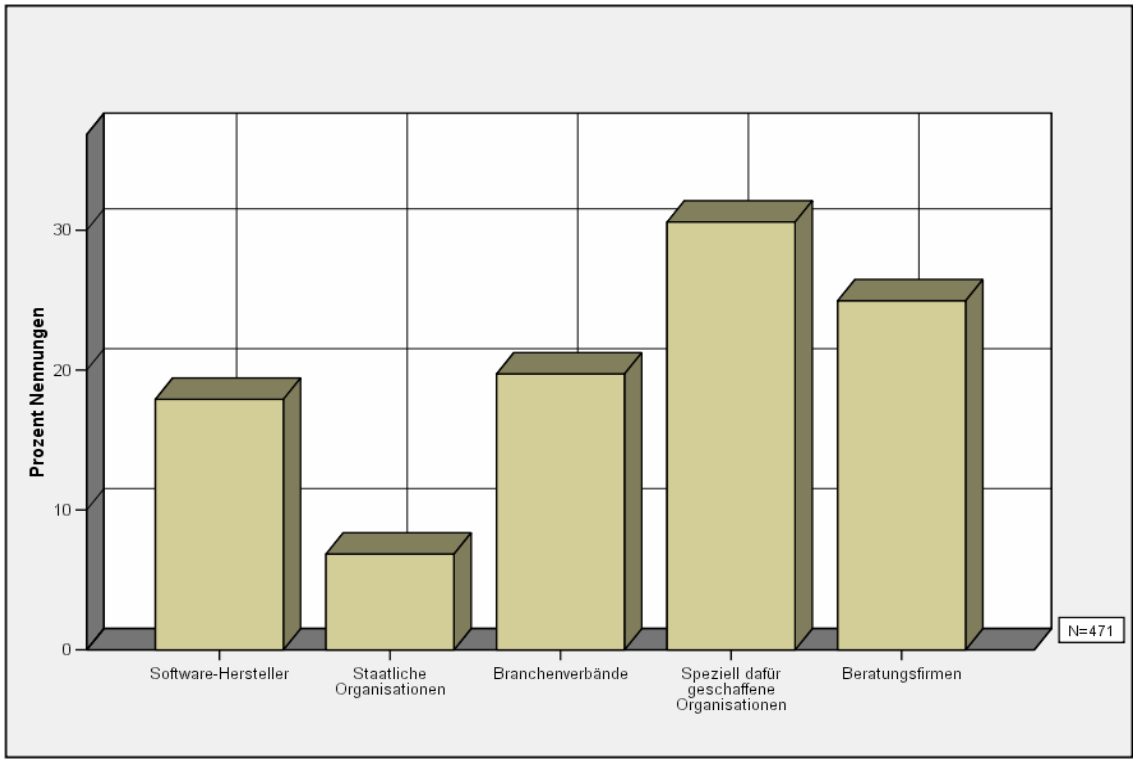
Am grössten ist die Bereitschaft zur Kooperation über persönliche Kontakte. Eine klare Mehrheit würde sich an einem Austausch dieser Art beteiligen. Auch die Idee von Workshops findet Anklang.[45] Das grosse Interesse an einem Austausch unter Kollegen ist bemerkenswert. Offensichtlich ist den Verantwortlichen für die Informationssicherheit bewusst, dass die Probleme in vielen Firmen ähnlich sind und dass man voneinander profitieren könnte. Rund ein Drittel der Befragten (31%) kann sich vorstellen, über das Internet Fragen der Informationssicherheit zu diskutieren.

Offenbar besteht ein Bedürfnis nach Kooperation. Deshalb ist es wichtig zu wissen, wer die allfällige Koordination der Zusammenarbeit übernehmen könnte und ob die Firmen eventuell bereit wären, einen finanziellen Beitrag an eine solche Organisation zu leisten.

4.2.2 Die Organisation der Kooperation

Selbst wenn viele Untenehmen eine Kooperation wünschen, so muss doch jemand bereit sein, die Organisation dieser Kooperation zu übernehmen. Deshalb wurden die Firmen gefragt, wer ihrer Meinung nach am besten geeignet wäre, im Sinne eines Kompetenzzentrums die Zusammenarbeit zwischen den Firmen zu koordinieren. Als Antwortenmöglichkeiten wurden die Software-Hersteller, staatliche Organisationen, die Branchenverbände, Beratungsfirmen und speziell dafür geschaffene Organisationen vorgeschlagen. Abbildung 12 stellt dar, welchen Akteur die befragten Unternehmen bevorzugen würden.

Abbildung 12 Mögliche Organisatoren der Kooperation



45 Es wurde differenziert zwischen Workshops, welche von Software-Herstellern organisiert werden und Workshops, die von unabhängigen Dritten durchgeführt werden. An Workshops von Softwareherstellern würden 41% teilnehmen, an solchen, die von unabhängigen Dritten durchgeführt werden, 50%. In der Graphik werden alle Firmen berücksichtigt, die an einer der beiden Möglichkeiten teilnehmen würden.

Es zeigt sich, dass über 30% der Unternehmen der Ansicht sind, dass die Koordination der Zusammenarbeit am besten durch Organisationen geleistet werden kann, die extra für diesen Zweck geschaffen werden. Wie diese Organisationen gestaltet werden könnten, wird vorläufig offengelassen.

25% aller Befragten wünschen sich Beratungsfirmen für die Zusammenarbeit. Auch Software-Hersteller (18%) dürften vor allem deshalb genannt worden sein, weil sie bereits mit vielen Firmen zusammenarbeiten. Die Branchenverbände werden auch recht oft genannt (20%). Deren Vorteil ist, dass sie bereits Erfahrung in der Koordination und Organisation von Kooperation haben.

Die kleineren Firmen favorisieren Software-Hersteller und Beratungsfirmen, während die mittleren und grossen Unternehmen häufiger Branchenverbände und vor allem speziell für diese Aufgaben geschaffene Organisationen nennen.[46] Vermutlich sind kleine Firmen stärker an einer Beratung im Sinne einer Wissensvermittlung interessiert. Mittlere und grosse Firmen suchen dagegen wohl eher eine Zusammenarbeit mit gegenseitigem Austausch.

Die Auswertung zeigt auch deutlich, dass die direkte Beratung und Betreuung der Kooperation nicht als Aufgabe des Staates verstanden wird. Zur Rolle, die der Staat spielt, wird im nächsten Kapitel noch mehr zu sagen sein. Zuvor wird die Frage besprochen, ob die Unternehmen bereit wären, einen finanziellen Beitrag zur Organisation der Zusammenarbeit zu leisten.

4.2.3 Die Finanzierung der Kooperation

Die Frage zur Finanzierung der Kooperation wurde sehr allgemein formuliert. Es wurde erhoben, ob sich die Unternehmen vorstellen können, sich mit bis zu 500 Fr. oder bis zu 2'000 Fr. jährlich an Organisationen zu beteiligen, die Informationen über Informationssicherheit anbieten und die Zusammenarbeit koordinieren. Die Angaben sollen Ausdruck der Bereitschaft sein, die Kosten für die Kooperation mitzutragen.

Weil die Frage wenig konkret formuliert war und einige der Ausfüllenden wohl auch nicht über die notwendige Kompetenz verfügen, über finanzielle Verpflichtungen ihrer Firma zu entscheiden, ist der Anteil jener, welche die Frage nicht beantworten konnten, mit 36% sehr hoch. Von den Antwortenden gaben schliesslich 71% an, dass sie nicht bereit wären, einen Beitrag zu zahlen, 22% würden bis zu 500 Fr. zahlen und 8% bis zu 2'000 Fr. Es sind vor allem Grossfirmen, welche bereit wären, einen Beitrag zu leisten, denn bei grossen Budgets fällt ein bescheidenes finanzielles Engagement für die Kooperation im Bereich der Informationssicherheit viel weniger ins Gewicht. 55% der Grossfirmen wären bereit, einen Beitrag zu zahlen. Bei den Mikrounternehmen sind es hingegen nur 15%, welche sich vorstellen könnten, bis 500 Fr. zu entrichten.

Es ist wenig erstaunlich, dass die überwiegende Mehrheit eine finanzielle Beteiligung ablehnt, besonders wenn man sich in Erinnerung ruft, dass die Budgets der meisten Firmen für die Informationssicherheit knapp sind. Dennoch wären mehr als die Hälfte der Grossfirmen und auch noch ein Drittel der mittleren Firmen mit 50-249 Mitarbeitern bereit, sich an den Kosten einer Organisation zur Zusammenarbeit im Bereich der Informationssicherheit zu beteiligen.

46 29% der kleinen und kleinsten Firmen mit weniger als 10 Mitarbeitern wünschen sich die Software-Anbieter als Organisatoren der Kooperation, weitere 28% halten die Beratungsfirmen für diesen Zweck am geeignetsten. 43% der Grossfirmen halten spezielle Organisationen für notwendig.

Dies verdeutlicht nochmals, dass zumindest die mittleren und grösseren Unternehmen ein Bedürfnis nach einer stärkeren Kooperation im Bereich der Informationssicherheit haben.

4.3 Kooperation mit dem Staat

Die Erkenntnis, dass die Informationssicherheit ein Problem ist, das die gesamte Wirtschaft betrifft, wirft auch die Frage auf, ob und wie der Staat die Unternehmen bei ihren Schutzmassnahmen unterstützen kann und soll.

Es gehört zu den traditionellen Aufgaben des Staates, die Infrastrukturen zu schützen, welche für das Wohlergehen der Bevölkerung von zentraler Bedeutung sind. Weil dieses Wohlergehen in modernen Gesellschaften stark von funktionierenden Informations- und Kommunikationstechnologien abhängt, ist der Schutz von Informationsinfrastrukturen zu einer wichtigen Staatsaufgabe geworden. Diese Aufgabe, die international unter dem Begriff *Critical Information Infrastructure Protection* (CIIP) diskutiert wird[47], kann der Staat nur in Zusammenarbeit mit den privatwirtschaftlichen Unternehmen erfüllen. Der Staat hat deshalb ein Interesse daran, mit den Unternehmen zu kooperieren und sie beim Schutz ihrer Informatik zu unterstützen. Im Gegensatz zu den Unternehmen verfolgt der Staat aber eine längerfristige Perspektive, die über die blosse Sicherstellung der Geschäftstätigkeit hinausgeht.

Auch wegen dieser unterschiedlichen Perspektiven im Bereich der Informationssicherheit stellt sich die Frage, ob auch die Unternehmen eine Zusammenarbeit mit dem Staat wünschen. Wie bereits gesehen, halten nur wenige Firmen den Staat für den geeigneten Akteur, um die Kooperation zwischen den Unternehmen zu koordinieren. Die Rolle des Staates wird also von den Firmen eher kritisch beurteilt. Aus diesen Gründen ist es wichtig zu überprüfen, wie intensiv die bisherige Zusammenarbeit zwischen Staat und Unternehmen ist.

4.3.1 Die Rolle der Polizei

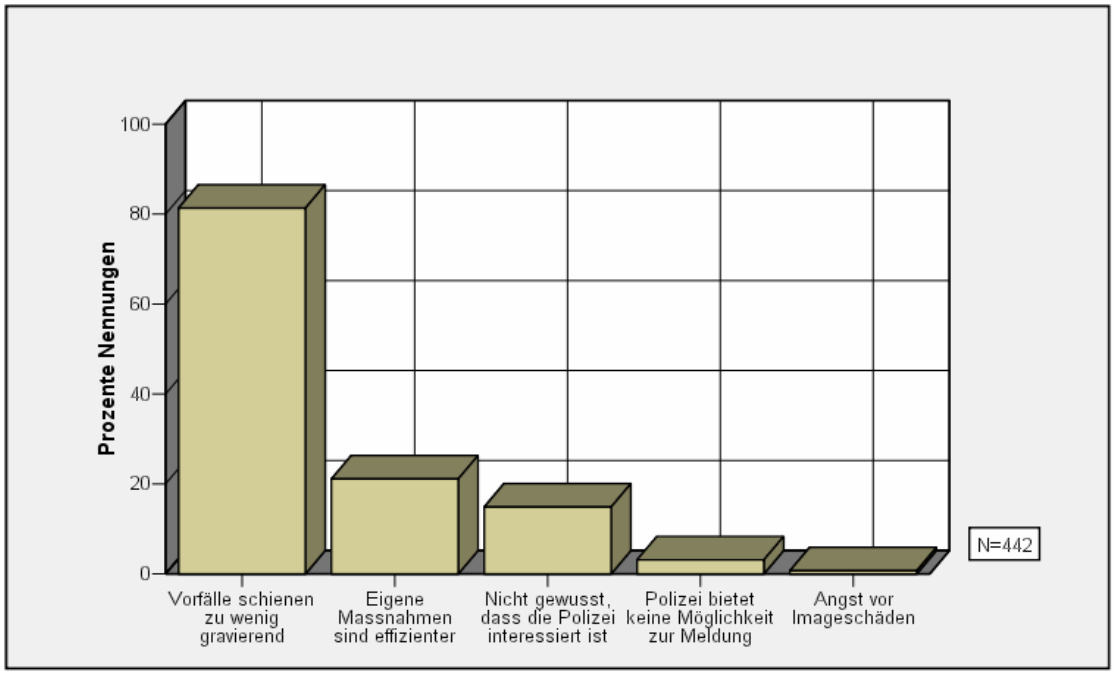
Wenn Privatpersonen oder Firmen betrogen oder bestohlen werden, wenden sie sich üblicherweise an die Polizei. Diese ist im Staat zuständig für die Gewährleistung der Sicherheit gegenüber Angriffen auf das Eigentum. Doch schalten die Unternehmen auch die Polizei ein, wenn ihre Informatikinfrastruktur angegriffen wird oder wenn Daten gestohlen werden?

In der Umfrage wurde erhoben, ob die Firmen schon einmal wegen eines Vorfalls betreffend die Informationssicherheit die Polizei eingeschaltet haben. Das Ergebnis ist deutlich: Nur 34 der 562 befragten Unternehmen (6%) bejahten die Frage. Von diesen 34 sind 15 Grossunternehmen. Im internationalen Vergleich bestätigt sich, dass die Firmen bei Vorfällen betreffend die Informationssicherheit nur sehr selten die Polizei benachrichtigen. Der FBI „Computer Crime Survey" hat ergeben, dass 9.1% der US-Firmen sich in einem solchen Fall an die Polizei wenden.

Nun interessiert natürlich, warum dieser Prozentsatz so tief ist. Die Unternehmen wurden deswegen nach den Gründen gefragt, weshalb sie die Polizei nicht eingeschaltet haben. Abbildung 13 zeigt die Häufigkeit der Nennungen der Gründe, wobei auch mehrere Gründe ausgewählt werden konnten.

47 Mehr zur Thematik der Critical Information Infrastructure Protection in: Abele-Wigert, Isabelle und Myriam Dunn, The International Critical Information Infrastructure Handbook 2006. An Inventory and Analysis of Protection Policies in Twenty Countries (Zurich, 2006).

Abbildung 13 Gründe, warum die Polizei nicht eingeschaltet wurde



Offenbar halten sehr viele Firmen ihre Vorfälle für zu wenig gravierend, um die Polizei zu benachrichtigen. Vorfälle mit Malware gehören für viele zum Geschäftsalltag und werden deshalb nicht gemeldet. Es ist auch wenig überraschend, dass jede fünfte Firma ihre eigenen Massnahmen für effizienter hält. Weniger entscheidend ist das Verhalten der Polizei. Nur wenige Firmen geben an, keine Meldung erstattet zu haben, weil sie glaubten, die Polizei interessiere sich nicht für solche Fälle oder biete keine Möglichkeiten zur Meldung an. Bemerkenswert ist auch, dass die Angst vor Imageschäden die Firmen entgegen weitverbreiteter Meinung kaum davon abhält, Meldung zu erstatten.

Wiederum werden diese Resultate im Vergleich mit dem „Computer Crime Survey" des FBI bestätigt. Auch dort ist der wichtigste Grund, der die Firmen veranlasst, die Polizei nicht einzuschalten, der, dass die Vorfälle als zu wenig gravierend eingeschätzt werden.[48]

4.3.2 Die Melde- und Analysestelle für Informationssicherung (MELANI)

Ein Polizeieinsatz erscheint den Firmen also in den wenigsten Fällen sinnvoll. Viele Probleme der Informationssicherheit lassen sich aber durch die konventionellen Strafverfolgungsbehörden auch gar nicht lösen. Darum werden von Seiten des Staates andere Formen gesucht, die Wirtschaft in Bezug auf die Informationssicherheit zu unterstützen. Zu diesem Zweck wurde die Melde- und Analysestelle für Informationssicherung (MELANI) gegründet. In Zusammenarbeit mit Organisationen aus der Wirtschaft und den Behörden soll MELANI neue Gefahren und Bedrohungen möglichst früh erkennen und den Unternehmen die Möglichkeit bieten, Vorfälle zu melden.[49] MELANI hat am 1. Oktober 2004 seine Tätigkeit aufgenommen. Regelmässig werden Hinweise zur aktuellen Bedrohungslage und Warnungen vor neuen Gefahren auf der

48 Federal Bureau of Investigation (FBI), *2005 FBI Computer Crime Survey* (2005), S. 12.

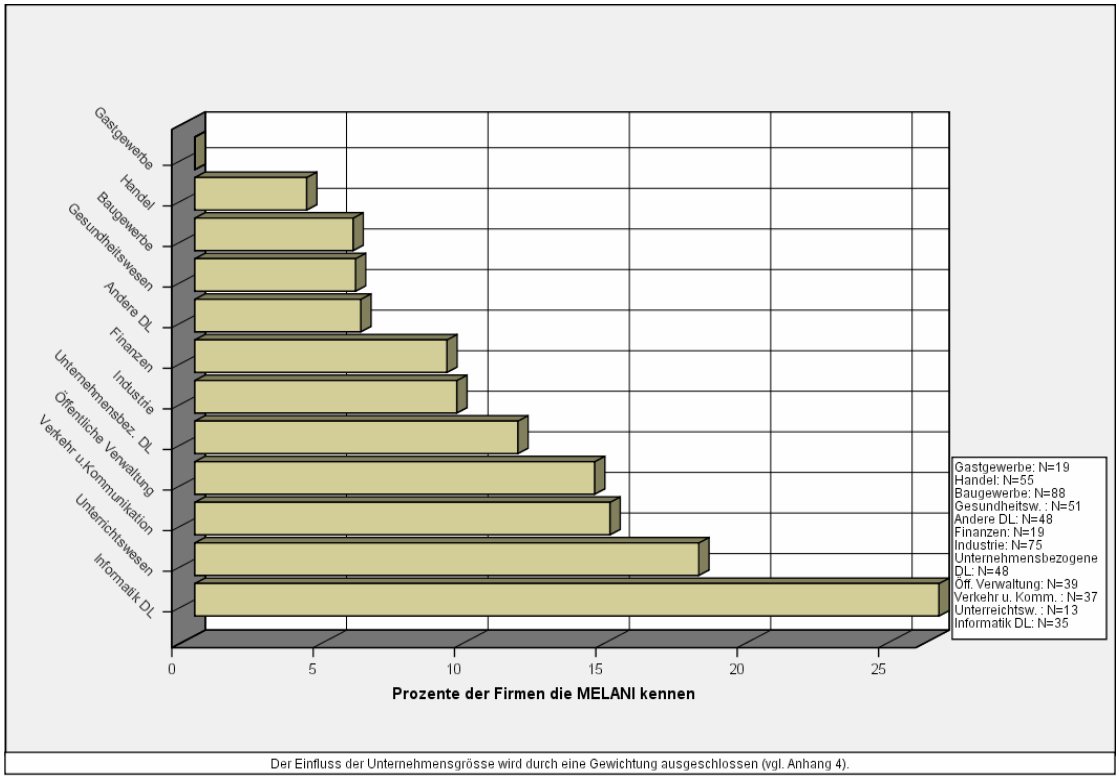
49 Die wichtigsten Partner sind dabei das Informatikstrategieorgan des Bundes (ISB), der Dienst für Analyse und Prävention (DAP) des Bundesamts für Polizei, sowie das Computer Emergency Response Team der Stiftung Switch (www.switch.ch).

Homepage von MELANI publiziert.[50] Natürlich nützen diese Angaben nur etwas, wenn sie von den Unternehmen auch beachtet werden. Es ist darum von grosser Bedeutung zu wissen, wie bekannt MELANI nach etwas mehr als einem Jahr bei den Firmen ist.

Von den befragten Firmen kennen 10% MELANI. Dabei gilt es zu beachten, dass MELANI mit ausgewählten grossen Betreibern kritischer Infrastrukturen enger zusammenarbeitet. Diese haben an der Umfrage nicht teilgenommen.

Der Anteil der Unternehmen, die MELANI kennen, nimmt mit der Grösse der Firma stark zu. Während nur 4% der Mikrounternehmen mit weniger als fünf Mitarbeitern MELANI kennen, sind es bei den Grossfirmen immerhin bereits 28%. Wie Abbildung 14 zeigt, bestehen auch unter den Branchen erhebliche Unterschiede.

Abbildung 14 Bekanntheit von MELANI nach Branchen



MELANI ist bei den Unternehmen der Informatikbranche mit Abstand am bekanntesten. Im ersten Jahr ihres Bestehens hat MELANI also bei den Unternehmen die sich stark mit dem Thema der Informationssicherheit auseinandersetzen (Grossfirmen und Unternehmen aus der Informatikbranche) bereits einen relativ hohen Bekanntheitsgrad erreicht.

Weil die Probleme mit der Informationssicherheit je nach Grösse und Branchenzugehörigkeit der Firmen eine unterschiedliche Qualität und Quantität haben, ist es für MELANI schwierig, alle Bedürfnisse abzudecken. Während für Grossfirmen eine spezifische Beratung unter Fachleuten notwendig ist, sind mittlere Firmen eher an allgemeinen Ratschlägen interessiert. Welche Lösungen für dieses Problem möglich wären, soll nun in den Schlussfolgerungen der Studie näher erläutert werden.

50 www.melani.admin.ch.

5 Erkenntnisse und Schlussfolgerungen

Das Ziel der Studie war, einen Überblick zu gewinnen, welchen Bedrohungen die Informatik der Schweizer Unternehmen ausgesetzt ist und wie sie geschützt wird. Die Analysen haben gezeigt, dass die Bedrohungen für die Informationssicherheit weit verbreitet sind und das Risikomanagement in diesem Bereich für alle Firmen ein wichtiges Thema ist. Es wurde aber auch klar, dass zwischen den verschiedenen Firmen wesentliche Unterschiede bestehen. Welche Konsequenzen sich aus diesen Befunden ergeben, soll in diesem letzten Kapitel diskutiert werden.

5.1 Unterschiedliche Bedrohungen – unterschiedliches Risikomanagement – unterschiedliche Bedürfnisse

Die erste wichtige Erkenntnis der Studie ist, dass die Bedrohungen in Sachen Informationssicherheit für die verschiedenen Firmen ein sehr unterschiedliches Ausmass annehmen können. Dabei hat die Branchenzugehörigkeit der Firmen einen Einfluss, aber noch wichtiger scheint die Grösse der Unternehmen. Während kleine und mittlere Betriebe vor allem von Malware betroffen sind, hat bereits jedes fünfte Grossunternehmen im Jahr 2005 einen gezielten Angriff auf seine Informatikinfrastruktur festgestellt. Bei der Beurteilung der Resultate soll deshalb zwischen Grossfirmen, mittleren Betrieben und Kleinstunternehmen unterschieden werden.

5.1.1 Die Kleinstunternehmen

Die Kleinstunternehmen mit weniger als fünf Mitarbeitern sind am wenigsten betroffen von den Bedrohungen für die Informationssicherheit. Ihr Betrieb hängt oft weniger stark von der Informatik ab als bei grösseren Firmen, und sie bieten meist auch kein attraktives Ziel für Hacker. Deshalb steht bei ihnen der elementare Schutz im Vordergrund. Aufwändige technische Massnahmen und ausführliche Sicherheitskonzepte machen häufig wenig Sinn. Deswegen kann von einer relativ hohen Selbständigkeit der Kleinstunternehmen im Bereich der Informationssicherheit ausgegangen werden – was nötig ist, können diese Firmen selbst umsetzen. Praxisbezogene Empfehlungen, eventuell auch Schulungen, dürften hingegen für die Kleinstunternehmen sehr hilfreich sein, sind doch in den wenigsten dieser Betriebe Informatiker beschäftigt.

5.1.2 Die mittleren Unternehmen

Die Informatik ist bei mittleren Firmen im Gegensatz zu den Kleinstunternehmen bereits ein entscheidender Faktor der Organisation des Betriebes. Mittlere Firmen sind häufig von einer funktionierenden Informatikinfrastruktur abhängig. Dadurch steigt natürlich auch das Sicherheitsbedürfnis in diesem Bereich. Der technische Schutz vor Malware kann nicht mehr genügen, es müssen Konzepte erarbeitet und Mitarbeiter instruiert werden. Meist sind die mittleren Firmen dann aber doch zu klein, um sich Spezialisten zu leisten, die für die Informationssicherheit verantwortlich sind. Es erstaunt darum nicht, dass vor allem mittlere Unternehmen Unterstützung im Bereich der Informationssicherheit suchen. Sie arbeiten am häufigsten mit Outsourcing-Partnern zusammen, versichern sich am meisten und suchen überdurchschnittlich oft externe Hilfe bei Vorfällen. Weil viele der mittleren Unternehmen keine

Informatiker angestellt haben, sich aber dennoch mit komplexen Schutzmassnahmen auseinandersetzen müssen, könnten vor allem Schulungen und Weiterbildungen sowie Plattformen für den Erfahrungsaustausch für diese Unternehmen nützlich sein.

5.1.3 Die Grossunternehmen

Wiederum andere Bedürfnisse haben die Grossunternehmen. Weil ihre Informatik am stärksten bedroht ist, müssen sie viel umfassendere Schutzmassnahmen ergreifen. Sie wenden mehr Geld und Personal auf, benutzen komplexere technische Massnahmen und setzen häufiger Sicherheitskonzepte ein. Allerdings sind sie wegen der häufigeren gezielten Angriffen auch viel umfassenderen Bedrohungen ausgesetzt. Die Methoden der Hacker ändern sich schnell, und es gilt möglichst immer auf dem neuesten Stand zu sein. Dabei gelangen auch die angestellten Spezialisten und Informatikteams schnell an ihre Kapazitätsgrenzen.

Grossunternehmen sind deshalb vor allem an spezifischer Beratung unter Fachleuten interessiert. Es geht nicht um allgemeine Fragen im Bereich der Informationssicherheit, sondern um konkrete Umsetzungen von aufwändigen und technisch anspruchsvollen Massnahmen. Zudem sind diese Firmen stark vernetzt, und es bestehen oft gegenseitige Abhängigkeiten. Neben der Beratung muss daher auch die Zusammenarbeit und der gegenseitige Austausch organisiert und gefördert werden. Auch die Zusammenarbeit mit der Polizei kann für Grossfirmen bei Angriffen auf ihre Informationssicherheit ein wichtiges Anliegen sein.

Die Anliegen der Grossfirmen unterscheiden sich damit deutlich von jenen der kleinen und mittleren Unternehmen. Ihre Bedürfnisse nach spezifischer Beratung und Kooperation sind aber schon länger bekannt, und es wurde ihnen mit dem Angebot einer engen Zusammenarbeit mit MELANI auch Rechnung getragen. Eine sehr intensive Kooperation kann aber aus Kosten- und Ressourcengründen nur einem relativ kleinen Kreis der Grossunternehmen zur Verfügung gestellt werden.

5.2 Kooperation trotz unterschiedlichen Bedürfnissen: Warning, Advice and Reporting Points (WARPs) als mögliche Lösung

Eine zweite wichtige Erkenntnis der Studie ist, dass die Schweizer Unternehmen im Bereich der Informationssicherheit gerne mehr zusammenarbeiten würden. Viele Firmen kämpfen mit ähnlichen Schwierigkeiten und könnten von einem Erfahrungsaustausch profitieren. Das Problem bei der Umsetzung der Kooperation liegt nun darin, dass die verschiedenen Unternehmen wie gesehen sehr unterschiedliche Bedürfnisse haben.

Eine mögliche Lösung dieses Problems könnte die Schaffung von Warning, Advice and Reporting Points (WARPs) sein. Das „National Infrastructure Security Co-ordintation Center" (NISCC) der britischen Regierung propagiert solche WARPs als ideale Platform für den Austausch und die Zusammenarbeit im Bereich der Informationssicherheit.[51] Mitglieder von WARPs tauschen Informationen aus und bekämpfen gemeinsam die Bedrohungen für die Informationssicherheit. Dadurch werden neue Bedrohungen früher erkannt und mögliche Lösungen allen Mitgliedern zur Verfügung gestellt. Entscheidend ist, dass WARPs je nach Bedürfnis unter Firmen aus der gleichen Branche, der gleichen Region oder ähnlicher Grössenklassen gebildet werden können. Innerhalb der WARPs kooperieren dann Unternehmen,

51 http://www.niscc.gov.uk/niscc/warpInfo-en.html.

die ähnliche Probleme und ähnliche Bedürfnisse haben. Die Resultate der Studie weisen darauf hin, dass die Grösse der Firmen ein Hauptkriterium bei der Gestaltung von WARPs sein müsste. Während nämlich Grossfirmen vor allem an spezifischer Beratung unter Fachleuten interessiert sind, besteht bei kleinen und mittleren Firmen ein Bedürfnis nach allgemeiner Beratung und gegenseitigem Austausch. Gerade für mittlere Firmen könnten deshalb WARPs geeignet sein, denn durch die Kooperation mit vergleichbaren Unternehmen kann die Informationssicherheit verbessert werden, ohne dass dabei hohe Kosten anfallen.

Der Staat könnte den Impetus für solche WARPs geben und diese anfänglich koordinieren. Bei der Gründung von WARPs dürfte die Unterstützung von Seiten des Staates nötig sein, weil die Firmen sich tendenziell erst an solchen Organisationen beteiligen, wenn diese ihren Nutzen bereits unter Beweis gestellt haben. Daneben wäre aber auch eine Koordination zwischen den verschiedenen WARPs wichtig, weil es zwischen diesen auch wieder Schnittstellen gäbe, die genutzt werden könnten. Während sich also die Unternehmen in spezialisierten WARPs auf die Sicherstellung ihrer Geschäftstätigkeit konzentrieren könnten, würde der Staat durch die Koordination dieser verschiedenen Organisationen die Sicherheit der gesamten Wirtschaft fördern, was seiner sicherheitspolitischen Motivation entspräche.

6 Literaturverzeichnis

Abele-Wigert, Isabelle and Myriam Dunn, *The International Critical InformationInfrastructure Protection (CIIP) Handbook 2006. An Inventory and Analysis of Protection Policies in Twenty Countries* (Zurich, 2006). http://www.isn.ethz.ch/pubs/ph/details.cfm?id=16156.

Bidgoli, Hossein et al. (eds.), *Handbook of Information Security Volume 1-3* (Hoboken, 2006).

Bundesamt für Sicherheit für Sicherheit in der Informationstechnik (BSI), *Die Lage der IT-Sicherheit in Deutschland 2005* (Juli 2005). http://www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf

Computer Security Institute(CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005). http://www.gocsi.com

Dübendorfer, Thomas, Arno Wagner und Bernhard Plattner, *An Economic Model for Large-Scale Internet Attacks* (Studie des Computer Engineering and Networks Laboratory der ETH Zürich, 2004). http://www.tik.ee.ethz.ch/~ddosvax/publications/papers/WETICE-ES-duebendorfer-economic_damage_model.pdf

Eckert, Claudia, *IT-Sicherheit: Konzepte – Verfahren – Protokolle* (3. überarb. und erw. Auflage, München und Oldenbourg, 2004).

Federal Bureau of Investigation (FBI), *2005 FBI Computer Crime Survey* (2005). http://www.fbi.gov/publications/ccs2005.pdf

Gartner Research, *Enterprises and Employees: The Growth of Distrust* (2005). Zusammenfassung der Resultate auf: http://www.csoonline.com/analyst/report3317.html

Haldemann, Lukas, *Versicherung von Internet-Risiken* (Seminararbeit am Departement Informatik der ETH Zürich, 2001). http://www.ifi.unizh.ch/ikm/Vorlesungen/inf_recht/2001/Haldemann.pdf

KPMG, *IT-Management 2005: Standortbestimmung und Trends in der Schweizer Informatik* (Zürich und Genf, 2005).

Melde- und Analysestelle Informationssicherung (MELANI), *Informationssicherung. Lage in der Schweiz und International. Halbjahresbericht 2005/1* (2005). http://www.melani.admin.ch/berichte/lageberichte/index.html?lang=de#sprungmarke0_3

Melde- und Analysestelle Informationssicherung (MELANI), *Informationssicherung. Lage in der Schweiz und International. Halbjahresbericht 2005/2* (2006). http://www.melani.admin.ch/berichte/lageberichte/index.html?lang=de#sprungmarke0_3

National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005). http://www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf

Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Studie im Auftrag des Staatssekretariates für Wirtschaft, Bern, 2002).

7 Anhang

Anhang 1: Zusammensetzung der Stichprobe / Einteilung der Unternehmen

- Die **Grundgesamtheit bilden alle Schweizer Unternehmen** aus dem zweiten und dritten Sektor.
- Ausgeschlossen wurden alle Grossunternehmen, die zum Kundenkreis von MELANI-Net gehören.
- Es wurde für die Umfrage ein Umfang von mind. 500 Teilnehmern angestrebt. Die Rücklaufquote wurde auf 10% der angefragten Unternehmen geschätzt. Daraus ergab sich eine **angestrebte Stichprobengrösse von 5'000 Firmen**.

- **Unterscheidungskriterien der Firmen:**
  a) **Grössenklassen:**
     - Kleinstfirmen (Mikrounternehmen): 0-4 Vollzeitstellen
     - Kleine Unternehmen: 5-9 Vollzeitstellen
     - Mittlere Unternehmen: 10-49 Vollzeitstellen
     - Grosse Unternehmen: 50-249 Vollzeitstellen
     - Grossunternehmen: mehr als 250 Vollzeitstellen

  b) **Branchen** gemäss der Systematik der Wirtschaftszweige des Bundesamtes für Statistik.[52]
     - **Industrie, Herstellung von Waren:** Einheiten, die Stoffe oder Teile mechanisch, physikalisch oder chemisch in Waren umwandeln.
     - **Baugewerbe:** Hoch- und Tiefbau, Bauinstallationen und sonstiger Ausbau.
     - **Handel:** Gross- und Detailhandel (Verkauf ohne Weiterverarbeitung) mit jeder Art von Waren und die Erbringung von Dienstleistungen beim Verkauf von Handelswaren.
     - **Gastgewerbe:** Gewährung von Unterkunft und/oder Zubereitung von Mahlzeiten, Snacks und Getränken zum sofortigen Verzehr für Gäste.
     - **Verkehr und Kommunikation:** Tätigkeiten im Zusammenhang mit der Personen- und Güterbeförderung im Linien- oder Gelegenheitsverkehr auf Schienen und Strassen, zu Wasser und in der Luft sowie Transport in Rohrfernleitungen. Hilfs- und Nebentätigkeiten im Zusammenhang mit Bahnhöfen, Häfen und Flughäfen, Parkplätzen und Parkhäusern sowie Frachtumschlag, Lagerung usw. Post- und Fernmeldewesen. Vermietung von Fahrzeugen mit Fahrer oder Bedienungspersonal.
     - **Finanzwesen:** Entgegennahme und Verteilung von Finanzmitteln zu anderen Zwecken als die obligatorische Altersversicherung, Versicherungen und Pensionskassen.
     - **Unternehmensbezogene Dienstleistungen:** Tätigkeiten, die sich im Wesentlichen auf den Unternehmenssektor beziehen. Doch mehr oder weniger alle der in diesem Unterabschnitt genannten Tätigkeiten können auch für private Haushalte erbracht werden, z.B. Vermietung von Gebrauchsgütern,

52 NOGA: Nomenclature Générale des Activités économiques. Mehr zu dieser Systematik auf der Homepage des Bundesamtes für Statistik:
http://www.bfs.admin.ch/bfs/portal/de/index/infothek/nomenklaturen/blank/blank/noga0/publikationen.html

Datenbanken, Rechtsberatung, Detekteien sowie Wach- und Sicherheitsdienste, Innendekorateuren oder Fotografie und Fotolabors.

- **Informatik Dienstleistungen:** Tätigkeiten im Zusammenhang mit Hard- oder Software und allgemeiner Datenverarbeitung.
- **Öffentliche Verwaltung:** die Tätigkeiten, die normalerweise von der öffentlichen Verwaltung ausgeführt werden. Dabei ist der rechtliche oder institutionelle Status der Verwaltung per se nicht entscheidend.
- **Unterrichtswesen:** öffentliches und privates Unterrichtswesen auf allen Stufen und in allen Fächern in den verschiedenen Lehranstalten des regulären Schulsystems, aber auch durch Erwachsenenbildung, Alphabetisierungsprogramme usw.
- **Gesundheitswesen:** Krankenhäuser, Arztpraxen, Veterinärwesen, Sozialwesen (inkl. Alters-, Pflege-, Jugendheime).
- **Andere Dienstleistungen:** Dienstleistungen die nicht in erster Linie auf den Unternehmenssektor beziehen (z.B.: Kultur, Sport, Wäscherei, Coiffeur-, Kosmetiksalons usw.).

- **Stichprobenplan:**
  Die Stichprobe musste so geschichtet werden, dass Aussagen für die verschiedenen Grössenklassen und für die verschiedenen Branchen möglich wurden. Es wurde deshalb ein disproportionaler Stichprobenansatz (Quota-Random) gewählt. Dabei sind einzelne Schichten über- oder untervertreten, was später mit einer Gewichtung wieder korrigiert werden musste. Für viele Branchen war bei der Kategorie der Firmen mit mehr als 250 Mitarbeitern eine Vollerhebung aller Firmen nötig, da nur wenige Grossfirmen existieren.
  Die Adressen der Firmen wurden nach folgendem Stichprobenplan beim Bundesamt für Statistik bestellt:

Quotenvorgaben für die Adressenbestellung

NOGA Abschnitte (Abteilungen)	Grössenkateogorien (Vzeq)		
	0-9	10-249	250+
D Herstellung von Waren (15-37)	330	420	250
F Bau (45)	300	390	VE
G Handel (50-52)	500	400	100
H Beherbergungs- und Gaststätten (55)	220	320	VE
I Verkehr und Nachrichtenübermittlung (60-64)	200	200	VE
J Kreditinstitute und Versicherungen (65-67)	120	160	VE
K Immobilienwesen, Dienstl. für Unternehmen (70-74)	550	350	VE
L Öffentliche Verwaltung, Verteidigung, Sozialversicherung (75)	60	130	VE
M Erziehung und Unterricht (80)	140	210	VE
N Gesundheits- Veterinär- und Sozialwesen (85)	270	220	100
O Sonstige Dienstleistungen für Dritte (90-93)	310	200	VE
Total	**3'000**	**3'000**	**~1000**

Vzeq=Vollzeitäquivalente
VE=Vollerhebung

- Es wurde eine Reserve von 2'000 Adressen bewahrt. Verschickt wurde die Umfrage an 5'000 Firmen, wobei die Adressen einiger Firmen veraltet waren. Es ergab sich eine tatsächliche Stichprobengrösse von 4'916 Firmen.

Anhang 2: Der Rücklauf

- 562 Firmen haben an der Umfrage teilgenommen, die **Rücklaufquote** beträgt somit **11.45%**.
- Es wurde keine systematische Analyse der **Nichtteilnehmer** durchgeführt. Wie bei jeder Umfrage, bei welcher nur ein Teil der Angeschriebenen den Fragebogen ausfüllt, besteht die Gefahr, dass sich die Teilnehmer in wichtigen Bereichen vom Durchschnitt abheben. Es wäre denkbar, dass die Teilnahme an der Umfrage bereits ein Hinweis darauf ist, dass sich eine Firma stärker für die Thematik der Informatiksicherheit interessiert als andere. Hinweise auf die Gründe für Nichtteilnahme an der Umfrage liefern die Firmen, welche sich von der Umfrage abgemeldet haben. Von **44 Abmeldungen** erfolgten die Hälfte wegen mangelndem Interesse oder fehlender Zeit. 8 Firmen gaben an, keine Informatik zu benutzen, weitere 10 bezeichneten sich für die Fragen als nicht zuständig, und 4 Firmen wollten den Fragebogen aus Sicherheitsgründen nicht ausfüllen.

- Rücklauf nach Grösseklassen:

Grösse	Anzahl	Prozent
0-4	132	23.49
5-9	62	11.03
10-49	195	34.70
50-249	86	15.30
>250	87	15.48

- Rücklauf nach Branche:

Branche	**Anzahl**	**Prozent**
Industrie	82	14.59
Baugewerbe	92	16.37
Handel	59	10.50
Gastgewerbe	20	3.56
Verkehr u. Komm.	37	6.58
Finanzwesen	21	3.74
Unternehmensbez. DL	53	9.43
Infomatik DL	37	6.58
Öffentliche Verwaltung	42	7.47
Unterrichtswesen	14	2.49
Gesundheitswesen	56	9.96
Andere DL	49	8.72

Anhang 3: Gewichtung der Daten

- **Die Teilnehmer der Umfrage sind in Bezug auf die Unternehmensgrösse und die Branchenzugehörigkeit kein Abbild der Realität**. Während in der Realität nur 0.3% aller Unternehmen mehr als 250 Mitarbeiter beschäftigen, sind es bei den Teilnehmern der Umfrage 15%. Bei den Branchen sind Firmen der Baubranche überproportional vertreten, während die unternehmensbezogenen Dienstleistungsunternehmen und das Gastgewerbe untervertreten sind.
- Die unproportionale Abbildung der Wirklichkeit ist notwendig, damit jeweils genügend Daten für einen Vergleich vorhanden sind. Gleichzeitig bedeutet dies aber, dass von den Aussagen über den Durchschnitt der Teilnehmer nicht direkt auf den Durchschnitt aller Schweizer Unternehmen aus dem zweiten und dritten Sektor geschlossen werden darf.
- Um trotzdem Schätzungen für alle Unternehmen in der Schweiz möglich zu machen, müssen die Daten gewichtet werden.
- Eine Gewichtung bedeutet, dass **alle Daten mit dem Gewichtungsfaktor w multipliziert** werden. Dieser errechnet sich folgendermassen:

$$w = \frac{n_{Ri}/N_R}{n_{Si}/N_S}$$

n_{Ri}= Anzahl Firmen der Kategorie i in der Realität
N_R= Anzahl Firmen in der Realität
n_{Si}= Anzahl Firmen der Kategorie i in der Stichprobe
N_S= Anzahl Firmen in der Stichprobe

- Insgesamt sind 60 Kategorien zu unterscheiden (5 Grössenklassen und 12 verschiedene Branchen). Für jede dieser Kategorien kann der Gewichtungsfaktor w ausgerechnet werden, indem ihr prozentualer Anteil in der Realität mit ihrem prozentualen Anteil in der Stichprobe dividiert wird.

Branche	Total (Realität)	Total (Umfrage)	Gewichtung	0-4 (R)	0-4 (U)	Gew.	5-9 (R)	5-9 (U)	Gew.
Industrie	12.82	14.64	0.88	8.17	1.43	5.72	1.86	0.71	2.61
Bau	10.91	16.43	0.66	7.11	2.50	2.85	1.88	3.39	0.55
Handel	22.60	10.54	2.14	17.36	3.21	5.41	3.08	1.07	2.88
Gastgewerbe	7.91	3.39	2.33	5.02	0.36	13.96	1.74	0.36	4.85
Verkehr u. Kommunikation	3.50	6.61	0.53	2.53	1.61	1.57	0.43	0.54	0.79
Finanzwesen	1.71	3.75	0.46	1.07	0.89	1.20	0.25	0.00	
Unternehmensbez. DL	19.39	9.46	2.05	16.39	3.21	5.11	1.78	1.25	1.43
Informatik DL	3.52	6.61	0.53	2.90	3.04	0.95	0.30	0.54	0.56
Öffentliche Verwaltung	0.74	7.50	0.10	0.29	0.89	0.32	0.11	0.89	0.13
Unterreichtswesen	2.21	2.50	0.89	1.28	1.07	1.20	0.25	0.00	
Gesundheitswesen	6.87	9.82	0.70	5.29	2.32	2.28	0.69	0.89	0.78
Andere DL	7.83	8.75	0.89	6.64	3.04	2.18	0.69	1.25	0.55
Total	100.00	100.00		74.06	23.57		13.08	10.89	

Branche	10-49 (R)	10-49 (U)	Gew.	50-249 (R)	50-249 (U)	Gew.	250+ (R)	250+ (U)	Gew.
Industrie	2.06	4.64	0.44	0.60	3.93	0.15	0.13	3.93	0.03
Bau	1.68	7.32	0.23	0.22	2.32	0.10	0.02	0.89	0.02
Handel	1.84	4.64	0.40	0.26	0.54	0.48	0.05	1.07	0.05
Gastgewerbe	1.03	2.14	0.48	0.10	0.36	0.28	0.01	0.18	0.05
Verkehr u. Kommunikation	0.43	2.68	0.16	0.09	0.89	0.10	0.02	0.89	0.02
Finanzwesen	0.30	0.54	0.55	0.06	0.18	0.34	0.03	2.14	0.02
Unternehmensbez. DL	1.05	2.32	0.45	0.14	1.79	0.08	0.02	0.89	0.02
Informatik DL	0.27	1.96	0.14	0.04	0.36	0.11	0.01	0.71	0.01
Öffentliche Verwaltung	0.21	1.79	0.12	0.09	1.79	0.05	0.03	2.14	0.01
Unterreichtswesen	0.49	1.07	0.46	0.16	0.18	0.91	0.02	0.18	0.14
Gesundheitswesen	0.59	2.86	0.20	0.25	1.96	0.13	0.06	1.79	0.03
Andere DL	0.42	2.86	0.15	0.06	0.89	0.07	0.01	0.71	0.01
Total	10.37	34.82		2.09	15.19		0.40	15.52	

Anhang 4: Gewichtungsverfahren zum Ausschluss des Einflusses der Branchenzugehörigkeit / der Unternehmensgrösse

- Bei einigen Analysen wird der Einfluss der Unternehmensgrösse oder der Branchenzugehörigkeit untersucht. Dabei ist es nötig, den jeweils anderen Einfluss auszuschliessen.
  Beispiel: Unter den befragten Firmen des Finanzwesens sind 57% Grossfirmen mit mehr als 250 Mitarbeitern. Im Vergleich zum Anteil der Grossfirmen in der gesamten Stichprobe (16%), sind diese Unternehmen in der Finanzbranche also klar übervertreten. Wenn nun eine Analyse ergibt, dass die Firmen der Finanzbranche viel in die Informatiksicherheit investieren, dann könnte dies auch nur eine Folge der überproportionalen Vertretung der Grossfirmen in dieser Branche sein.
- Deshalb muss der Gewichtungsfaktor w_2 angewendet werden, der die Daten so bewertet, dass in allen Branchen die Grössenklassen gleich gross sind und in allen Grössenklassen die Branchen gleich häufig vertreten sind. Die Formel für w_2 lautet:
-

$$w_2 = \frac{n_i / n_{Bi}}{n_{Gi} / N} = \frac{n_i \, N}{n_{Bi} \, n_{Gi}}$$

n_i = Anzahl Firmen in der Kategorie i.
n_{Bi} = Anzahl Firmen in der Branche der Kategorie i.
n_{Gi} = Anzahl Firmen in der Grössenklasse der Kategorie i.
N = Anzahl Firmen in der gesamten Stichprobe.

Berechnung von w_2 mit Hilfe der prozentualen Anteilen der Grössenklassen pro Branche:

Branche	0-4 (B)	0-4 (D)	Gew.	5-9 (B)	5-9 (D)	Gew.	10-49 (B)	10-49 (D)	Gew.	50-249 (B)	50-249 (D)	Gew.	250+ (B)	250+ (D)	Gew.
Industrie	9.76	23.57	2.41	4.88	10.89	2.23	31.71	34.82	1.10	26.83	15.19	0.57	26.83	15.52	0.58
Bau	15.22	23.57	1.55	20.65	10.89	0.53	44.57	34.82	0.78	14.13	15.19	1.08	5.43	15.52	2.86
Handel	30.51	23.57	0.77	10.17	10.89	1.07	44.07	34.82	0.79	5.08	15.19	2.99	10.17	15.52	1.53
Gastgewerbe	10.53	23.57	2.24	10.53	10.89	1.03	63.16	34.82	0.55	10.53	15.19	1.44	5.26	15.52	2.95
Verkehr u. Kommunikation	24.32	23.57	0.97	8.11	10.89	1.34	40.54	34.82	0.86	13.51	15.19	1.12	13.51	15.52	1.15
Finanzwesen	23.81	23.57	0.99		10.89		14.29	34.82	2.44	4.76	15.19	3.19	57.14	15.52	0.27
Unternehmensbez. DL	33.96	23.57	0.69	13.21	10.89	0.82	24.53	34.82	1.42	18.87	15.19	0.80	9.43	15.52	1.65
Informatik DL	45.95	23.57	0.51	8.11	10.89	1.34	29.73	34.82	1.17	5.41	15.19	2.81	10.81	15.52	1.44
Öffentliche Verwaltung	11.90	23.57	1.98	11.90	10.89	0.92	23.81	34.82	1.46	23.81	15.19	0.64	28.57	15.52	0.54
Unterreichtswesen	42.86	23.57	0.55		10.89		42.86	34.82	0.81	7.14	15.19	2.13	7.14	15.52	2.17
Gesundheitswesen	23.64	23.57	1.00	9.09	10.89	1.20	29.09	34.82	1.20	20.00	15.19	0.76	18.18	15.52	0.85
Andere DL	34.69	23.57	0.68	14.29	10.89	0.76	32.65	34.82	1.07	10.20	15.19	1.49	8.16	15.52	1.90

(B): Prozentualer Anteil in der jeweiligen Branche
(D): Durchschnittlicher prozentualer Anteil

Anhang 5: Fragebogen

- Die Befragung wurde online durchgeführt. Die Befragten erhielten ein Einladungsschreiben (brieflich oder per E-Mail), welches ein Passwort enthielt.
  Damit konnten sie sich auf der Seite www.unipark.de/informatiksicherheit einloggen.

- Die Umfrage dauerte vom 15.03.06 bis am 13.04.06.

Anfang

Herzlich Willkommen zur Online-Umfrage

"Informatiksicherheit in der Schweiz"

Durchgeführt wird diese Umfrage von der Forschunsstelle für Sicherheitspolitik der Eidgenössisch Technischen Hochschule Zürich (ETH).

Informationen zum Ausfüllen des Fragebogens:
Der Fragebogen richtet sich an Unternehmen und Behörden.
Alle Teilnehmenden werden in den Fragen vereinfachend mit Firma oder Unternehmen angesprochen.
Alle Angaben werden streng vertraulich und anonymisiert behandelt.
Für Rückfragen wenden Sie sich bitte an:
suter@sipo.gess.ethz.ch
Bitte füllen Sie den Fragebogen bis am 29.02.06 aus.

In welchem Bereich ist Ihr Unternehmen tätig (Hauptaktivität)?
Bitte nur einen Bereich auswählen.

- ○ Industrie, Warenherstellung
- ○ Baugewerbe
- ○ Handel (Lebensmittel und Gebrauchsgegenstände)
- ○ Gastgewerbe
- ○ Verkehr, Transport und Nachrichtenübermittlung
- ○ Kredit- und Versicherungsgewerbe
- ○ Immobilien
- ○ Informatikdienstleistungen
- ○ Andere Dienstleistungen für Unternehmen
- ○ Unterrichtswesen
- ○ Gesundheits- und Sozialwesen
- ○ Öffentliche Verwaltung
- ○ Anderes [ ]

Wie gross ist die Anzahl der Beschäftigten in Ihrer Firma?
Inkl. Lehrlinge; Teilzeitbeschäftigte bitte auf Vollzeitstellen umrechnen; falls vorhanden, auch Mitarbeiter im Ausland berücksichtigen.

- ○ 0-4
- ○ 5-9
- ○ 10-49
- ○ 50-249
- ○ mehr als 250

Wie hoch war der Umsatz, den Ihr Unternehmen im Jahr 2005 erzielt hat?
Angaben bitte in Schweizer Franken.

- ○ weniger als 1 Mio
- ○ 1-4.9 Mio
- ○ 5-9.9 Mio
- ○ 10-99 Mio
- ○ mehr als 100 Mio
- ○ Weiss ich nicht

Wie hoch ist der Anteil der Mitarbeitenden in Ihrer Firma, welche im Rahmen ihrer Arbeit folgende Hilfsmittel benutzen:

	0%	1-20%	21-40%	41-60%	61-80%	81-100%	Weiss nicht
Personal Computer (PC)	○	○	○	○	○	○	○
Laptop	○	○	○	○	○	○	○
Digitale Assistenten (Organizer, PDA)	○	○	○	○	○	○	○
Mobiltelefone	○	○	○	○	○	○	○
E-mails	○	○	○	○	○	○	○
Internet	○	○	○	○	○	○	○

Dürfen Ihre Mitarbeiter von zu Hause aus auf Ihr Firmennetzwerk zugreifen?

- ○ Ja
- ○ Ja, aber nur unter Auflagen
- ○ Nein
- ○ Weiss nicht

Welche Verbindung zum Internet benutzt Ihr Unternehmen?
Es sind mehrere Antworten möglich.

- ☐ Modem
- ☐ ISDN
- ☐ DSL (xDSL, ADSL, SDSL etc.) < 2Mb/sec
- ☐ Kabel-Modem oder andere Breitband-Verbindungen
- ☐ Anderes

Benutzt Ihre Firma Wireless-Netzwerke?

- ○ Ja
- ○ Nein
- ○ Weiss nicht

Ist Ihre Firma mit einer Homepage im Internet präsent?

- ○ Ja
- ○ Nein
- ○ Weiss nicht

Welche Angebote beinhaltet die Homepage
Mehrere Antworten möglich.

- ☐ Informationen über Ihre Firma (Adressen, Firmenzweck, etc.)
- ☐ Informationen zu Ihren Produkten (Werbung)
- ☐ Produkteverkauf ohne Online-Zahlungsabwicklung
- ☐ Produkteverkauf mit Online-Zahlungsabwicklung
- ☐ Anderes

Nutzt Ihre Firma folgende Möglichkeiten des Internets?

	Ja	Nein	Weiss nicht
Suche von Informationen	○	○	○
Aus- und Weiterbildung	○	○	○
Diskussionsforen	○	○	○
Einkauf von Produkten und Dienstleistungen	○	○	○

Beurteilen Sie bitte die Wichtigkeit der Informatikinfrastruktur für Ihr Unternehmen.

wenig wichtig ○ ○ ○ ○ ○ sehr wichtig

Wie hat sich der Anteil der Investitionen in die Informatikinfrastruktur in den letzten fünf Jahren entwickelt?

abgenommen	blieb stabil	zugenommen	Weiss nicht
○	○	○	○

Haben Sie im Verlauf des Jahres 2005 einen der folgenden Angriffe auf die Informatiksicherhei Ihrer Firma festgestellt?

- ☐ Viren, Würmer, Trojaner
- ☐ Spyware
- ☐ Angriff auf die Verfügbarkeit (Denial of Service, DoS)
- ☐ Eindringen in das System (Hacking)
- ☐ Datendiebstahl
- ☐ Diebstahl von Laptops oder anderem Informatikmaterial
- ☐ Missbrauch der Wirelessnetze
- ☐ Verunstaltung der Homepage
- ☐ Anderes
- ☐ Keinen Angriff festgestellt

Woher kamen diese Angriffe?

- ○ Die Angriffe kamen von aussen
- ○ Die Angriffe hatten ihren Urspung bei einem der Mitarbeiter
- ○ Es gab sowohl Angriffe von aussen wie auch von innen

Wie viele Personen umfasst das Team, welches sich in Ihrem Unternehmen um die Informatiksicherheit kümmert?

Teilzeitbeschäftigte bitte auf Vollzeitstellen umrechnen.

- ○ keine
- ○ 0-1
- ○ 2-5
- ○ 6-10
- ○ mehr als 10

Welche Ausbildung hat der Leiter dieses Teams?

- ○ Informatiker mit Hochschul- oder Fachhochschulabschluss
- ○ Abgeschlossene Informatiklehre
- ○ Eidgenössischer Fachausweis für Informatik
- ○ nebenberufliche Weiterbildungen
- ○ Andere Ausbildung

Wie viel wurde 2005 für die Informatiksicherheit ausgegeben?

Angaben in Schweizer Franken. Personal und Strukturkosten berücksichtigen.

- ○ 0-5'000
- ○ 5'001-20'000
- ○ 20'001-100'000
- ○ mehr als 100'000
- ○ Weiss ich nicht

Wird Ihre Firma 2006 voraussichtlich mehr oder weniger für den Bereich der Informatiksicherheit aufwenden?

- ○ Mehr
- ○ Weniger
- ○ Gleichviel
- ○ Weiss ich nicht

Welcher Prozentsatz der Mittel wird im Bereich der Informatiksicherheit an andere Firmen delegiert?

0%	1-20%	21-40%	41-60%	61-80%	81-100%	Weiss ich nicht
○	○	○	○	○	○	○

Wie sind Sie mit den folgenden Aussagen einverstanden: "Im Bereich der Informatiksicherheit investiert mein Unternehmen genügend Mittel...

	Trifft zu	Trifft eher zu	Weder noch	Trifft eher nicht zu	Trifft nicht zu	Weiss ich nicht
...in technische Schutzmechanismen."	○	○	○	○	○	○
...in die Weiterbildung der Verantwortlichen für die Informatik."	○	○	○	○	○	○
...in die Weiterbildung aller Mitarbeitenden bezüglich Informatiksicherheit."	○	○	○	○	○	○

Welche Schutzmechanismen setzen Sie ein, um die Sicherheit Ihrer Informatik-Systeme zu gewährleisten?

Mehrere Antworten möglich.

- ☐ Antiviren-Programme
- ☐ Firewall
- ☐ Verschlüsselung
- ☐ Anti-Spyware Programme
- ☐ Intrusion Detection
- ☐ Mitarbeiterschulung im Bereich Informatiksicherheit
- ☐ Biometrie
- ☐ Andere
- ☐ Keine

Führen Sie regelmässige Analysen der Informatiksicherheit durch?

- ○ Ja, firmenintern
- ○ Ja, durch eine externe Firma
- ○ Noch nicht, ist aber geplant
- ○ Nein
- ○ Weiss ich nicht

Welche der folgenden Konzepte setzen Sie in Ihrer Firma ein?
Mehrere Antworten möglich.

- ☐ Backup-Konzept
- ☐ Security Policy
- ☐ Update-Management (Vulnerability-Management)
- ☐ Vorfallmanagement (Incident Response Konzept)
- ☐ Andere
- ☐ Keine

Besitzt Ihre Firma eine Versicherung, um mögliche Schäden an Ihrer Informatikinfrastruk (Hardware, Software, Datenverluste) abzudecken?

- ○ Ja
- ○ Nein
- ○ Weiss ich nicht

Welches sind die Gründe dafür, dass Ihre Firma keine Versicherung gegen solche Schäden hat?
Mehrere Antworten möglich.

- ☐ Lohnt sich nicht
- ☐ Nicht gewusst, dass solche Versicherungen möglich sind
- ☐ Keine Mittel dafür vorhanden
- ☐ Angebote der Versicherungen sind unbefriedigend
- ☐ Andere Gründe

Suchen Sie (oder Ihre Firma) externe Hilfe bei Problemen in der Informatiksicherheit?

- ○ Ja
- ○ Nein
- ○ Weiss ich nicht

Wo suchen Sie diese Hilfe?
Mehrere Atnworten möglich.

- ☐ Beim Software-Hersteller
- ☐ Beim Internet Service Provider (ISP)
- ☐ Bei Kollegen/Bekannten in anderen Firmen
- ☐ Im Internet (Web, Internetforen)
- ☐ Anderes

Hat Ihre Firma schon einmal wegen eines Vorfalles betreffend der Informatiksicherheit die Polizei eingeschaltet?

- ○ Ja
- ○ Nein
- ○ Weiss ich nicht

Welches waren die Gründe warum Sie die Vorfälle nicht der Poliziei gemeldet haben?
Mehrere Antworten möglich.

- ☐ Nicht gewusst, dass die Polizei Interesse an solchen Vorfällen hat
- ☐ Die Polizei stellt keine Möglichkeiten zur Meldung solcher Vorfälle zur Verfügung
- ☐ Eigene Massnahmen sind effizienter
- ☐ Angst vor negativen Konsequenzen für das Image der Firma
- ☐ Die Vorfälle schienen zu wenig gravierend

Würden Sie die Dienste eines Help Desks, welches Sie in Fragen der Informatiksicherheit berät, nutzen?

- ○ Ja, auf jeden Fall
- ○ Ja, aber nur wenn es unabhängig von den Software-Herstellern geführt würde
- ○ Nein

So ein Help Desk (Beratungsstelle) könnte verschiedene Dienstleistungen anbieten. Welche Dienstleistungen wären für Sie hilfreich?

	hilfreich	nicht hilfreich
Telefonische Beratung	○	○
Beratung über E-mail oder Tickets	○	○
Persönliche Beratung vor Ort	○	○

Der Austausch von Erfahrungen und Wissen mit Berufskollegen kann auch eine nützliche Informationsquelle sein. Bei welcher Art von Austausch würden Sie teilnehmen?

	sicher teilnehmen	wahrscheinlich teilnehmen	wahrscheinlich nicht teilnehmen	sicher nic teilnehme
Anonymer Austausch über Internetforen	○	○	○	○
Austausch über persönliche Kontakte	○	○	○	○
Austausch im Rahmen von Workshops, organisiert durch die entsprechenden Software-Hersteller	○	○	○	○
Austausch im Rahmen von Workshops, organisiert durch unabhängige Dritte	○	○	○	○

Weitere Dienstleistungen und Unterlagen könnten Ihnen zur Verbesserung der Informatiksicherheit dienen. Bitte bewerten Sie die Nützlichkeit der folgenden Angebote.
1 bedeutet "wenig hilfreich"; 5 bedeuted "sehr hilfreich".

	1	2	3	4	5
Leitfaden für das Vorgehen zur Einreichung einer Strafanzeige	○	○	○	○	○
Grundlagenmaterial für die Ausbildung, resp. Sensibilisierung der Mitarbeiter	○	○	○	○	○
Empfehlung von "Best Practices" (z.B. ISO 17799)	○	○	○	○	○
Hilfestellung zur Anwendung von "Best Practices" (z.B. ISO 17799)	○	○	○	○	○
Leitfaden für die Bewältigung der Vorfälle	○	○	○	○	○

Wer wäre Ihrer Meinung nach am besten geeignet, die vorher erwähnten Dienstleistungen z erbringen (Help Desk, Aufbau von Platformen zum Informationsaustausch, sowie Bereitstellung von Unterlagen)?

- ○ Software-Hersteller
- ○ Staatliche Organisationen
- ○ Branchenverbände
- ○ Speziell dafür geschaffene Organisationen
- ○ Beratungsfirmen

Wäre Ihre Firma bereit, sich finanziell an einer solchen Organisation zu beteiligen?

- ○ Ja, bis höchstens CHF 500.-
- ○ Ja, bis höchstens CHF 2'000.-
- ○ Nein
- ○ Weiss ich nicht

Kennen Sie die "Melde- und Analysestelle Informationssicherung" (MELANI) des Bundes?

- ○ Ja
- ○ Nein

Wie hilfreich ist MELANI für Ihr Unternehmen bei der Verbesserung der Informatiksicherheit?

wenig hilfreich ○ ○ ○ ○ ○ sehr hilfreich

Sind die folgenden Dienstleistungen von MELANI für Sie nützlich?

	Ja	Nein	Weiss nicht
Warnungen (Newsticker)	○	○	○
Meldeformular für Vorfälle	○	○	○
Allgemeine Hinweise über die Gefahren und Schutz der Informationssysteme	○	○	○
Demonstrations- und Ausbildungsprogramme für Ihre Mitarbeiter	○	○	○
Checklisten und Anleitungen für Ihre Mitarbeiter	○	○	○
Berichte über wichtigste Tendenzen und Entwicklungen	○	○	○

Autor

Manuel Suter, lic. phil. I, wissenschaftlicher Mitarbeiter des Center for Security Studies (CSS) der ETH Zürich

Projektverantwortung

Dr. Myriam Dunn, Leiterin des Forschungsbereichs Neue Risiken und Koordinatorin des Crisis and Risk Network (CRN) des Center for Security Studies (CSS) der ETH Zürich

Dr. Victor Mauer, stellvertretender Leiter des Center for Security Studies (CSS) der ETH Zürich