Vertrauen und Sicherheit im Netz

BITKOM

Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Lutz Neugebauer | Tel.: 030.27576-242 | l.neugebauer@bitkom.org
Susanne Dehmel | Tel.: 030.27576-223 | s.dehmel@bitkom.org
Katja Hampe | Tel.: 030.944002-45 | k.hampe@bitkom-research.de

Redaktion: Katja Hampe (Bitkom Research), Martin Puppe (BITKOM)

Gestaltung / Layout: Design Bureau kokliko / Astrid Scheibe (BITKOM)

Titelbild: Daniela Stanek (BITKOM)

Vertrauen und Sicherheit im Netz

BITKOM

Inhaltsverzeichnis

Abbildungsverzeichnisverzeichnis

Vorwort

Prof. Dieter Kempf
BITKOM-Präsident,
Vorsitzender des Vorstands DATEV eG

Sehr geehrte Damen und Herren,

drei von vier Deutschen sind online. Bis auf die Senioren ab 65 Jahren nutzen alle Altersgruppen mit breiter Mehrheit das Internet.

Für viele User sind »online« und »offline« längst verschmolzen. Die künstliche Trennung zwischen »virtuellem Leben« und dem so genannten realen Leben ist passé. Das Digitale ist Teil dessen, was wir das »wirkliche« Leben nennen. Ob Möbel bestellen, die nächste Reise buchen oder Rechnungen per E-Banking bezahlen: Viele Aufgaben des Alltags erledigen wir mittlerweile im Internet. Auch Unternehmen haben gelernt, ihre Arbeitsprozesse durch den Einsatz des Internets effektiver zu gestalten. Hinzu kommt, dass das Internet als Kommunikationstool für den Austausch mit Freunden, Kollegen oder Geschäftspartnern inzwischen unverzichtbar ist.

Vor diesem Hintergrund gewinnt die Vertrauensfrage stark an Bedeutung. Privatverbraucher wie Unternehmen sind gleichermaßen stark für das Thema Datenschutz sensibilisiert: 63 Prozent der privaten Nutzer sind der Meinung, dieser werde unterschätzt. Zudem erwarten 93 Prozent eine steigende Bedeutung des Themas; bei den Unternehmen sind es 86 Prozent.

Doch wie sind Datenschutz und IT-Sicherheit hierzulande in Unternehmen organisiert? Wo bestehen Lücken? Welche Erfahrungen haben Privatnutzer und Unternehmen bereits gemacht und welche Erwartungshaltung haben sie gegenüber den Behörden? Antworten auf diese Fragen liefert die vorliegende Studie auf Basis zweier repräsentativer Befragungen von Unternehmen und Privatpersonen.

Der vorliegende Bericht will einerseits über die wichtigsten Ergebnisse der Studien informieren und andererseits den Lesern Tipps für Verbraucher und Unternehmen liefern. Diese finden Sie im letzten Teil der Broschüre.

Ich wünsche Ihnen eine informative Lektüre.

Mit besten Grüßen

Studienergebnisse im Überblick

Trend zur Online-Speicherung von privaten Daten

- 82 Prozent der privaten Internetnutzer legen Daten und Inhalte im Internet ab. 7 von 10 Usern speichern Daten in sozialen Netzwerken. Foto- und Videoplattformen werden von 21 Prozent der Privatnutzer zur Datenablage genutzt.

- Das Hauptmotiv der Nutzer für die Online-Speicherung von Daten ist, diese mit anderen Menschen teilen und austauschen zu wollen (71%).

- Den Verzicht auf die Online-Speicherung begründen Nutzer am häufigsten mit der komplizierten Technik (37 Prozent), gefolgt von der Angst vor Datenmissbrauch (26 Prozent), Zweifeln am Nutzen (26 Prozent) und der Angst vor Datensverlust (25 Prozent).

Sorge um Datenschutz und IT-Sicherheit treibt Mehrheit von Privatnutzern und Unternehmen

- 57 Prozent aller Unternehmen betrachten Angriffe auf ihre IT-Systeme als reale Gefahr.

- Bei den privaten Anwendern fühlen sich drei Viertel im Web bedroht. Vor allem fürchten sie eine Infizierung ihres Rechners mit Schadprogrammen (62 Prozent) oder das Ausspähen und den Missbrauch persönlicher Daten (45 Prozent). Die Befürchtungen korrespondieren mit den Erfahrungen der Privatnutzer mit Internetkriminalität.

Anwenderfirmen mit deutlichen Defiziten in puncto Organisation von Datenschutz und IT-Sicherheit

- Obwohl bereits 39 Prozent der Unternehmen konkrete Angriffe auf die IT erlebt haben und 33 Prozent Erfahrungen mit Datenverlusten gemacht haben, sind Notfallpläne für derartige Vorfälle keine Selbstverständlichkeit. Besonders bei den Anwenderfirmen, d.h. Unternehmen, die nicht selbst aus der IT- und Kommunikationsbranche kommen, haben nur 46 Prozent einen Notfallplan für Datenverluste.

- Darüber investieren ITK-Firmen tendenziell mehr für Datenschutz und IT-Sicherheit als Anwenderunternehmen, haben häufiger einen Datenschutzbeauftragten (75 vs. 61 Prozent) und verfügen eher über Sicherheitsstandards für mobile Endgeräte (75 vs. 56 Prozent).

Unternehmen unterschätzen die hohe Bedeutung von Datenschutz und -sicherheit für den Vertrauensaufbau im Web aus Sicht der Verbraucher

- Insgesamt messen sowohl Privatnutzer als auch Unternehmen dem Kundenvertrauen als Erfolgsfaktor für Geschäftsmodelle im Web eine hohe Bedeutung bei.

- Vor allem die nachvollziehbare Datensicherheit (78 Prozent), verständliche und faire Geschäftsbedingungen (76 Prozent) und nachvollziehbarer Datenschutz (75 Prozent) stärken aus Verbrauchersicht das Kundenvertrauen.

- Bei den Unternehmen spielen diese Kriterien eine nachrangige Rolle. Verbindliche Kommunikation (92 Prozent), kompetentes Auftreten der Mitarbeiter (92 Prozent), und ein persönlicher Ansprechpartner (91 Prozent) stehen hier an der Spitze.

Hohe Kooperationsbereitschaft der Unternehmen | Verbraucher: Teilweise Befürwortung von staatlichen Eingriffen

- Die Mehrheit der befragten Unternehmen (74 Prozent) zeigt grundsätzlich eine hohe Bereitschaft zur Zusammenarbeit mit Behörden bei IT-Sicherheitsvorfällen.

- Staatliche Eingriffe im Web stoßen bei Privatnutzern aufs Ressentiments: die Speicherung von Internetverbindungsdaten (57 Prozent) und die Überwachung von Nachrichten und Gesprächen (64 Prozent) für polizeiliche Zwecke lehnt die Mehrheit ab.

- Beim Schutz von Hackerangriffen (89 Prozent), der vorbeugenden Gefahrenabwehr, z. B. bei Terrorgefahr (79 Prozent), und dem Verbraucherschutz (77 Prozent) hingegen wünschen Privatnutzer einen stärken staatlichen Eingriff.

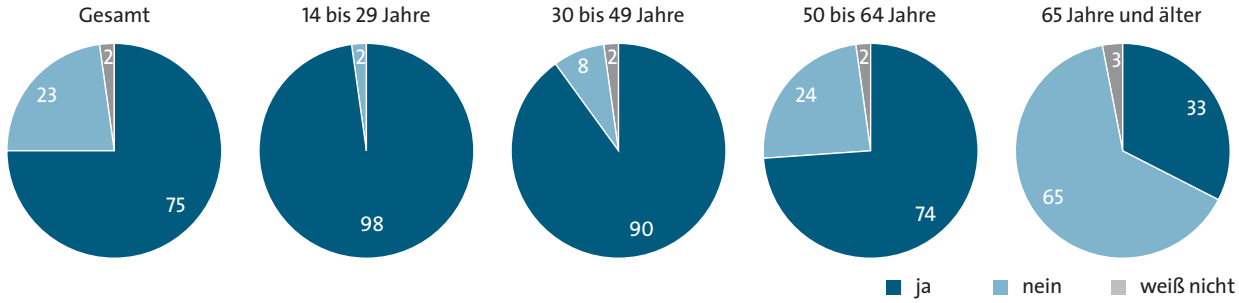
1 Privater Umgang mit Daten im Internet

1.1 Generelle Internet-Nutzung

Insgesamt nutzen in Deutschland 75 Prozent der Privatpersonen ab 14 Jahren das Internet. Je jünger die Zielpersonen, umso höher ist der Anteil der Privatanwender. In der Altersgruppe von 14-29 Jahren sind mit 98 Prozent nahezu alle online; bei den 30-49jährigen sind es 90 Prozent.

Im Vergleich zu einer BITKOM-Untersuchung aus dem Vorjahr hat der Anteil der Privatanwender zwischen 50 und 64 Jahren deutlich zugenommen. 74 Prozent dieser Altersgruppe sind im Web. 2011 waren es erst 68 Prozent[1]. Erst bei den Personen ab 65 ist die Internet-Nutzung mit 33 Prozent deutlich schwächer ausgeprägt.

Internetnutzung nach Alter



Basis: 1.008 private Internetnutzer — Angaben in Prozent

Frage: »Nutzen Sie privat und/oder beruflich, wenn auch nur gelegentlich das Internet?«

Abbildung 1: Internetnutzung nach Alter

1.2 Speicherung privater Daten im Internet

Der eigene Computer bleibt das meist verbreitete Speichermedium (85 Prozent der Internetnutzer). Bei den physischen Datenträgern folgen CDs/DVDs/Blue-Rays mit 43 Prozent, USB-Sticks mit 27 Prozent und externe Festplatten mit 26 Prozent.

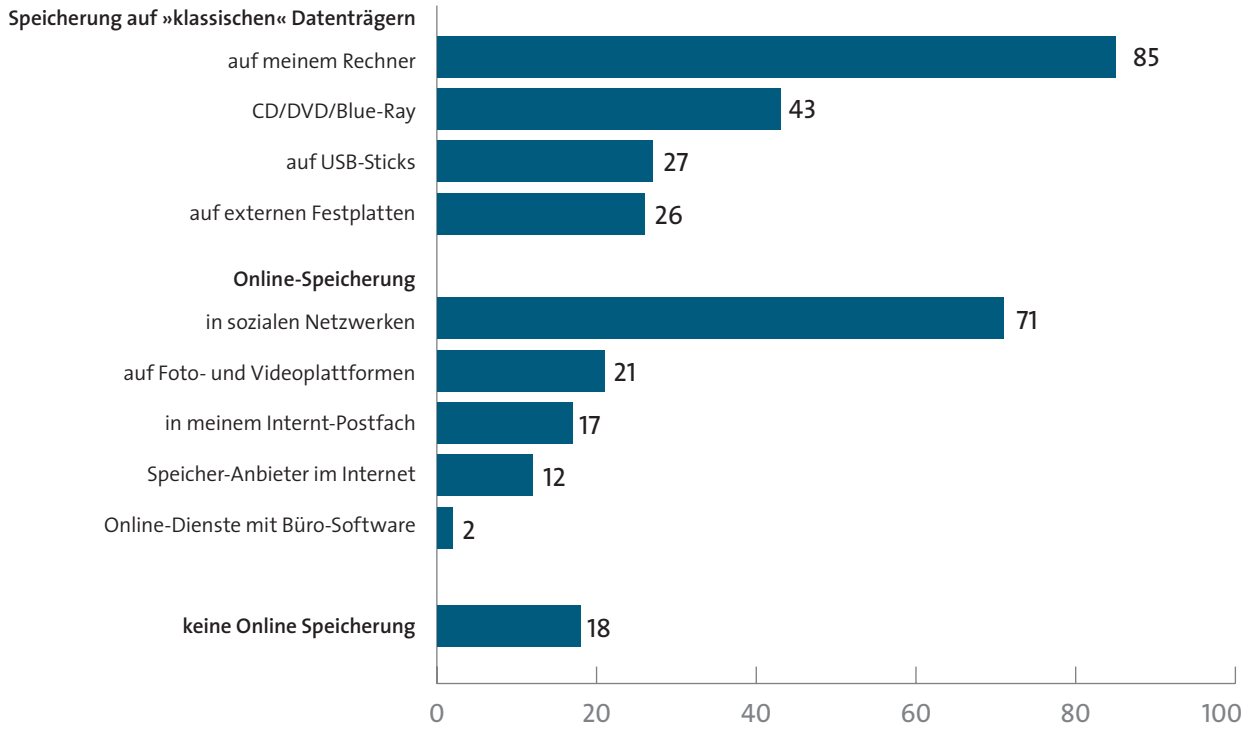
Erstaunlich ist, dass insgesamt bereits 7 von 10 Usern private Daten in sozialen Netzwerken speichern. Innerhalb der Gruppe der 14-29-Jährigen sind es sogar fast 90 Prozent. Foto- und Videoplattformen, wie z. B. Flickr, werden insgesamt von 21 Prozent genutzt. Das Internet-Postfach verwenden 17 Prozent als Speicherort. Speziellen Speicheranbietern im Internet (z. B. Telekom Cloud) vertrauen erst 12 Prozent der User ihre Daten an.

Kaum genutzt werden Online-Dienste mit Büro-Software, z. B. Google Docs (2 Prozent).

Hinter der Nutzung des Internets als Speicherort steht dabei weniger die die Absicht, persönliche Daten zu sichern. Vielmehr ist Kommunikation das Hauptmotiv: 71 Prozent wollen ihre Daten und Inhalte mit vielen Menschen auf einer Internet-Plattform teilen. 51 Prozent möchten Freunde, Bekannte oder Verwandte an ihren Daten teilhaben lassen. Gut jeder fünfte Privatnutzer will Daten mit Kollegen oder Geschäftspartnern austauschen. Als weitere Gründe folgen die Sicherung von Daten (22 Prozent) sowie die eigene Online-Publikation (20 Prozent).

[1] BITKOM (2011): Netzgesellschaft. Eine repräsentative Untersuchung zur Mediennutzung und dem Informationsverhalten der Gesellschaft in Deutschland, S. 9

Nutzung von klassischen Speichermedien und Online-Speicherung | Privatnutzer



Basis: 1.008 private Internetnutzer

Angaben in Prozent

Frage: »Es gibt im Internet und außerhalb viele Orte, an denen man private Daten und Dateien ablegen oder speichern kann. Wo legen Sie z.B. Dokumente, Fotos, Videos oder andere Daten ab bzw. speichern diese?« (Mehrfachnennung möglich)

Abbildung 2: Nutzung von klassischen Speichermedien und von Onlinespeicherung | Privatnutzer

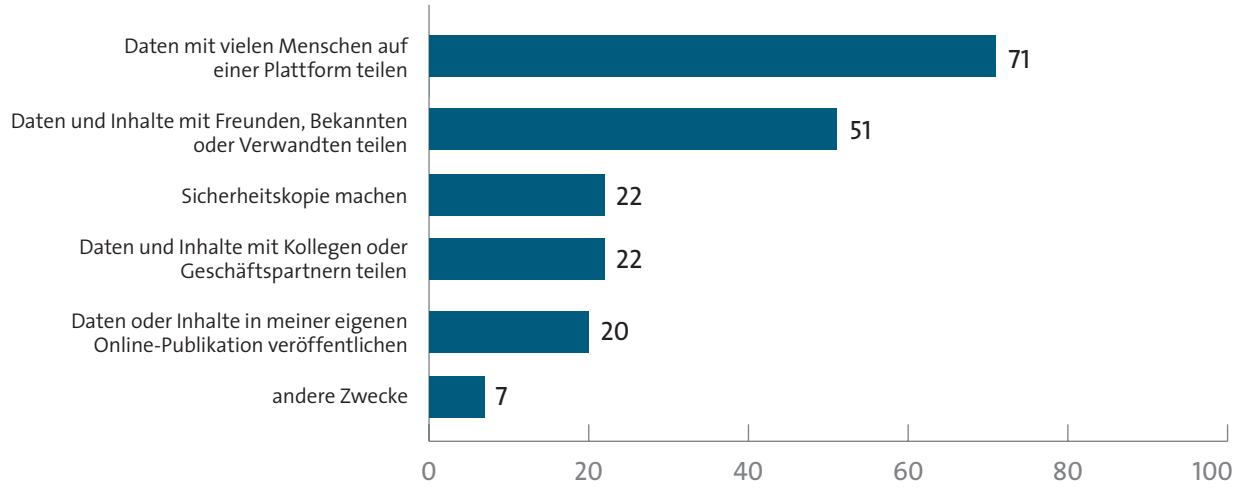
Die Ergebnisse zeigen damit klar den sozialen Charakter des Internets und machen die Herausforderung für den Datenschutz deutlich: Wo viele Menschen von sich aus Persönliches mitteilen, muss besonders auf Sicherheit und Vertrauen geachtet werden.

Immerhin legen 18 Prozent der privaten Nutzer gar keine Daten ab. Hier zeigt sich ein deutlicher Unterschied zwischen den Altersgruppen: Je älter die Nutzer, desto eher lehnen sie die Online-Speicherung ab. So sind es bei den 14-29-Jährigen gerade einmal 6 Prozent bei den 50-64-Jährigen hingegen schon 24 Prozent.

Alle Personen, die keine Daten und Inhalte im Internet speichern, wurden gefragt, welche Gründe sie für ihre Zurückhaltung haben, also warum sie keine Online-Dienste zum Speichern oder Veröffentlichen nutzen. 37 Prozent geben an, dass ihnen die Speicherung im Netz zu kompliziert ist. Je ein Viertel der Nichtnutzer hat Angst vor Datenmissbrauch oder Datenverlust, sieht keinen Nutzen oder kennt die Angebote nicht.

Hier wird Potenzial verschenkt, aus der Anwender- wie Anbieterperspektive. Unternehmen müssen noch vieles erklären.

Gründe für die Online-Speicherung von privaten Daten und Inhalten



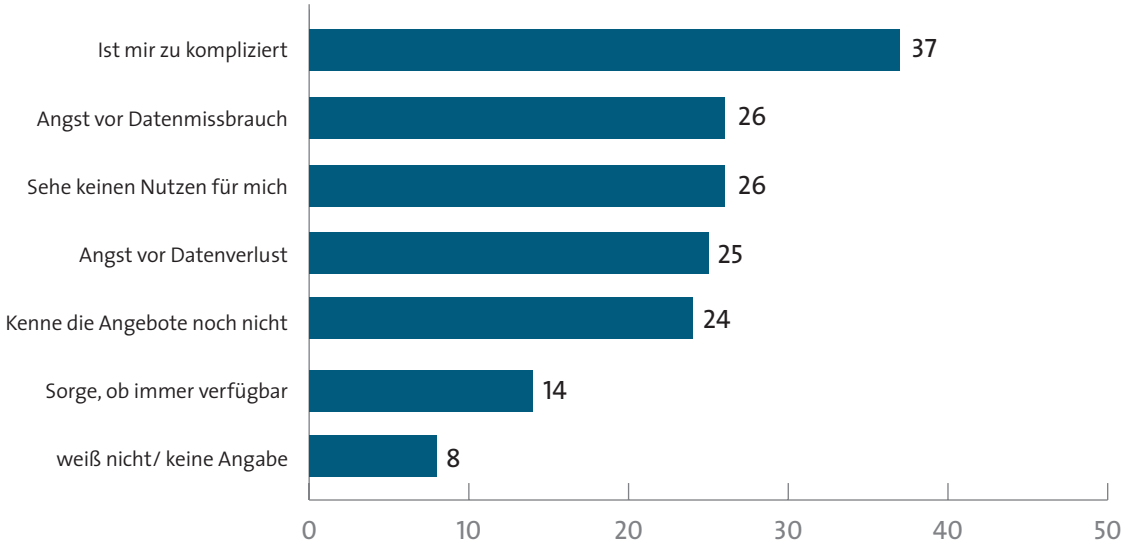
Basis: 1.008 private Internetnutzer

Angaben in Prozent

Frage: »Es gibt viele Möglichkeiten, im Internet Daten und Inhalte abzulegen, zu speichern oder zu veröffentlichen. Zu welchen Zwecken legen Sie Daten im Internet ab?« (Mehrfachnennung möglich)

Abbildung 3: Gründe für die Online-Speicherung von privaten Daten und Inhalten | Privatanwender

Gründe für Nicht-Nutzung von Online-Speicherdiensten



Basis: 183 private Internetnutzer, die keine Daten im Internet ablegen

Angaben in Prozent

Frage: »Warum nutzen Sie keine Internet-Dienste, um im Web Daten abzulegen, zu speichern oder zu veröffentlichen?«

Abbildung 4: Gründe für Nicht-Nutzung von Online-Speicherdiensten | Privatanwender

2 Datenschutz und IT-Sicherheit: Bedrohungsszenarien und Erfahrungen

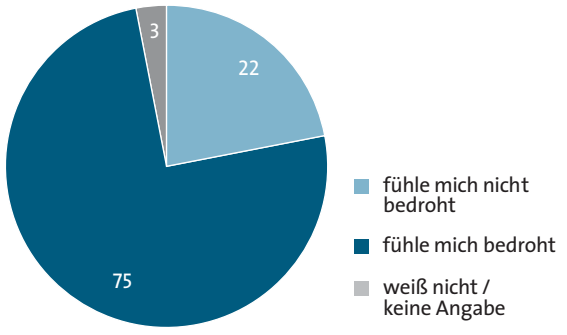
Unabhängig von der Nutzung von Speicherdiensten im Web treibt sowohl Verbraucher als auch Unternehmen die Sorge um die IT-Sicherheit.

2.1 Bedrohungsszenarien für Privatanwender und Unternehmen

Die meisten Unternehmen sorgen sich um ihre IT-Sicherheit. Angriffe auf ihre IT-Systeme sieht mehr als die Hälfte (57 Prozent) aller Unternehmen als reale Gefahr, quer durch alle Branchen und Unternehmensgrößen.

Bei den Anwendern ist die Sorge noch höher: Drei Viertel aller deutschen Privatanwender fühlen sich im Web bedroht. Die meisten Privatanwender (62 Prozent) fürchten eine Infizierung ihres Rechners mit Schadprogrammen. Vor Betrug beim Online-Einkauf oder einer Online-Auktion hat fast jeder dritte User Angst (31 Prozent). Das Ausspähen und der Missbrauch persönlicher Daten stellt für 45 Prozent eine gefühlte Bedrohung dar.

Gefühlte Bedrohung | Privatanwender

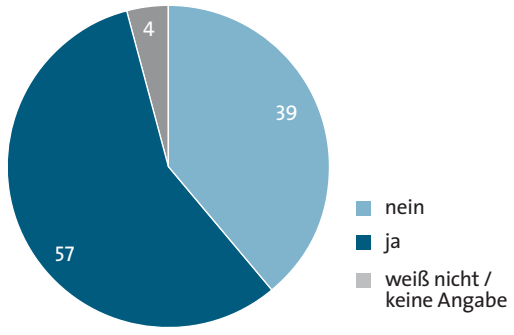


Basis: 1.008 private Internetnutzer — Angaben in Prozent

Frage: »Wodurch fühlen Sie sich im Internet bedroht?«

Abbildung 5: Gefühlte Bedrohung im Web | Privatanwender

Wahrnehmung von Angriffen auf IT-Systeme als reale Gefahr | Unternehmen

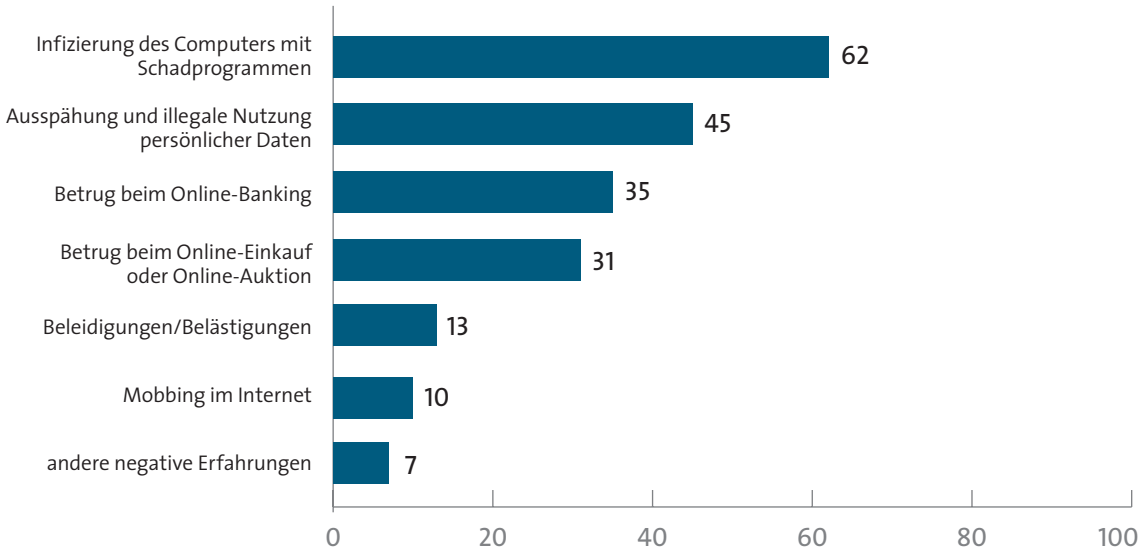


Basis: 810 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer — Angaben in Prozent

Frage: »Sehen Sie Angriffe auf Ihre IT-Systeme, etwa von Hackern, Konkurrenten, Kriminellen oder ausländischen Geheimdiensten, als reale Gefahr?«

Abbildung 6: Wahrnehmung von Angriffen auf IT-Systeme als reale Gefahr | Unternehmen

Wodurch sich Privatanwender im Web bedroht fühlen



Basis: 1.008 Internetnutzer

Angaben in Prozent

Frage: »Wodurch fühlen Sie sich im Internet bedroht?« (Mehrfachnennung möglich)

Abbildung 7: Wodurch sich Privatanwender im Web bedroht fühlen

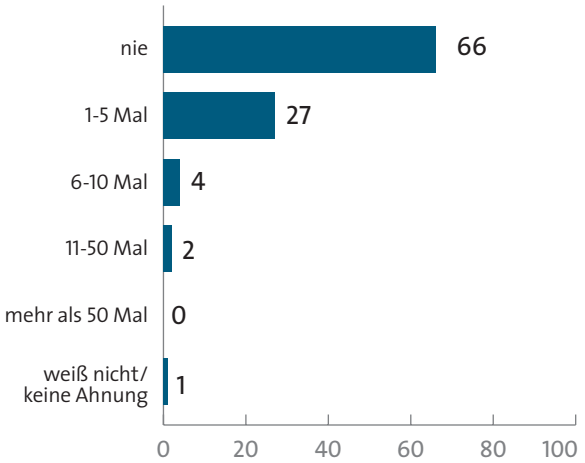
2.2 Erfahrungen der Privatanwender und Unternehmen

39 Prozent der Unternehmen haben bereits konkrete Angriffe auf die IT oder vergleichbare Sicherheitsvorfälle erlebt. Erfahrungen mit Datenverlusten oder anderen Datenschutzvorfällen haben 33 Prozent gemacht.

Bei den Nutzern hat jeder Zweite schlechte Erfahrungen gemacht. Bei rund 36 Prozent der Nutzer wurde der Rechner von Viren befallen. Jeder achte User (12 Prozent) ist beim Online-Shopping oder bei Auktionen von seinem Geschäftspartner betrogen worden.

Jeder Zehnte gab an, dass in seinem Namen unerwünschte Mails verschickt wurden. Der Missbrauch von Zugangsdaten ist ebenfalls ein Problem: 7 Prozent der Nutzer klagten, dass Unbekannte sich mit ihren Zugangsdaten in einen Internet-Shop oder Auktionshaus eingeloggt hatten. 6 Prozent der Nutzer von sozialen Netzwerken und Online-Foren sind ebenfalls betroffen.

Erfahrungen der Unternehmen mit Datenverlust

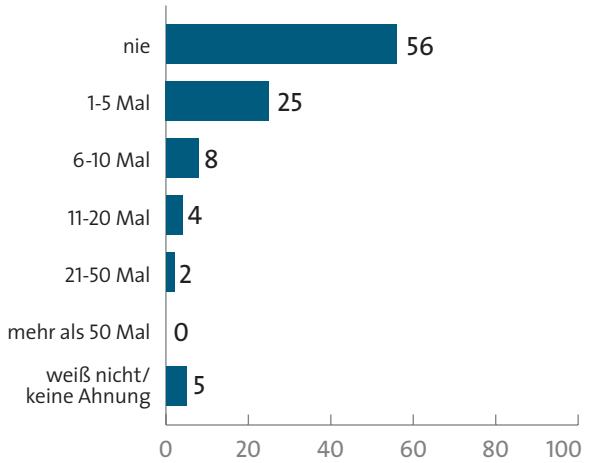


Basis: 810 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer — Angaben in Prozent

Frage: »Wie häufig gab es in Ihrem Unternehmen bisher Datenverluste oder andere Datenschutzvorfälle?«

Abbildung 8: Erfahrungen der Unternehmen mit Datenverlust

Erfahrungen der Unternehmen mit Angriffen auf IT-Systeme

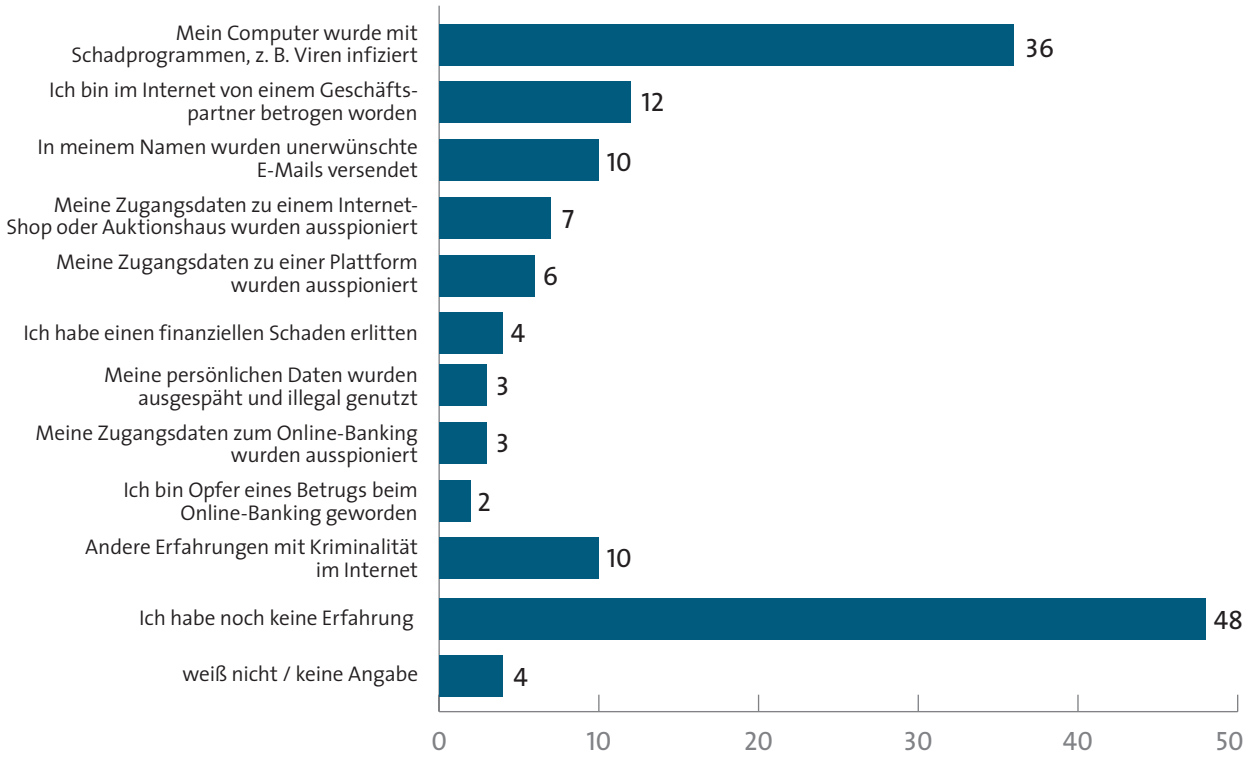


Basis: 810 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer — Angaben in Prozent

Frage: »Wie häufig gab es in Ihrem Unternehmen bisher Angriffe auf ihre IT-Systeme oder andere IT-Sicherheitsvorfälle?«

Abbildung 9: Erfahrungen der Unternehmen mit Angriffen auf IT-Systeme oder mit anderen Sicherheitsvorfällen

Erfahrungen der Privatanwender mit Internetkriminalität



Basis: 1.008 private Internetnutzer

Angaben in Prozent

Frage: »Welche der folgenden Erfahrungen mit kriminellen Vorfällen haben Sie persönlich bereits im Internet gemacht?« (Mehrfachnennung möglich)

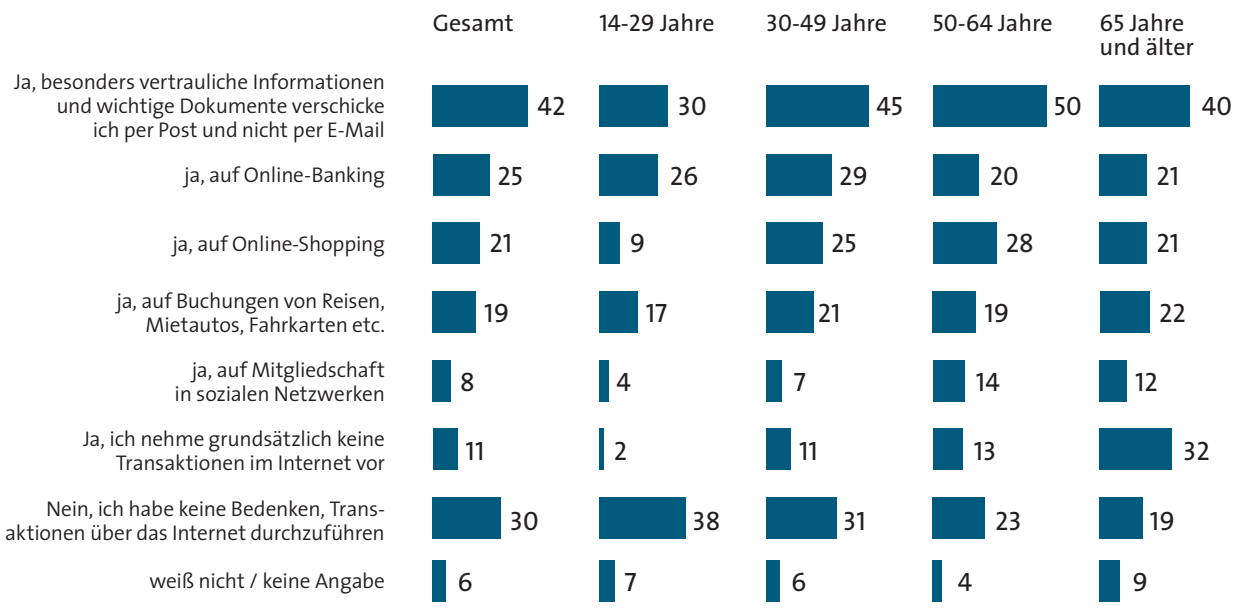
Abbildung 10: Erfahrungen der Privatanwender mit Internetkriminalität

2.3 Auswirkungen auf die Internetnutzung

Die Ergebnisse zeigen auch, dass das Vertrauen der Privatanwender in Online-Transaktionen wächst: Nur noch jeder neunte User (11 Prozent) verzichtet aus Sicherheitsgründen auf Online-Shopping, Internet-Banking und andere Geschäftstätigkeiten im Web. Hier zeigen sich altersbezogene Unterschiede, denn jüngere Zielgruppe geben deutlich seltener an, auf Online-Transaktionen zu verzichten. Zudem ist die Zurückhaltung insgesamt gesunken. Im vergangenen Jahr war noch jeder sechste entsprechend zurückhaltend[2] (16 Prozent). Nur noch jeder vierte User verzichtet aktuell aus Sicherheitsgründen auf Internet-Bankgeschäfte, gut jeder fünfte (21 Prozent) auf Online-Shopping. Besonders stark nahmen die Bedenken gegenüber Mitgliedschaften in sozialen Netzwerken ab. Im vergangenen Jahr blieb jeder achte Onliner den Netzwerken aus Sicherheitsgründen fern (13 Prozent), mittlerweile ist es noch jeder zwölfte (8 Prozent).

Auch bei den Unternehmen führen die Sorge um die Datensicherheit sowie negative Erfahrungen zur Einschränkung ihrer Online-Aktivitäten. Insgesamt verzichtet fast jede zweite Firma auf wichtige Internetanwendungen. Jedes vierte Unternehmen versendet vertrauliche Dokumente nicht per E-Mail (25 Prozent). Online-Überweisungen und Online-Shopping unterlassen 11 bzw. 12 Prozent der Firmen.

Verzicht auf Onlinetransaktionen aufgrund von Sicherheitsbedenken | Privatanwender



Basis: 1.008 private Internetnutzer

Angaben in Prozent

Frage: »Verzichten Sie aus Sicherheitsgründen bewusst auf eine der folgenden Aktivitäten im Internet?« (Mehrfachnennung möglich)

Abbildung 11: Verzicht auf Onlinetransaktionen aufgrund von Sicherheitsbedenken | Privatanwender

[2] BITKOM (2011): Datenschutz im Internet. Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht, S. 34

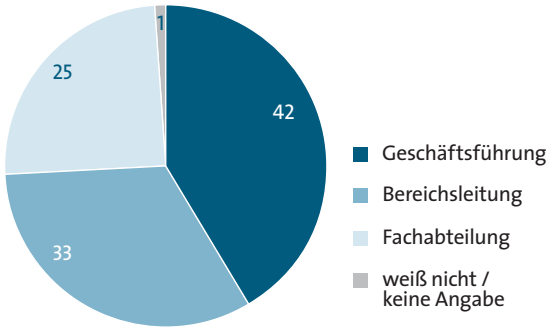
3 Organisation von Datenschutz in Unternehmen

Ein Schwerpunkt der Untersuchung lag darauf, wie Datenschutz und IT-Sicherheit in Unternehmen organisiert sind. Dazu wurden verschiedene Kriterien wie z. B. personelle Zuständigkeit, Höhe der finanziellen Aufwendungen und Vorhandensein spezifischer Sicherheitsstandards abgefragt. Die Ergebnisse zeigen insgesamt, dass Unternehmen der ITK-Branche in puncto Datenschutz und IT-Sicherheit besser aufgestellt sind als Anwenderfirmen.

3.1 Zuständigkeiten

Auf welcher Management-Ebene Datenschutz und IT-Sicherheit angesiedelt sind, ist unabhängig von der Zugehörigkeit zur ITK-Branche. Grundsätzlich gilt: Je größer das Unternehmen, desto eher liegt die Zuständigkeit bei der Bereichsleitung oder den zuständigen Fachbereichen.

Auf welcher Ebene ist Datenschutz angesiedelt | KMU

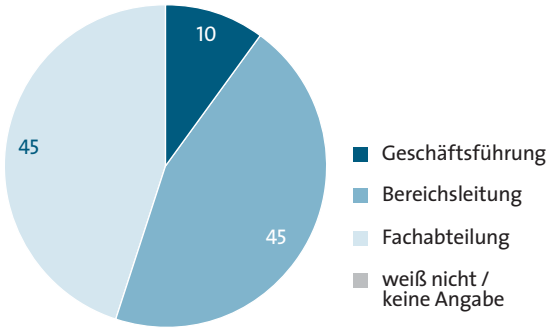


Basis: 658 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von kleinen und mittelständischen Unternehmen — Angaben in Prozent

Frage: »Auf welcher Management-Ebene ist das Thema Datenschutz bei Ihnen angesiedelt?«

Abbildung 12: Management-Ebene Datenschutz in KMU

Auf welcher Ebene ist Datenschutz angesiedelt | Großunternehmen

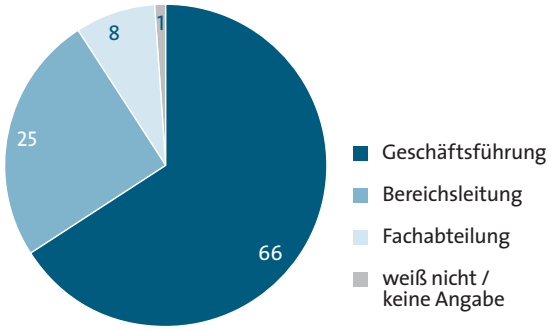


Basis: 152 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Großunternehmen — Angaben in Prozent

Frage: »Auf welcher Management-Ebene ist das Thema Datenschutz bei Ihnen angesiedelt?«

Abbildung 13: Management-Ebene Datenschutz in Großunternehmen

Auf welcher Ebene ist IT-Sicherheit angesiedelt | KMU

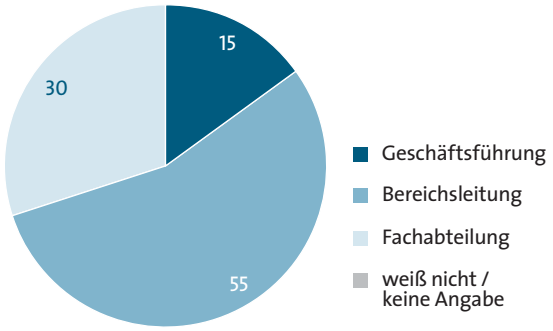


Basis: 658 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von kleinen und mittelständischen Unternehmen — Angaben in Prozent

Frage: »Auf welcher Management-Ebene ist das Thema IT-Sicherheit in Ihrem Unternehmen angesiedelt?«

Abbildung 14: Management-Ebene IT-Sicherheit in KMU

Auf welcher Ebene ist IT-Sicherheit angesiedelt | Großunternehmen



Basis: 152 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Großunternehmen — Angaben in Prozent

Frage: »Auf welcher Management-Ebene ist das Thema IT-Sicherheit in Ihrem Unternehmen angesiedelt?«

Abbildung 15: Management-Ebene IT-Sicherheit in Großunternehmen

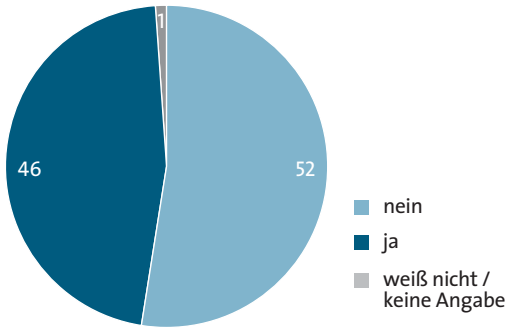
Datenschutzbeauftragter

Sechs von zehn Unternehmen haben einen Datenschutzbeauftragten. Meist sind es interne Mitarbeiter (49 Prozent). Weitere 13 Prozent beauftragen einen externen Mitarbeiter. Die restlichen Unternehmen haben keinen Datenschutzbeauftragten (38 Prozent). Der Mangel an Datenschutzbeauftragten ist bei den Anwenderfirmen deutlich größer als bei den ITK-Unternehmen (39 Prozent bzw. 25 Prozent).

3.2 Notfallpläne

Einen noch größeren Unterschied gibt es bei der Frage nach Notfallplänen für Datenverluste. Unter den Anwender-Unternehmen, d.h. Unternehmen, die nicht aus der IT- und Kommunikationsbranche kommen, hat etwa nur jedes zweite einen Notfallplan für Datenverluste. Hier besteht also ein deutlicher Nachholbedarf.

Notfallpläne für Datenverluste | Anwender-Unternehmen



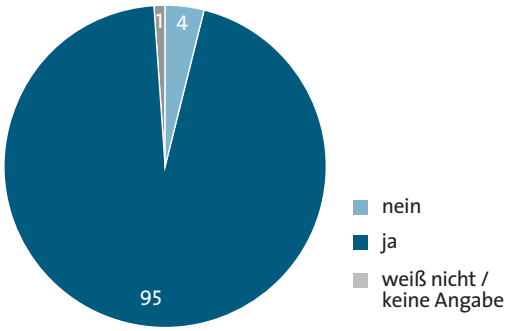
Basis: 506 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Anwender-Unternehmen

Angaben in Prozent

Frage: »Hat ihr Unternehmen einen Notfallplan für IT-Sicherheitsvorfälle?«

Abbildung 16: Notfallpläne für Datenverluste | Anwenderfirmen

Notfallpläne für Datenverluste | ITK-Firmen



Basis: 304 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von ITK-Firmen

Angaben in Prozent

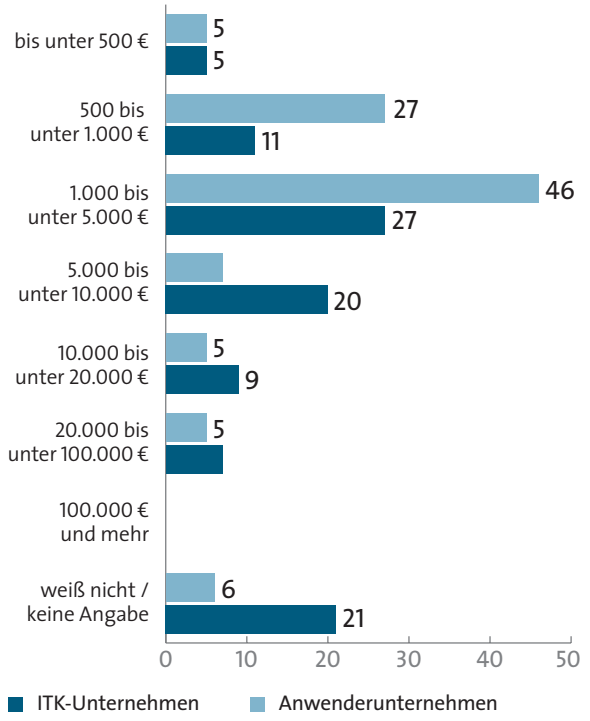
Frage: »Hat ihr Unternehmen einen Notfallplan für IT-Sicherheitsvorfälle?«

Abbildung 17: Notfallpläne für Datenverluste | ITK-Firmen

3.3 Jährliche Kosten für Datenschutz und IT-Sicherheit

Darüber hinaus zeigen die Ergebnisse, dass Firmen aus der ITK-Branche tendenziell mehr für Datenschutz und IT-Sicherheit investieren: Über 60 Prozent der ITK-Unternehmen geben jedes Jahr bis zu 10.000 Euro für Datenschutz und IT-Sicherheit aus. Fast jedem vierten IT-Unternehmen ist die IT-Sicherheit zwischen 5.000 und 20.000 Euro jährlich wert. Dagegen liegt bei dem überwiegenden Teil der Anwenderfirmen (78 Prozent bzw. 73 Prozent) das Jahresbudget für Datenschutz und IT-Sicherheit unter 5.000 Euro.

Kosten für Datenschutz



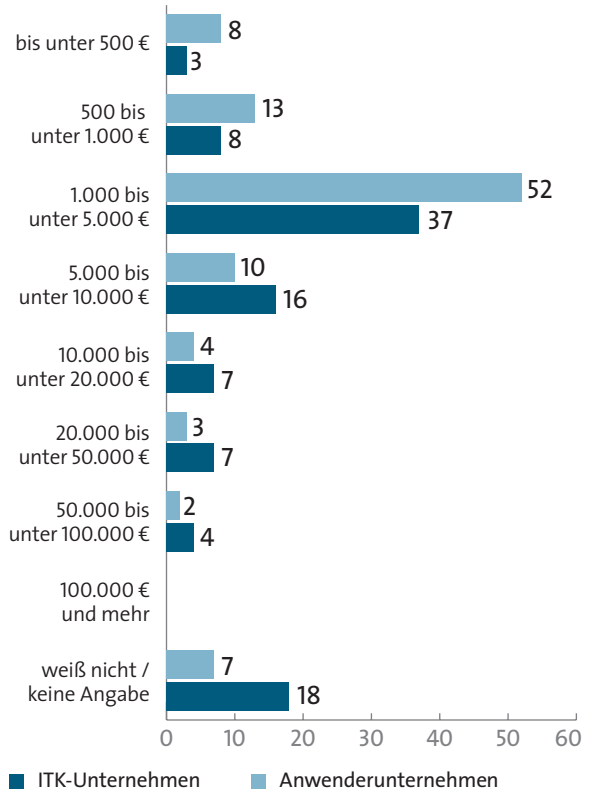
Basis: 810 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Anwender und ITK-Unternehmen

Angaben in Prozent

Frage: »Wie hoch ist Ihr jährlicher Kostenaufwand für Datenschutz ungefähr?«

Abbildung 18: Kosten für Datenschutz

Kosten für IT-Sicherheit



Basis: 810 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Anwender und ITK-Unternehmen

Angaben in Prozent

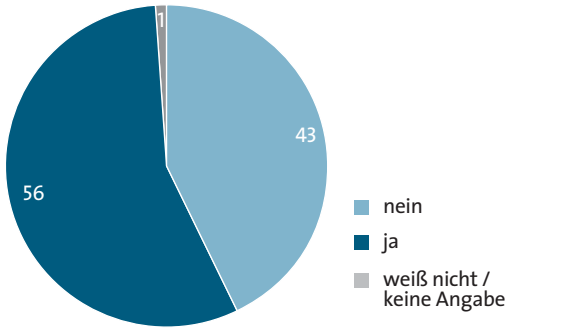
Frage: »Wie hoch ist der jährliche Kostenaufwand für IT-Sicherheit ungefähr?«

Abbildung 19: Kosten für IT-Sicherheit

3.4 Sicherheitsstandards für mobile Endgeräte

Auch wenn mobile Endgeräte inzwischen für viele Arbeitnehmer zum Arbeitsalltag gehören, sind Sicherheitsstandards für Handys, Tablets und Co. noch keine Selbstverständlichkeit. Von den Unternehmen, die ihren Mitarbeitern Dienste und Anwendungen auf mobilen Endgeräten zur Verfügung stellen, haben insgesamt nur 57 Prozent spezielle Sicherheitsstandards für diese. Erwartungsgemäß ist der Anteil bei den ITK-Firmen höher (75 Prozent) als bei den Anwender-Unternehmen (56 Prozent)

Sicherheits-Standards für mobile Geräte | Anwender-Unternehmen

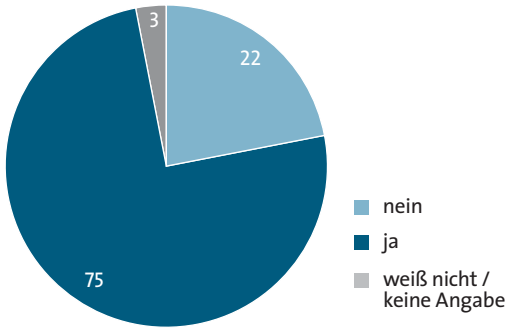


Basis: 348 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Anwender-Unternehmen, die ihren Mitarbeitern Dienste und Anwendungen auf mobilen Geräten zur Verfügung stellen — Angaben in Prozent

Frage: »Gibt es in Ihrem Unternehmen spezielle Sicherheits-Standards für mobile Endgeräte?«

Abbildung 20: Sicherheits-Standards für mobile Geräte | Anwender-Unternehmen

Sicherheits-Standards für mobile Geräte | ITK-Unternehmen



Basis: 234 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von ITK-Unternehmen, die ihren Mitarbeitern Dienste und Anwendungen auf mobilen Geräten zur Verfügung stellen — Angaben in Prozent

Frage: »Gibt es in Ihrem Unternehmen spezielle Sicherheits-Standards für mobile Endgeräte?«

Abbildung 21: Sicherheits-Standards für mobile Geräte | ITK-Unternehmen

3.5 Selbsteinschätzung

Insgesamt verdeutlichen die Ergebnisse, dass der betriebliche Datenschutz und die IT-Sicherheit in Unternehmen noch große Lücken aufweisen, die es zu schließen gilt. Dessen sind sich Unternehmen durchaus bewusst. Laut Selbsteinschätzung sieht jedes vierte Unternehmen in puncto Datenschutz noch Verbesserungsbedarf (26 Prozent). Beim Thema IT-Sicherheit ist es jedes dritte Unternehmen (33 Prozent). Gar keinen Nachholbedarf sehen 19 Prozent der befragten Firmen.

4 Vertrauen als Erfolgsfaktor für Geschäftsmodelle im Internet

4.1 Bedeutung von Vertrauen für den Geschäftserfolg im Web

69 Prozent der User tun sich online schwerer, die Vertrauenswürdigkeit von Personen und Unternehmen einzuschätzen, als bei Begegnungen von Angesicht zu Angesicht oder dem Besuch eines stationären Ladens. Vor diesem Hintergrund stellt sich die Frage, welche Bedeutung die Anwender dem Kundenvertrauen für den wirtschaftlichen Erfolg im Web beimessen. Danach gefragt, geben sowohl Verbraucher als auch Unternehmen am häufigsten an, dass dies vom Geschäftsmodell abhängt (45 Prozent bzw. 49 Prozent).

Vier von zehn Privatanwendern sehen im Kundenvertrauen einen Erfolgsfaktor für (39 Prozent). Bei den Unternehmen ist der Anteil mit 40 Prozent ähnlich hoch. Hier sind es jedoch vor allem die ITK-Firmen, die das Kundenvertrauen als unabdingbar für den wirtschaftlichen Erfolg einschätzen (53 Prozent).

4.2 Kriterien für Kundenvertrauen: Divergierende Verbraucher- und Unternehmensmeinungen

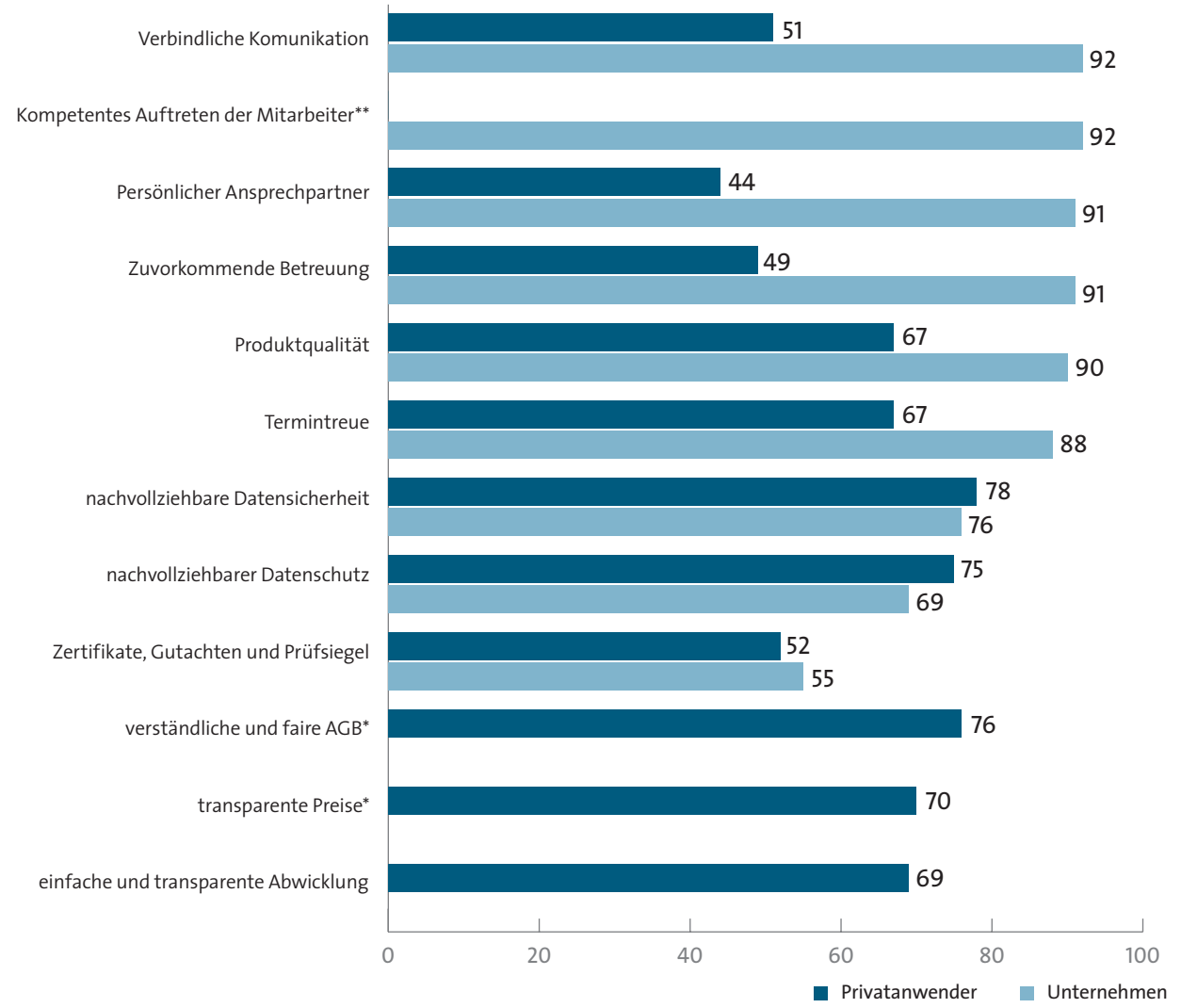
Doch wodurch Unternehmen das Vertrauen ihrer Kunden gewinnen können, darüber gehen die Einschätzungen von Verbrauchern und Unternehmen deutlich auseinander. Aus Verbrauchersicht gewinnen Unternehmen vor allem durch nachvollziehbare Datensicherheit (78 Prozent), verständliche und faire Geschäftsbedingungen (76 Prozent) und nachvollziehbaren Datenschutz (75 Prozent) das Kundenvertrauen. Die Nutzer bewerten diese Top-Kriterien sogar höher als die Produktqualität (67 Prozent), einen großen Firmennamen (49 Prozent) oder eine interessante Webseite (31 Prozent).

Bei den Unternehmen rangieren verbindliche Kommunikation (92 Prozent), kompetentes Auftreten der Mitarbeiter (92 Prozent), persönlicher Ansprechpartner (91 Prozent) ganz oben. Informationssicherheit und Datenschutz kommen hier erst auf den Plätzen 7 bzw. 8.

4.3 Folgen für Unternehmen

Für die Anbieter heißt das: Sie können sich nicht darauf verlassen, dass ihre zufriedenen Kunden für Vertrauen im Markt sorgen. Sie können Vertrauen auch nicht einkaufen, indem sie sich den oft aufwändigen Prüf- und Zertifizierungsprozessen unterziehen. Sie müssen es sich immer wieder hart erarbeiten, vor allem durch beste Datensicherheit und Datenschutz.

Kriterien für Kundenvertrauen



Basis Privatnutzerbefragung: 1.008 private Internetnutzer
Basis Unternehmensbefragung: 810 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Unternehmen Angaben in Prozent

Frage Privatnutzer: »Wodurch gewinnen Unternehmen im Internet in besonderem Maße Vertrauen bei Ihnen?« (Mehrfachnennung möglich) **Kriterium wurden bei nicht Privatanwendern abgefragt

Frage Unternehmen: »Was meinen Sie, wodurch gewinnen Unternehmen in besonderem Maße Vertrauen bei Ihren Kunden?« (Mehrfachnennung möglich) *Kriterien wurden bei Unternehmen nicht abgefragt

Abbildung 22: Kriterien für Kundenvertrauen aus Privatnutzer- und Unternehmenssicht

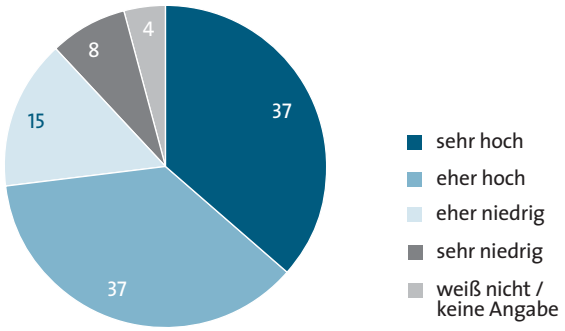
5 Verantwortung für Datenschutz und IT-Sicherheit

5.1 Kooperationsbereitschaft der Unternehmen und Erwartungen der Privatnutzer

Eine wichtige Voraussetzung für eine effektive Arbeit der Behörden im Bereich Datenschutz und IT-Sicherheit ist die Aufklärung von Sicherheitsvorfällen. Nur wenn Polizei, Staatsanwaltschaft oder andere Stellen darüber informiert sind, können sie im Krisenfall schnell und adäquat handeln. Dazu müssen die Unternehmen entsprechende Vorfälle melden und sich austauschen. 74 Prozent der Unternehmen geben an, ihre Bereitschaft zur Zusammenarbeit mit staatlichen Behörden sei eher hoch oder sehr hoch.

Doch wo ist der staatliche Eingriff vom Verbraucher überhaupt gewünscht? Die Ergebnisse zeigen, dass private Nutzer in bestimmten Bereichen der staatlichen Kontrolle eher ablehnend gegenüber stehen. So wünschen sich 57 Prozent, dass die Speicherung von Internetverbindungsraten gar nicht stattfindet oder reduziert wird. Bei der Überwachung von Nachrichten oder Gesprächen für polizeiliche Zwecke sind es sogar 64 Prozent. Demgegenüber fordern Privatnutzer beim Schutz vor Hackerangriffen (89 Prozent) sowie zur vorbeugenden Gefahrenabwehr (79 Prozent) ein stärkeres Durchgreifen.

Bereitschaft der Unternehmen zur Zusammenarbeit mit Behörden bei IT-Sicherheitsvorfällen

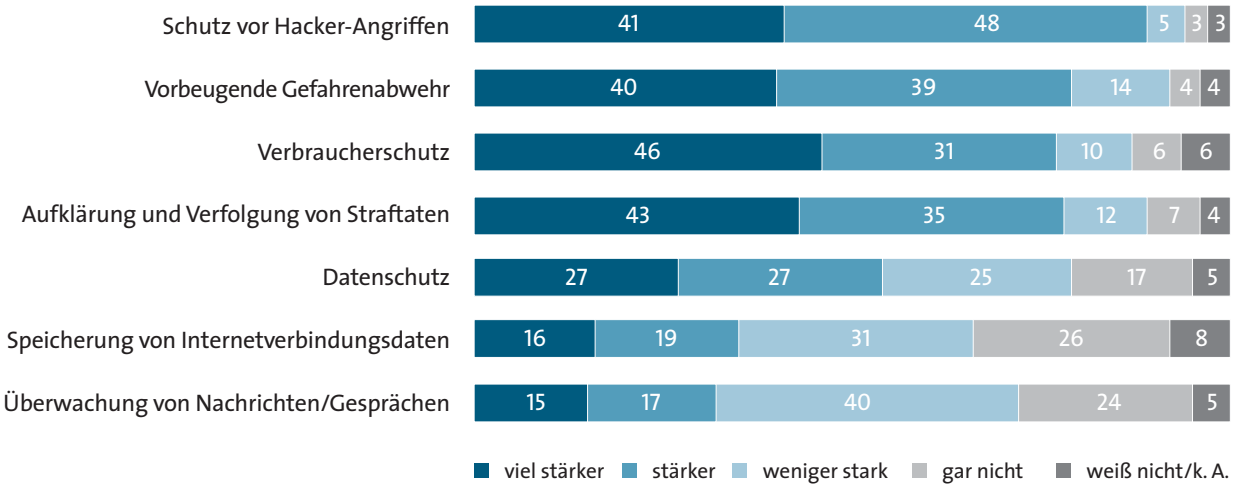


Basis: 810 IT-Leiter, CIOs, Datenschutzbeauftragte und Geschäftsführer von Unternehmen — Angaben in Prozent

Frage: »Wie hoch ist die Bereitschaft in Ihrem Unternehmen, bei IT-Sicherheitsvorfällen mit Behörden zusammenzuarbeiten?«

Abbildung 23: Bereitschaft der Unternehmen zur Zusammenarbeit mit Behörden bei IT-Sicherheitsvorfällen

Erwartungen privater Internetnutzer zum staatlichen Eingriff im Internet



Basis: 1.008 private Internetnutzer — Angaben in Prozent

Frage: »Ich lese Ihnen nun verschiedene Bereiche vor, in denen der Staat mehr oder weniger stark eingreifen kann. In welchen Bereichen soll der Staat im Internet viel stärker, stärker, weniger stark oder gar nicht eingreifen?«

Abbildung 24: Erwartungen privater Internetnutzer zum staatlichen Eingriff im Internet

5.2 BITKOM-Grundsätze zum Datenschutz und zur IT-Sicherheit

Die Verbreitung des Internets hat in den vergangenen Jahren stetig zugenommen. Zudem hat es immer mehr Lebens- und Geschäftsbereiche erfasst. Damit sind auch die Themen Datenschutz und IT-Sicherheit zunehmend wichtiger geworden. Dies gilt sowohl für Privatpersonen wie für Unternehmen. Der BITKOM gibt am Ende dieser Studie wichtige Tipps, wie Privatnutzer ihre Daten und internetfähigen Geräte besser schützen können. Zudem werden Handlungsempfehlungen für Unternehmen gegeben, um bei Sicherheitsvorfällen in der IT besser gerüstet zu sein. Abschließend benennt der BITKOM drei Hauptziele für eine höhere IT-Sicherheit in Deutschland.

Datenschutz- und Sicherheitstipps für Privatpersonen

Privatpersonen können die Sicherheit ihrer persönlichen Informationen schon mit ein paar einfachen Regeln erhöhen. Der BITKOM gibt einige grundlegende Tipps zum Umgang mit den eigenen Daten im Internet und zum Schutz von PCs und Smartphones:

- **Datensparsamkeit**
  Grundsätzlich gilt es, mit den eigenen Daten sparsam umzugehen und bewusst zu entscheiden, welchen Diensten sie anvertraut werden. Je weniger persönliche Informationen im Internet zu einer Person vorhanden sind, desto schwieriger ist es für potenzielle Betrüger, diese zu missbrauchen. Die Daten-Sparsamkeit gilt auch bei der Registrierung für Internet-Dienste. Anwender sollten nur die unbedingt notwendigen Informationen angeben. Auf die Eingabe von Namen, Adressdaten oder gar Kontoverbindungen bei angeblich kostenlosen Online-Diensten sollte daher verzichtet werden. Auch bei Gewinnspielen ist besondere Vorsicht angebracht. Im Zweifel sollte auf die Eingabe persönlicher Informationen lieber verzichtet werden. Der sparsame Umgang mit den eigenen Daten betrifft auch Smartphone-Nutzer. Sie sollten die Ortungsfunktion ihres Geräts nur aktivieren, wenn dies für den gewünschten Dienst nachvollziehbar notwendig ist.

- **Private Daten schützen**
  Die Sparsamkeit mit den eigenen Daten ist auch deshalb wichtig, weil das Internet nichts vergisst. Selbst wenn persönliche Informationen bereits gelöscht wurden, können sie als Kopien an anderer Stelle im Internet noch vorhanden sein. Daher ist es wichtig, den Zugang zu privaten Informationen, beispielsweise in sozialen Netzwerken oder auf privaten Webseiten, zu beschränken. Auch im Alltag würden die meisten Menschen Unbekannten nicht ihr gesamtes Privatleben offenbaren. Der Zugriff auf persönliche Fotos oder die Kontaktdaten sollten nur guten Bekannten zugänglich gemacht werden. Potenziell peinliche Fotos und Texte in Netzwerk-Profilen sollten konsequent gelöscht werden oder am besten gar nicht online gehen.

- **Anbieter-Check**
  Internetnutzer sollten bei der Auswahl von Anbietern von Online-Diensten auf deren Datenschutzerklärung achten. Darin ist beschrieben, wie mit den persönlichen Daten der Kunden umgegangen wird und wie sie unter Umständen weiter genutzt werden. Bleiben dennoch Unklarheiten, sollte im Zweifel vor der Anmeldung per E-Mail nachgefragt werden. Nutzern steht außerdem das Recht zu, der Weitergabe der eigenen Daten an Dritte, beispielsweise zu Werbezwecken, zu widersprechen. Bei der Auswahl von Online-Shops sollte auf ein Impressum mit Anschrift des Geschäftsführers sowie klare Geschäftsbedingungen (AGB) geachtet werden. Auch bei der Installation von Apps können Smartphone-Nutzer in der Datenschutzerklärung und den AGBs erfahren, wie der Anbieter mit den persönlichen Informationen umgeht.

- **Benutzername**
  Ob Internet-Nutzer besser mit ihrem echten Namen oder einem Pseudonym (Nickname) auftreten, hängt von der Art der Web-Plattform ab. Für Einträge in Fach-Foren, beim Twittern oder in Verbraucherportalen empfiehlt es sich, einen Nicknamen zu verwenden. Nur wenn man leichter gefunden werden möchte, sollte der echte Name genutzt werden. Das ist bei einigen Internet-Communitys oder sozialen Netzwerken üblich.

- **Suchmaschinen**
  Bei der Anmeldung zu einer Internet-Gemeinschaft sollte eine Einstellung gewählt werden, die das Profil nicht über Suchmaschinen auffindbar macht. Dann können es nur die Mitglieder der Community finden und lesen und nicht jeder Internet-Nutzer. Bei den meisten solcher Netzwerke sind die Profile nur dann über Suchmaschinen auffindbar, wenn die Nutzer es ausdrücklich wünschen. Da es aber auch Communitys gibt, die dies anders handhaben, sollte jeder die entsprechende Einstellung gleich bei der Registrierung prüfen.

- **Eigener Ruf**
  Jeder sollte regelmäßig mit Suchmaschinen prüfen, welche Informationen im Netz über seine Person vorhanden sind. Dies gilt insbesondere für alle, die viel veröffentlichen oder in der Öffentlichkeit arbeiten. Wer einen häufigen Namen trägt, gibt Vor- und Nachnamen in Anführungszeichen ein («Max Müller«) und danach etwa Wohnort, Beruf oder Sportverein. So lassen sich Ergebnisse filtern. Neben allgemeinen Suchmaschinen wie Google oder Bing können auch spezielle Suchmaschinen für Personen genutzt werden. Diese beziehen auch soziale Netzwerke in die Suche ein.

- **Urheber- und Persönlichkeitsrechte**
  Wenn jemand Ihre Fotos oder Texte unerlaubt ins Netz gestellt hat, können Sie die Löschung verlangen. Dies gilt auch, wenn Ihnen das Bild nicht gehört, Sie aber darauf zu sehen sind. Jeder hat ein »Recht am eigenen Bild«. Sie dürfen bestimmen, ob und in welchem Zusammenhang Bilder von Ihnen veröffentlicht werden. Daher sollten auch Sie keine Fotos von anderen veröffentlichen, ohne vorher zu fragen. Im privaten Umfeld sollte eine Aufforderung zur Löschung per E-Mail oder Telefon reichen. Passiert nichts, können Sie einen Anwalt einschalten.

- **Passwörter und Sperrcodes**
  Für viele Online-Dienste müssen die Nutzer ein Passwort zur Anmeldung benutzen. Um möglichst sichere Passwörter zu erzeugen und zu verwenden, gilt es daher ein paar Tipps zu beachten:

  - Verwenden Sie nicht dasselbe Passwort bei mehreren Diensten
  - Je länger das Passwort, desto sicherer. Es sollte mindestens acht, besser zehn Zeichen lang sein.
  - Nutzen Sie willkürlich Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
  - Das Passwort sollte sich in keinem Wörterbuch wiederfinden.

  Sichere Passwörter lassen sich leicht merken, wenn man sich einen Satz ausdenkt und dann jeweils die ersten Buchstaben der Wörter sowie die Satzzeichen als Passwort verwendet. Hilfreich sind auch spezielle Programme, sogenannte Passwort-Safes. Sie können die Geheimzahlen und Passwörter sicher speichern. Der Anwender braucht sich dann nur noch das Haupt-Passwort zu merken. Zudem sollten die Passwörter gelegentlich geändert werden. Gleiches gilt auch für die PIN und gegebenenfalls den Sperrcode von Mobiltelefonen.

- **Verschlüsselte Verbindungen**
  Sensible Informationen, etwa Konto- und Kreditkartendaten, sollten nur über verschlüsselte Verbindungen übertragen werden. Ob die Verbindung sicher ist, erkennen Sie an den Buchstaben »https« vor der Internetadresse oder an einem kleinen Schlosssymbol im Internet-Programm (Browser). Zunehmend sind sichere Webseiten auch an einer grün hinterlegten Adresszeile erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat. Zahlungen

können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahldienste, bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist verbreitet, aber riskanter.

- **E-Mails und Chat**
  Öffnen Sie nur E-Mails, die von vertrauenswürdigen Absendern stammen und bei denen Sie sich den Hintergrund des Versandes plausibel erklären können. Denn technisch versierte Betrüger können die Absenderadresse fälschen. Dubiose Mails von unbekannten Absendern möglichst sofort löschen. Schadprogramme verbergen sich oft in Grafiken oder E-Mail-Anhängen. Verdächtige Dateien auf keinen Fall öffnen! Folgen Sie auch nicht den Links in verdächtigen E-Mails, denn diese können auf verseuchte Webseiten führen. Auch bei E-Mails von Kreditinstituten ist besondere Vorsicht geboten: Banken bitten Kunden unter keinen Umständen per Mail, vertrauliche Daten, wie Transaktionsnummern (TAN), im Netz einzugeben. Auch bei Chat-Nachrichten von Unbekannten ist Vorsicht geboten: Kriminelle versenden oft Links zu Webseiten mit Viren.

- **Online-Banking**
  Beim Online-Banking sollte man die offizielle Adresse der Bank immer direkt eingeben oder über eigene Lesezeichen (Favoriten) aufrufen. Zudem muss darauf geachtet werden, dass die Verbindung, wie bei anderen Zahlvorgängen im Web verschlüsselt ist. Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen dieser Codes aus einer Liste frei wählen. Sicherer ist das iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufallsgenerator der Bank bestimmt, welche TAN aus der Liste eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren. Dabei werden die Codes per Kurzmitteilung direkt auf das Mobiltelefon geschickt. Weitere Schutzverfahren sind chipTAN und HBCI, bei denen der Kunde als Zusatzgeräte einen TAN-Generator oder ein Kartenlesegerät nutzt. Wichtig: Kreditinstitute fragen niemals mehr als eine TAN gleichzeitig ab.

- **PC-Schutz**
  Viren und andere Schadprogramme beeinträchtigen nicht nur die Funktion von PCs, sondern werden zunehmend zur Ausspähung digitaler Identitäten eingesetzt. Vor der ersten Internet-Nutzung müssen ein Anti-Viren-Programm und eine Firewall installiert werden, um den PC zu schützen. Diese Schutzprogramme sowie Betriebssystem und Internet-Programm des PCs müssen regelmäßig aktualisiert werden. Da Schadsoftware auch über Datenträger, wie DVDs und CDs, USB-Sticks und Speicherkarten, verbreitet wird, sollten auch diese regelmäßig überprüft werden. Tipps gibt es beispielsweise unter www.verbraucher-sicher-online.de, www.bis-fuer-buerger.de, www.deutschland-sicher-im-netz.de und www.klicksafe.de.

- **Schutz für Smartphone-Nutzer**
  Schadprogramme gibt es auch für Smartphones. Um Sicherheitslücken zu schließen, müssen die Updates der Geräte-Hersteller regelmäßig installiert werden. Auch bei den Mobil-Geräten gilt: Viren-Schutz und Firewall sind für die eigene Sicherheit zu installieren. Zudem ist es ratsam, grundsätzlich alle Daten zu verschlüsseln. Bei Verlust des eigenen Mobiltelefons sollten die eigenen Daten aus der Ferne gelöscht werden. Für viele Smartphones ist dies kostenlos. Nutzer von Apples iPhone können sich unter www.icloud.com für den Service registrieren. Für Smartphones mit dem Microsoft Betriebssystem Windows Phone gibt es einen ähnlichen Service unter www.windowsphone.com. Auch viele Hersteller von Android-Smartphones, etwa Samsung oder Motorola, bieten die Fernlöschung des eigenen Geräts an.

- **Funkverbindungen**
  Smartphone-Nutzer sollten Funkverbindungen, wie WLAN oder Bluetooth, nur dann aktivieren, wenn diese tatsächlich benötigt werden. Potenziellen Angreifern wird dadurch der Zugriff auf das Gerät erschwert. Zudem sollten sensible Informationen nicht über ungesicherte WLAN-Netze übertragen werden. Nur Drahtlos-Netzwerke, die den Standard WPA2 verwenden, bieten ausreichend Schutz für persönliche Daten, da eine verschlüsselte Übertragung genutzt

wird. Zudem sollte die Ortungsfunktion der Smartphones nur aktiviert werden, wenn der gewünschte Dienst die Daten gerade benötigt.

Handlungsempfehlungen des BITKOM zu Informationssicherheit für Unternehmen

Für Unternehmen ist der Bereich Datenschutz und IT-Sicherheit zunehmend wichtiger geworden. Wie die Studie zeigt, haben bereits 39 Prozent direkte Angriffe auf ihre IT oder vergleichbare Sicherheitsvorfälle erlebt. Dennoch sind viele Unternehmen nicht auf Störfälle vorbereitet. So hat fast jedes zweite Unternehmen keinen Notfallplan für IT-Sicherheitsvorfälle. Der BITKOM gibt Handlungsempfehlungen für Unternehmen, um besser auf Sicherheitsvorfälle eingestellt zu sein:

- **Sicherheitsrisikoanalyse**
  Eine Sicherheitsrisikoanalyse hilft den Schutzbedarf des Unternehmens zu ermitteln und ein entsprechendes Sicherheitskonzept zu entwickeln. Zudem liefert es wertvolle Informationen zu der Frage, welche Sicherheitsprodukte eingesetzt werden können, um die Risiken eines IT-Angriffs zu minimieren.
  Auf folgende Fragen sollte eine Sicherheitsrisikoanalyse Antworten liefern:
  - Welche Gefahren existieren, die den reibungslosen Geschäftsbetrieb, beziehungsweise die Geschäftsgrundlage meines Unternehmens bedrohen können?
  - Wie hoch sind die Eintrittswahrscheinlichkeiten dieser Gefahren?
  - Mit welchem Schadensausmaß muss jeweils gerechnet werden?
  - Ab wann ist der Geschäftsbetrieb soweit gestört, dass die Existenz meines Unternehmens gefährdet ist?

- **Notfallplan für IT-Sicherheit in Unternehmen**
  Ein wichtiges Instrument zur Gefahrenabwehr im Fall eines Angriffs ist ein Notfallplan. Dieser listet die wichtigsten Geschäftsprozesse auf und gibt klare Handlungsempfehlungen vor. Dazu gehören Anweisungen, was im Schadensfall zu unternehmen ist, sowie Personen, die umgehend zu informieren sind. Wer ein klares Vorgehen und die richtigen Ansprechpartner dokumentiert hat, kann schnell reagieren und die Auswirkungen eines IT-Sicherheitsvorfalls weitgehend minimieren. Denn Zeit wird bei einem Angriff zum kritischen Faktor.

- **Einführung von Sicherheitsrichtlinien**
  Die Sicherheitsrichtlinien sollten die Grundlage für alle Sicherheitsmaßnahmen im Unternehmen darstellen. Sie umfassen allgemeine Regelungen, Prozesse und Richtlinien, die für alle Mitarbeiter bindenden Charakter haben. Außer für die konkreten Maßnahmen können sie auch für die Auswahl der Sicherheitsprodukte als Grundlage dienen. Die Richtlinien sollten schriftlich festgehalten und fortlaufend aktualisert werden. Zudem sind sie als Handlungsanweisungen an die Mitarbeiter zu verteilen.

- **Mitarbeiter für Sicherheit sensibilisieren**
  Die besten Sicherheitsrichtlinien und -maßnahmen versprechen keinen Erfolg, wenn sie nicht von den Mitarbeitern angewendet werden. Deshalb ist es wichtig, die Belegschaft für das Thema Sicherheit zu sensibilisieren. Eine Informationskampagne kann bei der Bewusstseinsbildung sehr hilfreich sein. Wichtig ist es hierbei, das Thema Sicherheit gut verständlich zu kommunizieren. Die Kampagne sollte, sowohl zur Auffrischung als auch für neue Mitarbeiter, in gewissen Abständen wiederholt werden. Hierbei können auch gewisse thematische Schwerpunkte variieren.

- **Kosten für IT-Sicherheit**
  Die Frage nach den Kosten für die IT-Sicherheit ist abhängig vom individuellen Schutzbedarf des Unternehmens, der Branche und dem Wert derzu schützenden Informationen. Als repräsentativer Richtwert hat sich die Zahl von 15 Prozent des gesamten IT-Budgets etabliert. Grundsätzlich sollte auf ein ausgegelichenes Verhältnis zwischen dem Wert der Informationen und den Investitionen zu deren Schutz geachtet werden.

Außerdem sollten die Lösungen am Markt für Sicherheitssysteme umfangreich verglichen und mit den eigenen Bedürfnissen abgeglichen werden, bevor man sich für eine Investition entscheidet.

- **Datenschutz**
  Der Datenschutz sollte in Unternehmen einen hohen Stellenwert genießen. Hauptgründe dafür sind neben den verbindlichen Vorgaben der Datenschutzgesetze auch Risiken, wie Image- oder Vertrauensverlust, wenn etwa Kundendaten an die Öffentlichkeit gelangen. Unter den Datenschutz fallen sämtliche personenbezogenen Daten, also auch jene zu Kunden und Mitarbeitern. Grundsätzlich sollte nach dem Prinzip der Datensparsamkeit gearbeitet werden, um Risiken von vornherein zu minimieren.

- **Datenschutzbeauftragte**
  Der betriebliche Datenschutzbeauftragte übernimmt die Aufgaben einer internen Selbstkontrolle. Außerdem macht er die Beschäftigten im Unternehmen mit den Erfordernissen des Datenschutzes vertraut. Unternehmen, bei denen mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Daten ständig beschäftigt sind, müssen einen Datenschutzbeauftragten bestellen. Erfolgt die Datenverarbeitung nicht automatisiert, gilt diese Regel erst ab 20 Personen. Der Datenschutzbeauftragte kann entweder intern ernannt werden oder durch einen externen Dienstleister gestellt werden.

- **Unbefugte Einsichtnahme verhindern**
  Die Sicherheit von Daten hängt maßgeblich von ihrer Verarbeitung ab. Computer, Software und Netzwerke müssen daher vor unauthorisierten Zugriffen von außen geschützt werden. Das ist vor allem eine große technische Herausforderung. Aber auch jeder einzelne Mitarbeiter hat mit Daten an seinem Arbeitsplatz vertrauensvoll umzugehen.

- **Unrechtmäßige Datennutzung verhindern**
  Auch innerhalb des Unternehmens gilt es, die Daten vor unauthorisierten Zugriffen zu schützen. Für die Organisation eines Unternehmens heißt das u.a., dass jeder Mitarbeiter ausschließlich auf die Informationen zugreifen können sollte, die er für seine Funktion benötigt.

- **Integrität der Daten sicherstellen**
  Daten dürfen nicht verloren gehen oder durch unauthorisierte Zugriffe manipuliert werden. Integrität ist daher ein wichtiges Ziel der Datensicherheit. Hierfür gilt es sowohl technische wie organisationelle Vorraussetzungen zu schaffen.

- **Auftragsdatenverarbeitung**
  Bei der Verarbeitung personenbezogener Daten sind technische und organisatorische Sicherheitsmaßnahmen einzuhalten, um unauthorisierte Zugriffe zu vermeiden und die Integrität der Daten sicherzustellen. Die Verantwortlichkeit für die Sicherheit der Daten gilt aber auch, wenn sie zur Verarbeitung an einen Dienstleister weitergeleitet werden. Das verantwortliche Unternehmen muss spezielle vertragliche Regelungen mit dem Dienstleister vereinbaren, um sicherzustellen, dass der Dienstleister die datenschutzrechtlich notwendigen Maßnahmen ergreift. Schon vor der Weitergabe der Daten an den Dienstleister muss die Einhaltung der Sicherheitsmaßnahmen aktiv überprüft werden.

Zusammenarbeit von Unternehmen und Behörden

Cyber-Sicherheit wird zu einem entscheidenden Standortfaktor. Sie wird künftig die gleiche Bedeutung bei Investitionsentscheidungen haben wie innere und äußere Sicherheit oder ordnungspolitische und rechtliche Planungssicherheit. IT-Sicherheit kann nicht von oben verordnet und durchgesetzt werden. Im Gegenteil: Jeder Einzelne muss mitmachen, denn jeder Einzelne kann das Einfallstor sein, über das ein großes, komplexes System angegriffen wird. Daher müssen einzelne Unternehmen, ganze Branchen und staatliche Stellen zusammenarbeiten, um die Cyber-Sicherheit insgesamt zu gewährleisten und den Wirtschaftsstandort Deutschland gegen Cyberbedrohungen widerstandsfähiger zu machen.

BITKOM und BSI haben daher eine »Allianz für Cybersicherheit« ins Leben gerufen. Sie ist dringend notwendig um diese drei Ziele zu erreichen. Bestehende Initiativen sind wichtig und hilfreich, konzentrieren sich aber häufig auf die Prävention. Sie steigern vor allem die Aufmerksamkeit oder arbeiten regional. Zusätzlich ist aber vor Ort in den Regionen ein Informations- und Erfahrungsaustausch und Hilfe im Schadensfall notwendig. Um dies erreichen zu können, müssen nationale wie regionale Akteure zusammenarbeiten. Wesentliche Multiplikatoren des Themas IT-Sicherheit können hier IHKs, regionale Unternehmerverbände und staatliche Stellen wie Landeskriminalämter sein.

Der BITKOM sieht daher für die Zukunft drei Hauptziele:

- Unternehmen müssen erstens in der Lage sein, Sicherheitsinformationen zu verarbeiten. Jedes Unternehmen, das IT intensiv nutzt, sollte einen Beauftragten für die IT-Sicherheit benennen und diese Rolle möglichst qualifiziert besetzen. In Zeiten des Fachkräftemangels ist das nicht leicht, aber unerlässlich. Ein solcher Experte sollte vor allem aus den aktuellen internen und externen Informationen die richtigen Schlüsse für das IT-Risikomanagement des eigenen Unternehmens ziehen.

- Zweitens müssen Unternehmen bereit sein, Informationen zu teilen. Sowohl für die Strafverfolgung wie für die Warnung anderer Unternehmen und Organisationen sind einzelne Meldungen zu Vorfällen wichtige Informationen. Wenn solche Informationen zusammengeführt werden, können schnell Strategien und Handlungsmuster der Täter abgeleitet werden. Außerdem können Unternehmen durch einen vertrauensvollen Informationsaustausch aus den Erfahrungen anderer viel lernen.

- Drittens brauchen wir ein aktuelles Lagebild der IT-Sicherheit in Deutschland. Dazu gehören aktuelle Informationen über Spam oder neue Schadsoftware, beispielsweise von den Honeypot-Systemen der Netzbetreiber und Sicherheitsdienstleister sowie Lageinformationen von den Computer Emergency Response Teams (CERTs) der Unternehmen und Behörden. Eine Institution wie das Bundesamt für Sicherheit in der Informationssicherheit (BSI) kann solche Daten aufnehmen und auswerten. Ein Lagebild ist dabei kein Selbstzweck. Die Ressourcen sind knapp, sie müssen effizient eingesetzt werden. Deshalb muss man sich auf die wirklichen kritischen Vorgänge konzentrieren.

Untersuchungsdesign und Methodik

Auftraggeber:	BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Institut:	ARIS UMFRAGEFORSCHUNG Markt-, Media- und Sozialforschungsgesellschaft mbH
Erhebungszeitraum:	12.12.2011 – 23.01.2012 (Unternehmensbefragung) 17. bis 24. Januar 2012 (Verbraucherumfrage)
Grundgesamtheit:	Internetnutzer ab 14 Jahre Unternehmen in Deutschland mit 3-249 Mitarbeitern oder 250 und mehr Mitarbeitern*
Stichprobengröße:	1.339 Personen ab 14 Jahren sowie 810 Unternehmen, davon 304 aus der ITK-Branche und 506 Anwenderfirmen; Zufallsstichprobe
Erhebungsmethode:	Telefonische Befragung (CATI)
Gewichtung:	repräsentative Gewichtung der Personenstichprobe nach Region, Alter, Geschlecht und Bildung (Privatpersonen) bzw. nach Branchen und Größenklassen (Unternehmen)
Statistische Fehlertoleranz:	+/- 3 Prozentpunkte in der Gesamtstichprobe

* Wirtschaftszweige WZ 2008 Abschnitte A bis N und P bis S (d. h. ohne Öffentliche Verwaltung, Verteidigung und Sozialversicherung)

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org