TRUST IN
GERMAN
SICHERHEIT

# Cybersicherheit

## Ein aktuelles Stimmungsbild deutscher Unternehmen

TNS Infratest

# Vorwort

Die steigende Bedeutung und Verbreitung des Internets hat in den letzten Jahren zu einer starken Vereinfachung und Bereicherung aller Wirtschaftsaktivitäten geführt. Vernetzte Computersysteme und digitale Technologien verzweigen sich immer tiefer in alle Wertschöpfungsprozesse unserer Wirtschaft und das Internet wird zur kritischen und zugleich höchst relevanten Infrastruktur.

**Diese Entwicklung birgt jedoch gleichzeitig enorme Gefahren durch immer neue Möglichkeiten des Missbrauchs und der Kriminalität: Industriespionage und der Diebstahl geistigen Eigentums über das Netz sind in unserer modernen Gesellschaft die Gefahren, die ganze Unternehmen stark schädigen oder zu Fall bringen können.**

Während die IT-Verantwortlichen in den Unternehmen bisher darauf fokussiert waren, die eigenen Daten durch Backups vor Verlust durch interne Störungen wie Strom- oder Systemausfälle zu schützen, geht es aktuell zunehmend darum, die eigene Infrastruktur gegenüber Angriffen von außen abzuschirmen. Die Verwendung neuester Sicherheitssoftware wird zur Grundvoraussetzung, der Investitionsbedarf an IT-Sicherheit steigt.

Technologie- und Softwareunternehmen sowie IT-Sicherheitsspezialisten sind gefordert, Lösungen auf dem neuesten Stand der Technik zu entwickeln und das Bewusstsein für digitale Sicherheit zu schärfen. G DATA stellt sich dieser Herausforderung und zeigt u. a. mit dieser Studie auf, wie es um die IT-Sicherheit in deutschen Unternehmen steht, welche Gefahren und Risiken es gibt und wo Handlungsbedarf besteht.

# Hintergrund und Zielsetzung der Studie

G DATA hat bereits im Herbst 2013, kurz nach den ersten Enthüllungen der NSA-Spionageaffäre und dem Bekanntwerden geheimdienstlicher Aktivitäten, eine Erhebung zum Thema Cybersicherheit durchgeführt, um ein Stimmungsbild deutscher Unternehmen zu erhalten. Es ging insbesondere darum zu erfahren, wie sicher sich Unternehmen in Deutschland in der digitalen Welt fühlen, für wie wahrscheinlich sie Angriffe aus dem Internet halten, wie häufig sie von Angriffen betroffen sind und welche Maßnahmen sie dagegen ergreifen bzw. ergriffen haben.

Ein halbes Jahr später - im März 2014 - hat G DATA das Thema noch einmal aufgegriffen, um zu untersuchen, wie sich im Vergleich zu August/September 2013 das Stimmungsbild der Unternehmen verändert hat. Zu diesem Zweck wurde das Institut TNS Infratest beauftragt, die Studie 2014 im Auftrag von G DATA durchzuführen.

Die Tatsache, dass seit den ersten Enthüllungen von Edward Snowden in der Zwischenzeit weitere Details zur Spionageaffäre ans Licht kamen und auch die mediale Aufmerksamkeit rund um die Themen IT-Sicherheit und Datenschutz machen eine weitere Befragung zu diesem Zeitpunkt lohnenswert. Gerade auch die jüngsten Nachrichten zu millionenfachem Datenklau und geknackten E-Mail-Konten haben dazu beigetragen, das Thema noch stärker in das öffentliche Bewusstsein und damit in die Köpfe der Anwender zu bringen, und machen eine tiefgehende Auseinandersetzung unumgänglich.

# Methodik und Stichprobe

**1. Welle (August/September 2013): n=90**

**2. Welle (März/April 2014): n=218**

**PAPI (Paper & Pencil) postalisch-schriftliche Befragung**

**Befragungswellen**

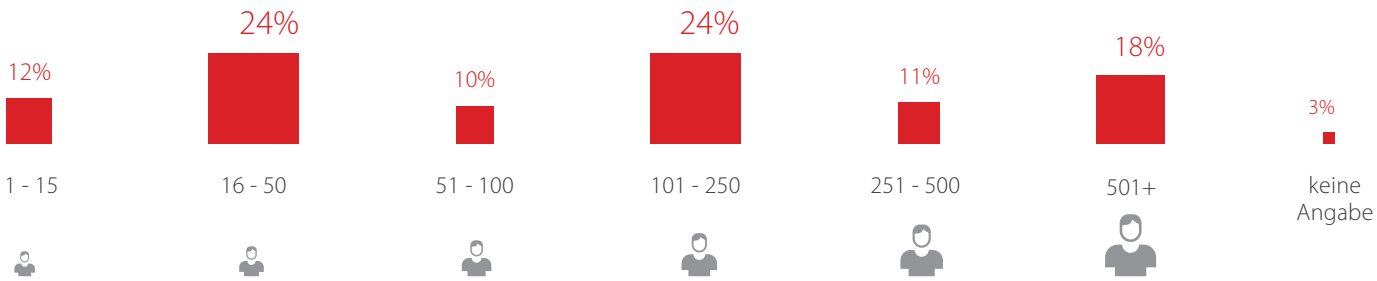
Die erste Welle der Befragung wurde im August/September 2013 von G DATA selbst durchgeführt und es wurden insgesamt 90 IT-Verantwortliche aus deutschen Unternehmen befragt. An der zweiten Welle, durchgeführt von TNS Infratest im März/April 2014, beteiligten sich in Summe 218 IT-Verantwortliche aus deutschen Unternehmen.

**Erhebungsmethode**

Im Jahr 2014 wurden Unternehmen verschiedener Größen und Branchen via postalisch-schriftlicher Zufallsbefragung (PAPI-Methode/Paper & Pencil), gewissermaßen ein „Querschnitt deutscher Unternehmen", befragt. Um die Daten der beiden Jahre vergleichbar zu machen, wurden die Daten aus dem Jahr 2013 nach der Struktur von 2014 gewichtet (nach Anzahl der Mitarbeiter und Branchen).

# Zusammensetzung der Stichprobe 2014
## Befragung quer durch alle Unternehmensgrößen

**Unternehmensgröße nach Anzahl der Mitarbeiter ( ):**




*FRAGE: Wie viele Mitarbeiter sind in Ihrem Unternehmen beschäftigt? BASIS: Alle befragten Unternehmen (2014: n=218; 2013: n=90)*

# Zusammenfassung

## Zentrale Erkenntnisse

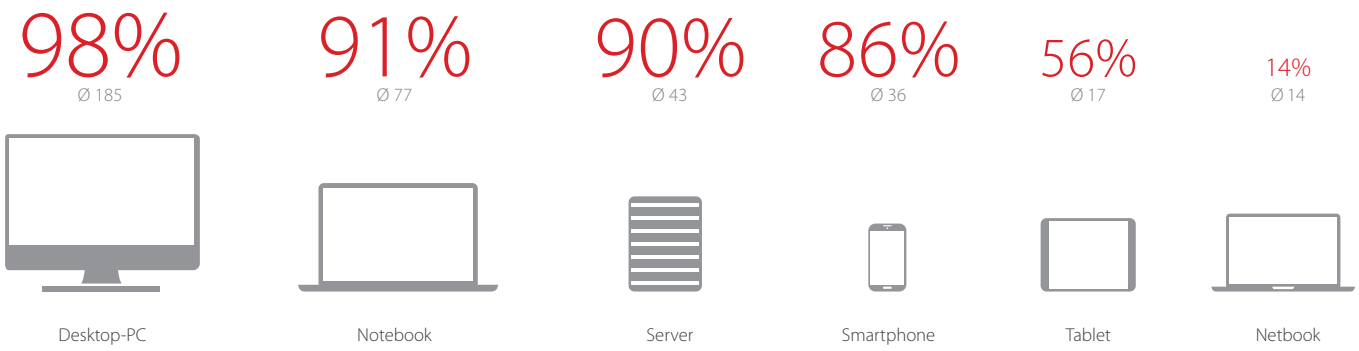
- Im Vergleich zu 2013 steigt das **Sicherheitsbewusstsein** der Unternehmen.
- Es ist ein leichter Anstieg der durch **Internetangriffe** verursachten Schäden zu verzeichnen.
- „Standardmaßnahmen" wie Updates und Datensicherungen sind weit verbreitet, jedoch gibt es Nachholbedarf bei weitergehenden Maßnahmen wie **Verschlüsselungen** und **Richtlinien**, die größtenteils sogar weniger häufig im Vergleich zum Vorjahr eingesetzt werden.
- In kleineren Unternehmen (bis 50 Mitarbeiter) ist **IT-Sicherheit** häufig nicht professionalisiert.
- **Professionalisierung von IT-Sicherheit** in größeren Unternehmen (ab 50 Mitarbeiter) führt trotz größerer Angriffsfläche zu weniger Schäden durch Internetangriffe.

## Empfehlungen

- IT-Sicherheit, Datensicherheit und Datenschutz müssen in der digitalen Welt weiterhin an **oberster Stelle stehen**. Das Schadenspotenzial hier ist enorm und das **Bewusstsein** für dieses Thema in der Wirtschaft und in der Gesellschaft muss weiter geschärft werden.
- Insbesondere kleinere Unternehmen (bis 50 Mitarbeiter) sollten mit dem Thema IT-Sicherheit deutlich **professioneller** umgehen und dezidierte **Experten** dafür einsetzen.
- Weitergehende Maßnahmen wie Verschlüsselungen, Definition von Rechten und Vertraulichkeitsstufen, Unternehmensrichtlinien und gezielte Schulungen müssen **Standard** in allen Unternehmen werden.
- **Jeder einzelne Mitarbeiter** eines Unternehmens (und damit auch jeder Bürger unserer Gesellschaft) ist gefordert und sollte entsprechend **sensibilisiert** und **motiviert** werden, IT-Sicherheit ernst zu nehmen um entsprechend sein Verhalten danach ausrichten zu können.

# Vorhandene Hardware im Unternehmen

## Hohe Durchdringung mit Endgeräten bietet Angriffsfläche



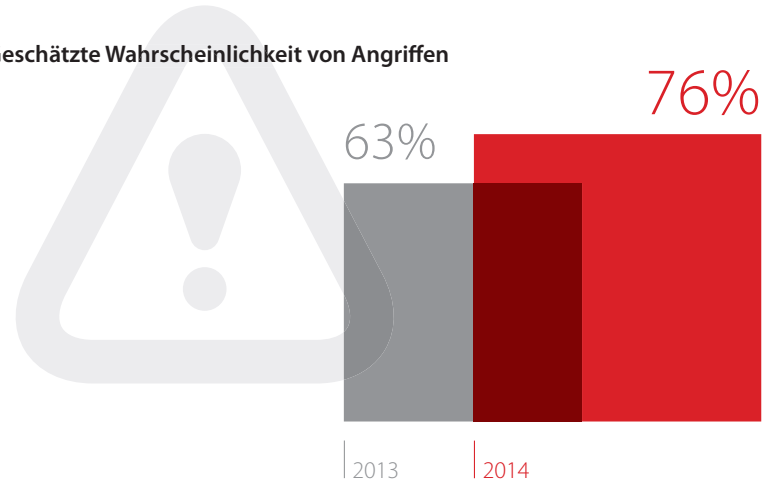

*FRAGE: Welche Hardware ist in Ihrem Unternehmen vorhanden? BASIS: Alle befragten Unternehmen (2014: n=218)*

**In 86% der befragten Unternehmen sind Smartphones vorhanden.**

# Wahrscheinlichkeit für Angriffe aus dem Internet

## Gestiegenes Sicherheitsbewusstsein im Vergleich zu 2013

**Geschätzte Wahrscheinlichkeit von Angriffen**




Wahrscheinliche bzw. sehr wahrscheinliche Gefahr
2014/2013

*2014 2013*

*Top-2-Nennungen („Sehr wahrscheinlich"/„Eher wahrscheinlich")*
*Frage: Für wie wahrscheinlich halten Sie die Gefahr von Schäden für Ihr Unternehmen durch Computerschädlinge oder Angriffe aus dem Internet (Viren, Trojaner, Würmer, Phishing)?*
*BASIS: Alle Befragten Unternehmen (2014: n=218; 2013: n=90)*

Aktuell halten rund drei Viertel (76 Prozent) aller Befragten Angriffe aus dem Internet für wahrscheinlich bzw. sehr wahrscheinlich. Dies ist eine Steigerung von 13 Prozentpunkten im Vergleich zur letztjährigen Erhebung (2013: 63 Prozent).

Hier zeigt sich deutlich die als höher eingestufte Gefahr bzw. die höhere Sensibilität für dieses Thema. Dieser Zuwachs ist vor allem vor dem Hintergrund der NSA-Spionageaffäre im Jahr 2013 sehr interessant. Zwar fand auch die letztjährige Erhebung im Herbst

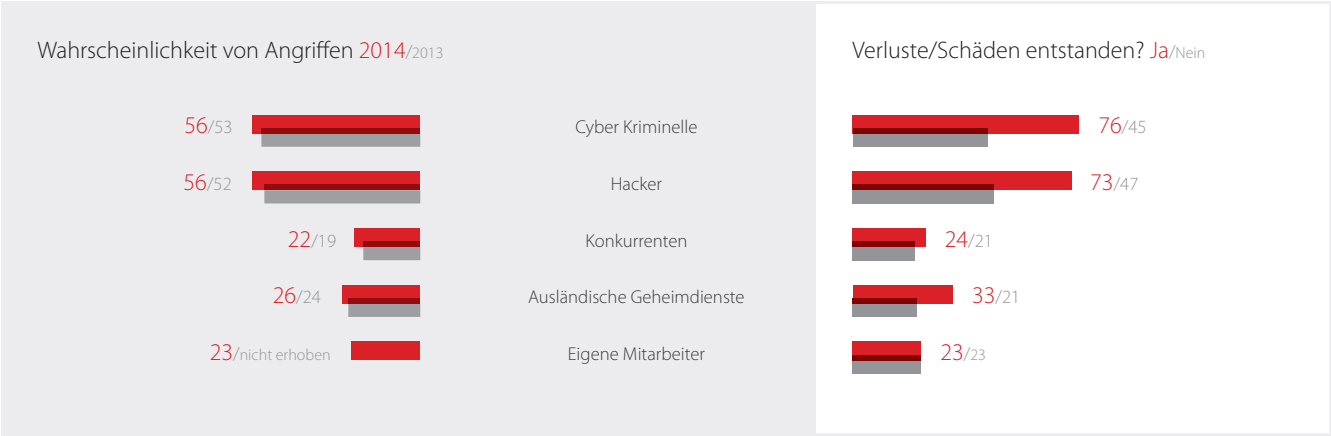
2013 nach den ersten Enthüllungen statt, jedoch sind seitdem zum einen noch deutlich mehr Informationen und weitere Nachrichten zu Datenmissbrauch und Datenklau zutage getreten und haben das Ausmaß klar gemacht, zum anderen sind gerade die IT-Verantwortlichen hier augenscheinlich risikobewusster.

Gefragt nach der Wahrscheinlichkeit von Netzangriffen durch bestimmte Personen bzw. Institutionen schätzten die Befragten diese jeweils geringfügig höher im Vergleich zum Vorjahr ein: Bei Cyber-Kriminellen und Hackern gehen die Befragten von einer relativ hohen Angriffswahrscheinlichkeit aus (jeweils 56 Prozent halten dies für wahrscheinlich bzw. sehr wahrscheinlich), bei Angriffen von Konkurrenten (22 Prozent), ausländischen Geheimdiensten (26 Prozent) und eigenen Mitarbeitern (23 Prozent) gehen die IT-Verantwortlichen der befragten Unternehmen von deutlich niedrigeren Wahrscheinlichkeiten für Angriffe aus.

Eine weitergehende Analyse zeigt folgendes Bild: Unternehmen, in denen es bereits Verluste bzw. Schäden nach Internetangriffen gegeben hat, schätzen die Wahrscheinlichkeit für Angriffe bestimmter Personen bzw. Institutionen – wenig überraschend – als deutlich höher ein. Dies gilt insbesondere für Angriffe von Cyber-Kriminellen (76 Prozent der Unternehmen mit Schäden halten diese für sehr wahrscheinlich oder eher wahrscheinlich, hingegen nur 45 Prozent der Unternehmen ohne Schäden) und für Angriffe von Hackern (73 Prozent vs. 47 Prozent). Auch bei Angriffen von ausländischen Geheimdiensten gehen Befragte aus geschädigten Unternehmen von höheren Wahrscheinlichkeiten aus (33 Prozent vs. 21 Prozent). Angriffe seitens Wettbewerber oder eigener Mitarbeiter werden als weniger wahrscheinlich erachtet und es zeigt sich hier auch kein nennenswerter Unterschied zwischen Geschädigten und Nicht-Geschädigten.

**Bei Geschädigten höhere Sensibilität gegenüber Cyber-Kriminellen und Hackern – Konkurrenten und ausländische Geheimdienste werden weniger gefürchtet.**

**Wahrscheinlichkeit von Angriffen bestimmter Institutionen**




2014 2013

*Top-2-Nennungen („Sehr wahrscheinlich"/„Eher wahrscheinlich")*

*FRAGE: Für wie wahrscheinlich halten Sie es, dass die folgenden Personen/Institutionen die IT-Systeme Ihres Unternehmens angreifen?*

*BASIS: Alle befragten Unternehmen (2014: n=218; 2013: n=90)*

Ja Nein

*Top-2-Nennungen („Sehr wahrscheinlich"/„Eher wahrscheinlich")*

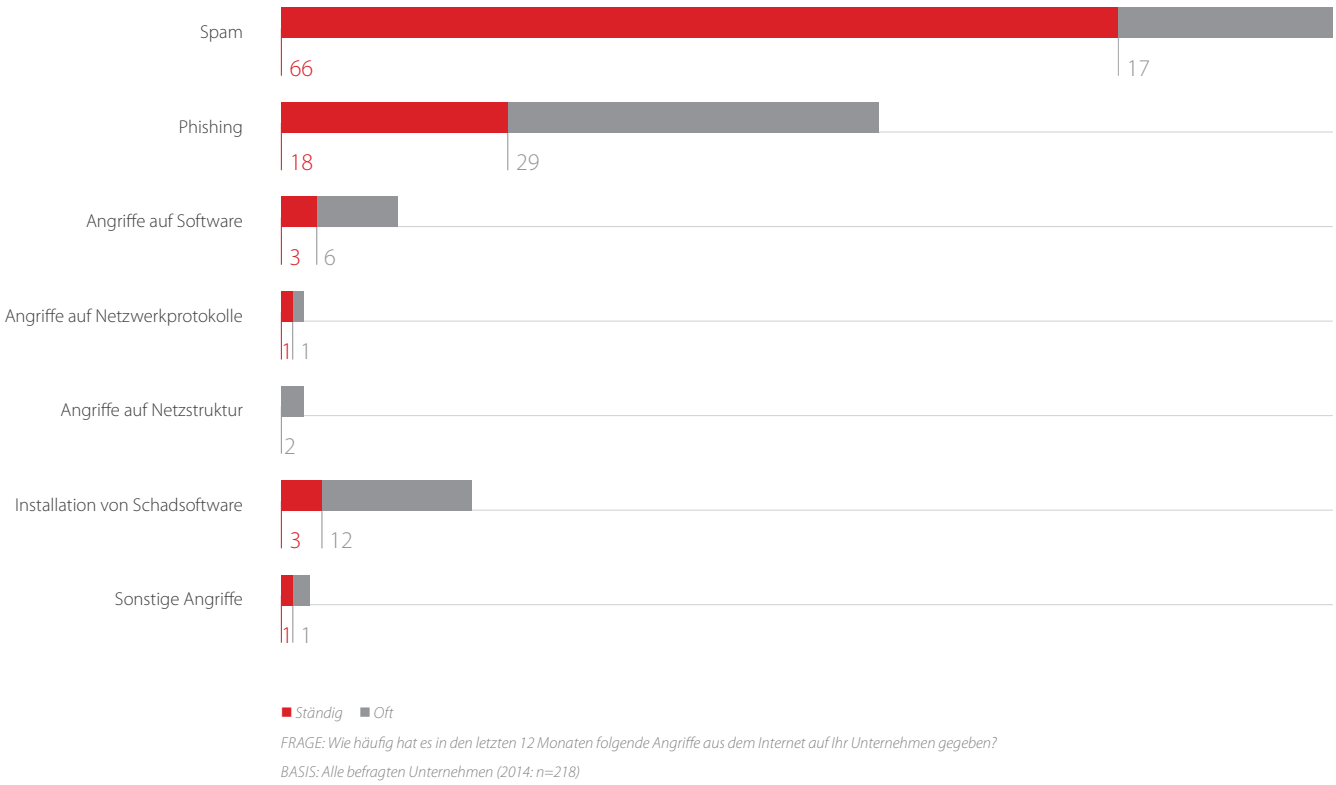
*FRAGE: Für wie wahrscheinlich halten Sie es, dass die folgenden Personen/Institutionen die IT-Systeme Ihres Unternehmens angreifen?*

*BASIS: Alle befragten Unternehmen (2014: Ja: n=78; Nein: n=140)*

# Häufigkeit von Angriffen aus dem Internet (2014)

## Spam und Phishing sind häufigste Angriffsformen

**Häufigkeit von Angriffen**



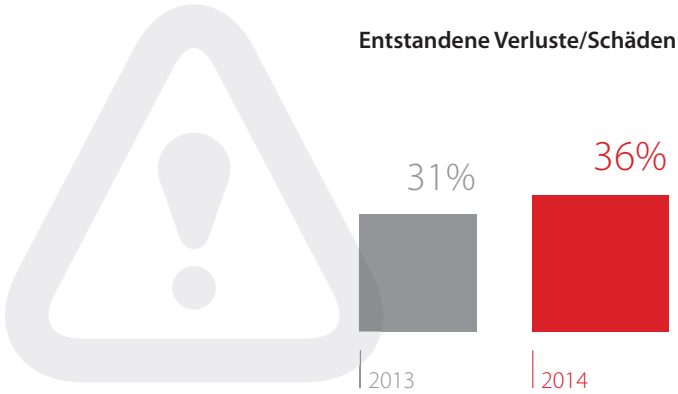

*FRAGE: Wie häufig hat es in den letzten 12 Monaten folgende Angriffe aus dem Internet auf Ihr Unternehmen gegeben?*

*BASIS: Alle befragten Unternehmen (2014: n=218)*

Betrachtet man die Häufigkeit von Cyberangriffen auf die befragten Unternehmen in den letzten zwölf Monaten, so zeigt sich ein differenziertes Bild: Die mit Abstand häufigsten Angriffe beziehen sich auf Spam (83 Prozent der Befragten schätzen die Häufigkeit als „ständig" oder „oft" ein), gefolgt von Phishing (47 Prozent), Installation von Schadsoftware (15 Prozent) und Angriffe auf Software (neun Prozent). Sonstige Angriffe, insbesondere auch auf Netzprotokolle und Netzstruktur, kommen vergleichsweise selten vor.

# Entstandene Verluste/Schäden durch Angriffe aus dem Internet

**Entstandene Verluste/Schäden 2013/2014**




*FRAGE: Welche Verluste/Schäden sind in Ihrem Unternehmen in den letzten 12 Monaten durch Computerschädlinge oder Angriffe aus dem Internet entstanden?*
*BASIS: Alle befragten Unternehmen (2014: n=218; 2013: n=90)*

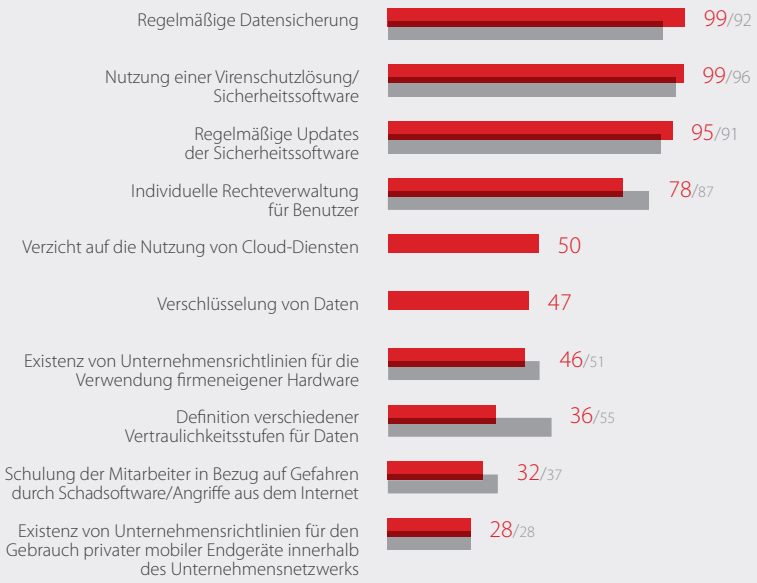
Mehr als ein Drittel (36 Prozent) der befragten Unternehmen vermeldet 2014 Verluste bzw. Schäden durch Angriffe aus dem Internet, dies sind fünf Prozentpunkte mehr im Vergleich zum Vorjahr. Vor allem Betriebsstörungen und -unterbrechungen kommen sehr häufig vor (83 Prozent der entstandenen Verluste/Schäden). Übertragen auf die Unternehmenslandschaft in Deutschland lässt sich folgern, dass knapp 30 Prozent von Betriebsstörungen betroffen sind. Wenn man dies wiederum umrechnet in entgangene Arbeitszeit, lässt sich der Schaden für die Wirtschaft schnell zu hohen Summen addieren.

Mit weitem Abstand folgen die Beschädigung von Betriebsmitteln und Geräten (26 Prozent), der Verlust von Daten (12 Prozent), die Kosten für Rechtsstreitigkeiten (neun Prozent) und die Schädigung des Images (acht Prozent). Dabei zeigt sich im Vergleich zur Vorjahresstudie eine z. T. deutliche Steigerung der einzelnen Werte, wie die Grafik verdeutlicht.

# Ergriffene Maßnahmen gegen Angriffe aus dem Internet

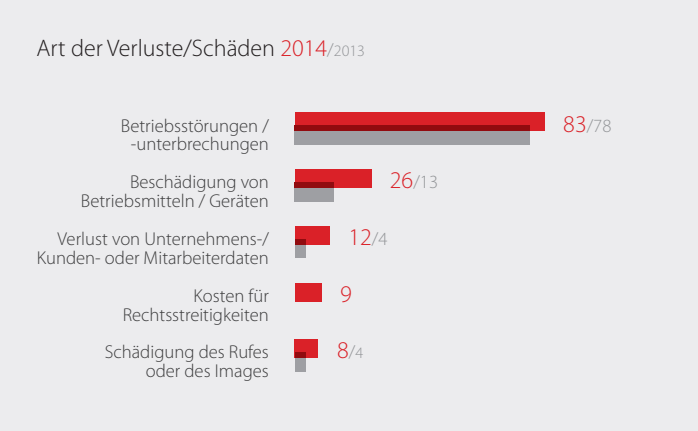
(Fast) alle Unternehmen, die an der Befragung teilgenommen haben, ergreifen Maßnahmen gegen Angriffe aus dem Internet. Hierzu gehören insbesondere eine regelmäßige Datensicherung (99 Prozent der Unternehmen tun dies), die Nutzung einer Virenschutzlösung/Sicherheitssoftware (99 Prozent), regelmäßige Updates der Sicherheitssoftware und der im Unternehmen genutzten Software (jeweils 95 Prozent). Im

**Ergriffene Maßnahmen (Auswahl)**



Je mehr Geld Unternehmen in Sicherheitssoftware investieren, desto geringer sind die Verluste bzw. Schäden, welche sie zu verzeichnen haben. Bei Unternehmen, die bis zu 1.000 € für Sicherheitssoftware ausgeben, liegt der Anteil der Geschädigten noch bei 42 Prozent. Bei Unternehmen mit Ausgaben zwischen 1.000 und 5.000 € sinkt er bereits leicht auf 39 Prozent und bei Firmen mit Investitionen von mehr als 5.000 € für Sicherheitssoftware beträgt der Anteil nur noch ein Drittel.

**Entstandene Verluste/Schäden (Top 5)**

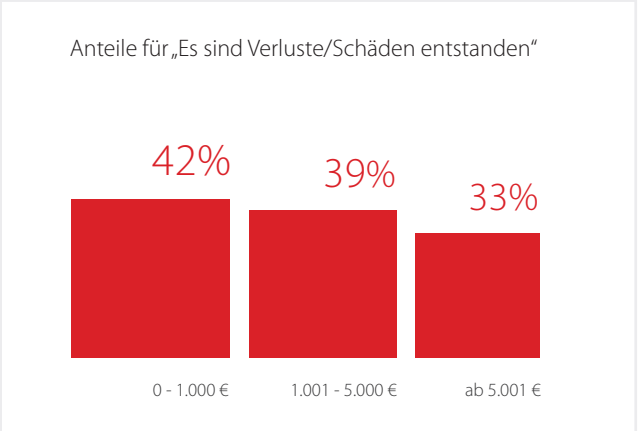



*2014 2013*

*FRAGE: Welche Verluste/Schäden sind in Ihrem Unternehmen in den letzten 12 Monaten durch Computerschädlinge oder Angriffe aus dem Internet entstanden?*

*BASIS: Alle befragten Unternehmen mit Verlusten/Schäden (2014: n=78; 2013: n=26)*

**Verluste/Schäden nach Aufwand Sicherheitssoftware**




*Verluste/Schäden*

*FRAGE: Welche Verluste/Schäden sind in Ihrem Unternehmen in den letzten 12 Monaten durch Computerschädlinge oder Angriffe aus dem Internet entstanden? (Darstellung der Anteile für „Es sind Verluste/Schäden entstanden“)*

*BASIS: Alle befragten Unternehmen mit den jeweiligen Aufwänden für Sicherheitssoftware 2014: 0-1.000 €: n=50; 1.001-5.000 €: n=70; ab 5.001 €: n=75)*

*2014 2013*

*FRAGE: Welche Maßnahmen werden in Ihrem Unternehmen ergriffen, um sich vor Computerschädlingen oder Angriffen aus dem Internet zu schützen? (Mehrfachantworten möglich)*

*BASIS: Alle befragten Unternehmen (2014: n=218; 2013: n=90)*

**„Standardmaßnahmen“ wie Updates und Datensicherung werden in fast allen Firmen ergriffen und auch häufiger als 2013, jedoch gibt es Nachholbedarf bei weitergehenden Maßnahmen.**

Vergleich zum Vorjahr sind die Anteile um bis zu sieben Prozentpunkte höher, was auf ein gestiegenes Bewusstsein für IT-Sicherheit hindeutet.

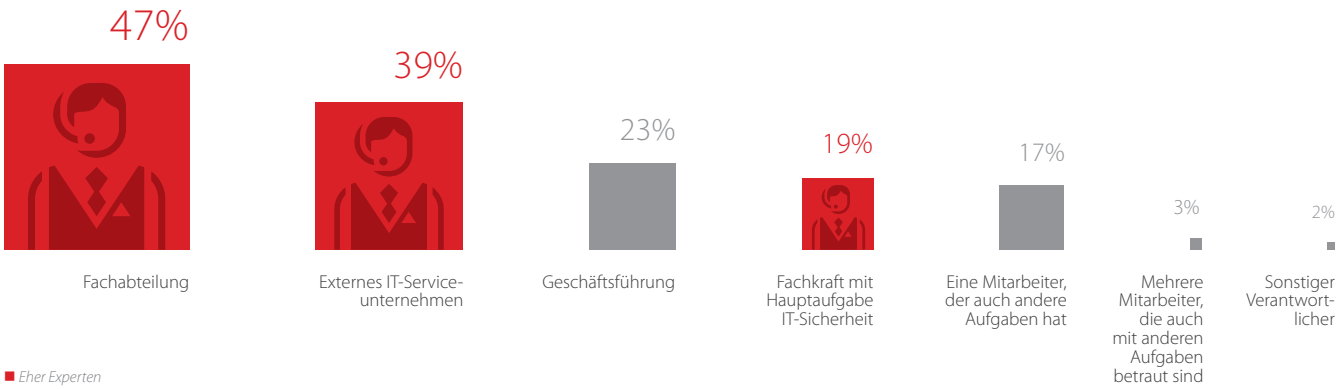
Allerdings gibt es auch weniger verbreitete Maßnahmen, bei denen die Nutzung im Vergleich zu 2013 auch zurückging. Z. B. werden die individuelle Rechteverwaltung für Benutzer (2014: 78 Prozent; 2013: 87 Prozent), die Definition verschiedener Vertraulichkeitsstufen von Daten (2014: 36 Prozent; 2013: 55 Prozent) und auch die Schulung der Mitarbeiter in Bezug auf Internetgefahren (2014: 32 Prozent; 2013: 37 Prozent) von den befragten Unternehmen seltener ergriffen.

So lässt sich das Resumee ziehen, dass zwar die „Standardmaßnahmen“ wie regelmäßige Softwareupdates und Datensicherung weit verbreitet sind, es aber zur Erhöhung der Sicherheit durchaus Nachholbedarf an anderer Stelle gibt.

# Verantwortlicher für IT-Sicherheit (2014)

## Nicht in allen Firmen sind Experten (  ) für IT-Sicherheit verantwortlich

**Verantwortlicher für IT-Sicherheit**




*Eher Experten*

*Eher keine Experten*

*FRAGE: Wer kümmert sich in Ihrem Unternehmen um IT-Sicherheit? (Mehrfachantworten möglich)*

*BASIS: Alle befragten Unternehmen (2014: n=218)*

Knapp die Hälfte (47 Prozent) der befragten Unternehmen hat eine eigene Fachabteilung, welche sich mit dem Thema IT-Sicherheit befasst und in 39 Prozent der Fälle wird ein externes IT-Serviceunternehmen beauftragt. Die Geschäftsführung ist bei 23 Prozent der Unternehmen involviert und bei knapp einem Fünftel (19 Prozent) der Firmen ist eine Fachkraft mit Hauptaufgabe IT-Sicherheit in der Verantwortung. In 17 Prozent der Fälle kümmert sich ein Mitarbeiter, der auch andere Aufgaben hat, um dieses Thema.

Für einige Firmen wäre deshalb eine Professionalisierung dieses Themas ratsam. Dies gilt vor allem für Unternehmen, in denen das Thema IT-Sicherheit von Mitarbeitern nebenbei mitbetreut wird, obwohl an dieser Stelle aufgrund der hohen aktuellen Bedeutung eine eindeutige Verantwortlichkeit und ein fundiertes Expertenwissen notwendig wäre.

# Bewertung verschiedener Aussagen

Im Rahmen der Befragung wurden auch verschiedene allgemeine Statements zum Verhalten am firmeneigenen Computer und zu IT-Sicherheit im Unternehmen erhoben. Auch hier zeigt sich bei vielen Aussagen eine erhöhte Sensibilität für das Thema Cybersicherheit, wenngleich es an vielen Stellen noch Nachholbedarf gibt.

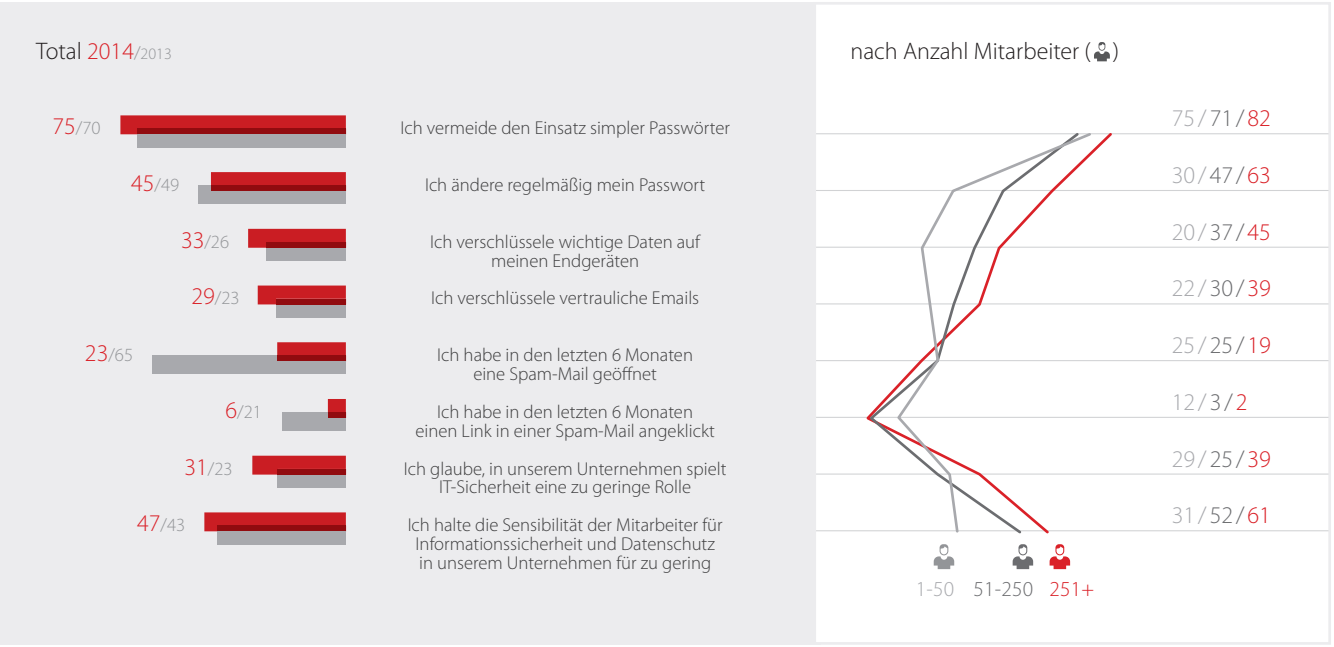
So werden z. B. Verschlüsselungen bisher noch von wenigen IT-Verantwortlichen in den Unternehmen genutzt, allerdings kommt dies im Vergleich zum Vorjahr etwas häufiger vor (Verschlüsselung von Daten auf Endgeräten: Aktuell macht dies ein Drittel – eine Steigerung um sieben Prozentpunkte; Verschlüsselung von E-Mails: Aktuell 29 Prozent, Vorjahr 23 Prozent). Das Thema Verschlüsselung wird von den Befragten umso ernster genommen, je größer die jeweiligen Unternehmen sind: Bei Firmen mit 1-50 Mitarbeitern verschlüsselt nur ein Fünftel der Befragten Daten auf Endgeräten, bei Unternehmen mit 51-250 Mitarbeitern sind es bereits 37 Prozent und bei Betrieben mit mehr als 250 Mitarbeiter verschlüsseln 45 Prozent der IT-Verantwortlichen ihre Daten.

Nachholbedarf gibt es auch im Umgang mit Passwörtern: Aktuell ändern nur etwas weniger als die Hälfte (45 Prozent) der Befragten regelmäßig Passwörter, immerhin vermeiden drei Viertel den Einsatz simpler Passwörter. Dies ist nur ein geringer Anstieg zur letztjährigen Erhebung (70 Prozent haben 2013 angegeben, den Einsatz simpler Passwörter zu vermeiden). Beim regelmäßigen Ändern von Passwörtern ist sogar ein Rückgang im Vergleich zur ersten Welle sichtbar (2013 waren es 49 Prozent). Betrachtet man diese Aussage nach der Anzahl der Mitarbeiter, so zeigt sich ein eindeutiger Trend: Je höher die Anzahl der Mitarbeiter im Unternehmen, desto regelmäßiger werden Passwörter geändert (1-50 Mitarbeiter: Hier ändern 30 Prozent der Befragten regelmäßig ihr Passwort; 51-250 Mitarbeiter: 47 Prozent; mehr als 250 Mitarbeiter: 63 Prozent). Hintergrund dieses Verhaltens kann eine professionellere IT-Struktur, wie es sie in größeren Unternehmen gibt, sein.

Deutlich ist das Bewusstsein beim Umgang mit Spam-Mails gestiegen. Hier haben in der Umfrage 2014 nur 23 Prozent der Befragten eine Spam-Mail geöffnet und nur sechs Prozent haben gar einen Link in einer Spam-Mail angeklickt. 2013 waren dies noch 65 bzw. 21 Prozent.

Bezüglich der IT-Sicherheit im Unternehmen gehen aktuell 31 Prozent der Befragten davon aus, dass diese eine zu geringe Rolle spielt (2013: 23 Prozent) und fast die Hälfte (47 Prozent) der Befragten hält die Sensibilität der Mitarbeiter für Informationssicherheit und Datenschutz im jeweiligen Unternehmen für zu gering (Vorjahr: 43 Prozent). Diese Haltung ist umso ausgeprägter, je größer das Unternehmen ist: Bei Unternehmen mit 1-50 Mitarbeiter halten nur 31 Prozent der Befragten die Sensibilität für Sicherheitsthemen für zu gering, bei 51-250 Mitarbeitern sind es bereits über die Hälfte (52 Prozent) und bei Firmen mit mehr als 250 Mitarbeiter sind es 61 Prozent. Dies ist ein sehr erstaunliches Ergebnis und deutet darauf hin, dass die befragten IT-Verantwortlichen in größeren Unternehmen umso kritischer sind, weil sie sich der wachsenden und überall lauernden Gefahren deutlich bewusster sind.

**Verhalten am firmeneigenen Computer**




2014 2013

*Top-2-Nennungen („Trifft voll und ganz zu"/„Trifft eher zu")*

*FRAGE: Bitte geben Sie an, inwiefern die folgenden Aussagen auf Ihr Verhalten am firmeneigenen Computer zutreffen.*

*BASIS: Alle befragten Unternehmen (2014: n=218; 2013: n=90)*

1-50 Mitarbeiter 51-250 Mitarbeiter 251+ Mitarbeiter

*Top-2-Nennungen („Trifft voll und ganz zu"/„Trifft eher zu")*

*FRAGE: Bitte geben Sie an, inwiefern die folgenden Aussagen auf Ihr Verhalten am firmeneigenen Computer zutreffen.*

*BASIS: Alle befragten Unternehmen (2014: 1-50 Mitarbeiter: n=77; 51-250: n=73; 251+: n=62)*

**IT-Sicherheit, Datensicherheit und Datenschutz** müssen in der digitalen Welt weiterhin an oberster Stelle stehen. Das Schadenspotenzial hier ist enorm und das Bewusstsein für dieses Thema in der Wirtschaft und in der Gesellschaft muss weiter geschärft werden.

## Impressum


**HERAUSGEBER**
**G DATA Software AG**
www.gdata.de
Ansprechpartner: Robert Niesbach
*robert.niesbach@gdata.de*

**VERANTWORTLICH FÜR DEN INHALT (PROJEKTLEITUNG)**
**TNS Deutschland GmbH**
www.tns-infratest.com
Ansprechpartner: Michael Boberach
*michael.boberach@tns-infratest.com*

**GESTALTUNG UND PRODUKTION**
**Werkstatt für visuelle Kommunikation**
www.werkstatt-trier.de
Silke Wohner, Stefanie Brendle i. A.