2011 | 2012 | 2013 | 2014

DsiN SICHERHEITS MONITOR

MITTELSTAND

IT-Sicherheitslage 2014
in Deutschland

Schirmherrschaft:
Bundesministerium des Innern

DEUTSCHLAND DsiN.de SICHER IM NETZ

Prof. Dieter Kempf

Dr. Michael Littger

Mehr Engagement für IT-Sicherheit!

Deutschland sicher im Netz beobachtet seit vier Jahren die Entwicklung der IT-Sicherheitslage im Mittelstand. Grundlage ist der DsiN-Sicherheitscheck, den in den vergangenen 12 Monaten wieder 1.500 Unternehmen nutzten: als kostenfreies Angebot mit einem fundierten Überblick zu IT-Sicherheitsfragen.

Die diesjährige Auswertung zeigt, dass die Verbreitung von IT in allen Geschäftsprozessen weiter deutlich zulegt – die notwendigen Sicherheitsmaßnahmen aber nicht immer Schritt halten, im Gegenteil. Gemessen an der gestiegenen Relevanz und Verbreitung von IT sind Aktivitäten der Unternehmen teilweise sogar rückläufig.

Dabei fällt ein Paradox ins Auge: Obwohl Sicherheitsfragen in Unternehmen als wichtig empfunden werden – auch im Lichte der NSA-Enthüllungen – mangelt es an einer wirksamen Umsetzung. Unkenntnis, organisatorische Defizite sowie Überforderung spielen eine Rolle – bei der Sicherung des elektronischen Mail-Verkehrs bis zum mobilen Internet.

Insgesamt deutet die IT-Sicherheitslage im Mittelstand auf einen umfassenden Handlungsbedarf hin, insbesondere bei kleinen und kleinsten Betrieben. Ganzheitliche IT-Sicherheitskonzepte und organisatorische Maßnahmen, eine Sensibilisierung von Mitarbeitern sowie auch technische Vorkehrungen sind zu selten tägliche Praxis.

Der DsiN-Sicherheitsmonitor zeigt konkrete Handlungsfelder auf – für mehr IT-Sicherheitsbewusstsein und -maßnahmen im Mittelstand. Es geht um die Verantwortung aller Beteiligten, die einen Beitrag zur Aufklärung leisten können, um ein koordiniertes Engagement der IT-Wirtschaft, der Politik – und nicht zuletzt der betroffenen Unternehmen!

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Prof. Dieter Kempf
Beirat Deutschland sicher im Netz e.V.
Vorsitzender des Vorstands DATEV eG

Dr. Michael Littger
Geschäftsführer Deutschland sicher im Netz e.V.

Studienziel

Der „DsiN-Sicherheitsmonitor Mittelstand“ untersucht die Sicherheitslage in kleinen und mittleren Unternehmen und identifiziert Schwachstellen, um daraus kommunikative Maßnahmen zu entwickeln, die das Sicherheitsbewusstsein in Unternehmen nachhaltig stärken.

2011

2012

2013

2014

Der Untersuchungszeitraum über mehrere Jahre – seit 2011 – ermöglicht eine zuverlässige Betrachtung der IT-Sicherheitslage. Nachhaltige IT-Sicherheitstrends werden identifiziert, so dass vorübergehende Ereignisse mit kurzfristigen Ausschlägen besser eingeordnet werden können. Im Fokus stehen Risiko- und Sicherheitsbewusstsein auf der einen und die konkret getroffenen Maßnahmen im Unternehmen auf der anderen Seite.

Auf dieser Grundlage ermittelt die Studie Themenfelder im Mittelstand und entwickelt daraus Empfehlungen zur Verbesserung der IT-Sicherheitslage. Sie betreffen Handlungsbereiche, in denen Geschäftsführer und Mitarbeiter in Deutschland konkret befähigt werden, sicherheitsrelevante Maßnahmen aktiv zu ergreifen. Damit leistet die Studie einen eigenen Beitrag zur konkreten Verbesserung der IT-Sicherheitslage.

Inhalt

Untersuchungsdesign

Vorschlag: Die kontinuierliche Befragung von mittelständischen Unternehmen über den Zeitraum von April 2011 bis März 2014 über den IT-Sicherheitscheck von DsiN ermöglicht einen aussagekräftigen Vergleich der Umfragedaten.

6.000

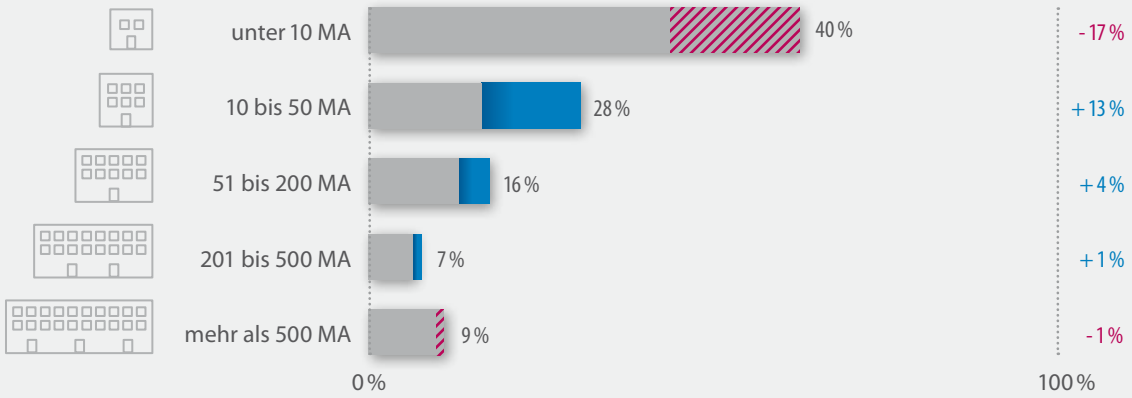
Unternehmen, die seit 2011 mittels standardisiertem Online-Fragebogen befragt wurden.

Der „DsiN-Sicherheitsmonitor Mittelstand" zeigt im Jahresvergleich auf, wie und auf welchem Sicherheitsniveau Unternehmen digitale Dienste und Geräte nutzen. Die Schwerpunkte sind IT-Infrastruktur und IT-Management, Internet- und E-Mail-Nutzung, Mobile Business sowie Datenschutz.

Seit 2011 wurden rund 6.000 Unternehmen mittels standardisiertem Online-Fragebogen in anonymisierter Form befragt. Von April 2013 bis März 2014 nahmen 1.519 Nutzer an der Umfrage teil. Zeitraum, Fragen und Teilnehmerzahl waren nahezu identisch mit der Basis der DsiN-Sicherheitsstudie 2011, was einen validen Zeitreihenvergleich der Ergebnisse aus beiden Jahren ermöglicht. Teilnehmer der Befragung sind überwiegend Unternehmen mit bis zu 50 Mitarbeitern. Davon erhöhte sich im Betrachtungszeitraum die Größenklasse von 10-50 Mitarbeitern um 13 Prozentpunkte auf 28 %, während sich der Anteil der ganz kleinen Unternehmen von 57 % auf 40 % reduzierte. Mit einem Zuwachs von 4 % nutzen auch zunehmend größere KMU mit bis zu 200 Mitarbeitern den Sicherheitscheck (Grafik 1).

Der Fragenkatalog des IT-Sicherheitschecks wurde von Deutschland sicher im Netz e.V. mit Unterstützung von BITKOM, DATEV, SAP und Sophos entwickelt. Mit dem DsiN-Sicherheitscheck können sich Unternehmen ein Bild von IT-Sicherheit verschaffen und erhalten geeignete Handlungsempfehlungen. www.sicher-im-netz.de/dsin-sicherheitscheck.de

Befragte Untermehmen nach Anzahl der Mitarbeiter



Grafik 1 03/2014 03/2014 Zunahme 03/2014 Abnahme

Die Ausgangslage: Der digitale Geschäftsalltag

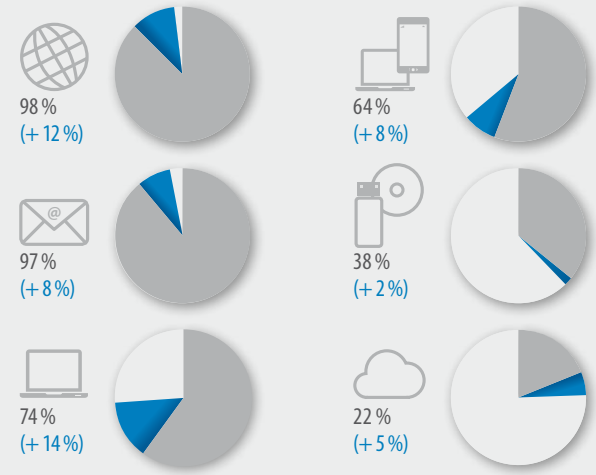
Der Digitalisierungsgrad bei kleinen und mittelständischen Unternehmen ist seit März 2011 in allen Bereichen erwartungsgemäß erheblich angestiegen – von Internet- und E-Mail-Nutzung bis zur Verwendung mobiler Endgeräte.

Die Nutzungsmöglichkeiten des Internets sind in nahezu allen Unternehmen angekommen und werden praktisch gelebt (98 %). E-Mail-Kommunikation findet mittlerweile in 97 % der Unternehmen statt. Die deutlich gestiegene Verbreitung von Notebooks um 14 %, von Smartphones/Netbooks um 8 % und von Cloud-Computing um 5 % bestätigen den Digitalisierungstrend auf breiter Front (Grafik 2).

Auch die mobile Anbindung der Kommunikation an die Unternehmensnetze hat sich nochmals verstärkt (Grafik 3). Besonders signifikant ist die Veränderung bei der Postfach- und Kalendersynchronisation um 22 % und der direkte Zugriff aufs Firmennetzwerk um 15 %. Die Anzahl der Unternehmen, die überhaupt keinen externen Zugriff anbieten, ist hingegen im selben Zeitraum deutlich zurückgegangen (16 %).

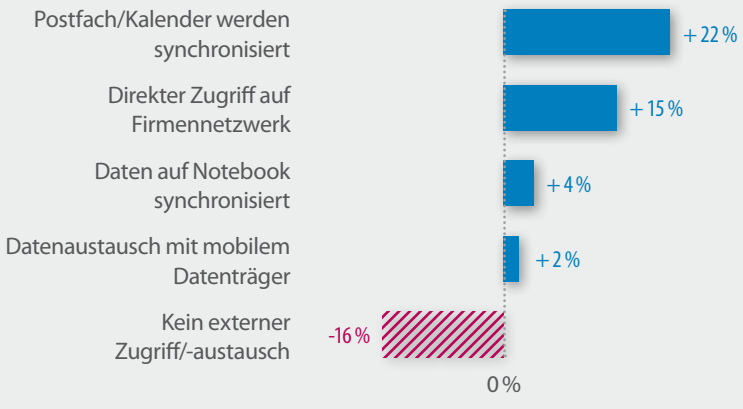
Im Ergebnis steht damit eine deutlich steigende digitale Vernetzung auf allen Ebenen, die auch auf eine steigende Relevanz der IT-Sicherheit in Unternehmen hinweist.

Wachsende Digitalisierung des Geschäftsalltags



Grafik 2

Veränderungen bei der Art des mobilen Zugriffs auf das Unternehmensnetzwerk zum Vergleichsjahr 2011



Grafik 3

-14 %

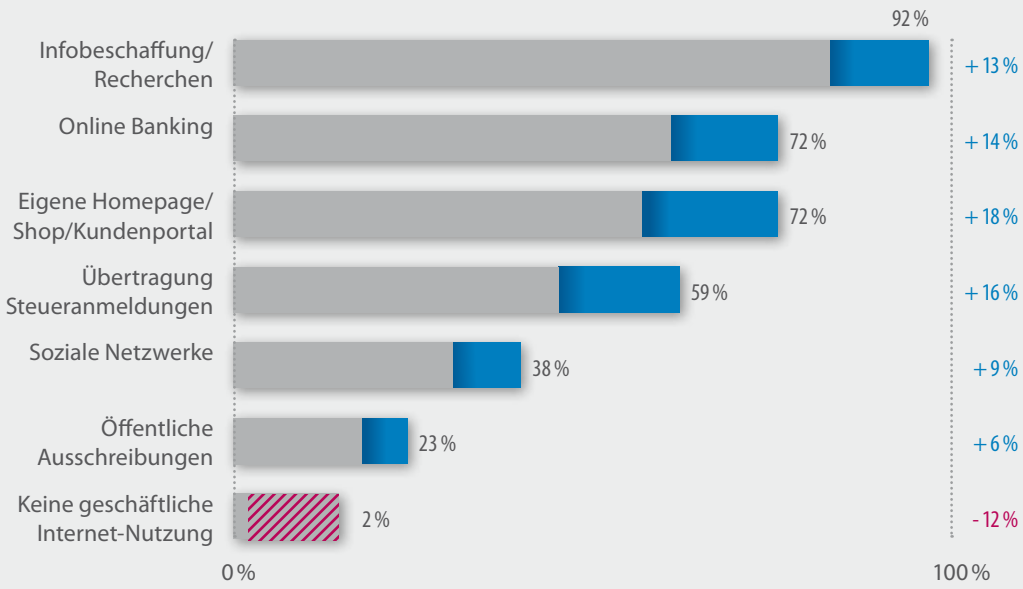
Rückgang der Unternehmen, die keinen Zugriff aufs eigene Netzwerk anbieten.

Ein weiterer Trend ist, dass auch die in Unternehmen verwendeten Dienste seit 2011 stärker genutzt wurden (Grafik 4):

- Recherchearbeiten sind für 92 % der Befragten unabdingbar geworden und haben damit nochmals um 13 % seit 2011 zugelegt.
- Online-Banking ist deutlich um 14 % angestiegen, ebenso die Verwendung eigener Websites und Kundenportale um 18 % auf jeweils 72 %.
- Steuermeldungen werden von 59 % der Nutzer elektronisch übertragen – mit stark steigender Tendenz.

Insgesamt werden auch deutlich mehr schützenswerte und sensible Informationen über Internet und E-Mail geschäftlich verarbeitet und versendet (Grafik 8 / S. 15). Die Zahl der Nichtnutzer des Internets im Geschäftsalltag tendiert heute nun gegen Null (2011: 14 %).

Veränderung der geschäftlichen Nutzung des Internets



Grafik 4 03/2014 03/2014 Zunahme 03/2014 Abnahme

Digitalisierung steigt – Sicherheitsbewusstsein sinkt

Das Sicherheitsbewusstsein hält mit dem Digitalisierungszuwachs – auf der Basismessung 2011 – nicht Schritt, ist teilweise sogar rückläufig (Grafik 5). Deuteten die Zwischenmessungen in den letzten drei Jahren noch eine positive Tendenz an, so hat sich diese nicht fortgesetzt. Größere Unternehmen verfügen über mehr Schutzmaßnahmen als kleinere, die Schwachstellen sind aber vergleichbar.

Zwar hat sich der reine Internetschutz über die vergangenen Jahre gut etabliert: Firewalls, Virenscannern, Spamfiltern gehören in Unternehmen heute mit über 90% zur Regel. Ein systematischer Einsatz weiterer Sicherheitstechnologien (Brennpunkt 1) sowie eine Sensibilisierung von Mitarbeitern (Brennpunkt 2) stehen dahinter aber deutlich zurück.

Besonders problematisch erweist sich die mangelnde Sicherheit der E-Mail-Kommunikation (Brennpunkt 3) und Absicherung mobiler Geräte (Brennpunkt 4). Als wichtiger Trend wird seit 2012 auch die Entwicklung des Cloud Computing beobachtet, wobei die Auseinandersetzung mit grundlegenden Sicherheitsanforderungen noch wenig ausgeprägt ist (Brennpunkt 5).

Die Brennpunkte

- Ganzheitliche IT-Sicherheitskonzepte
- Sensibilisierung der Mitarbeiter
- Sichere Kommunikation und E-Mail-Verkehr
- Schutzmaßnahmen für mobile Geräte
- Supertrend Cloud Computing

Ganzheitliche IT-Sicherheitskonzepte

Sicherheitsvorkehrungen bedürfen verbesserter Abstimmung, um die Wirksamkeit zu erhöhen.

98 %

einfache Schutzmaßnahmen wie Internetschutz und Einspielen von Sicherheitsupdates sind fast in jedem Unternehmen üblich.

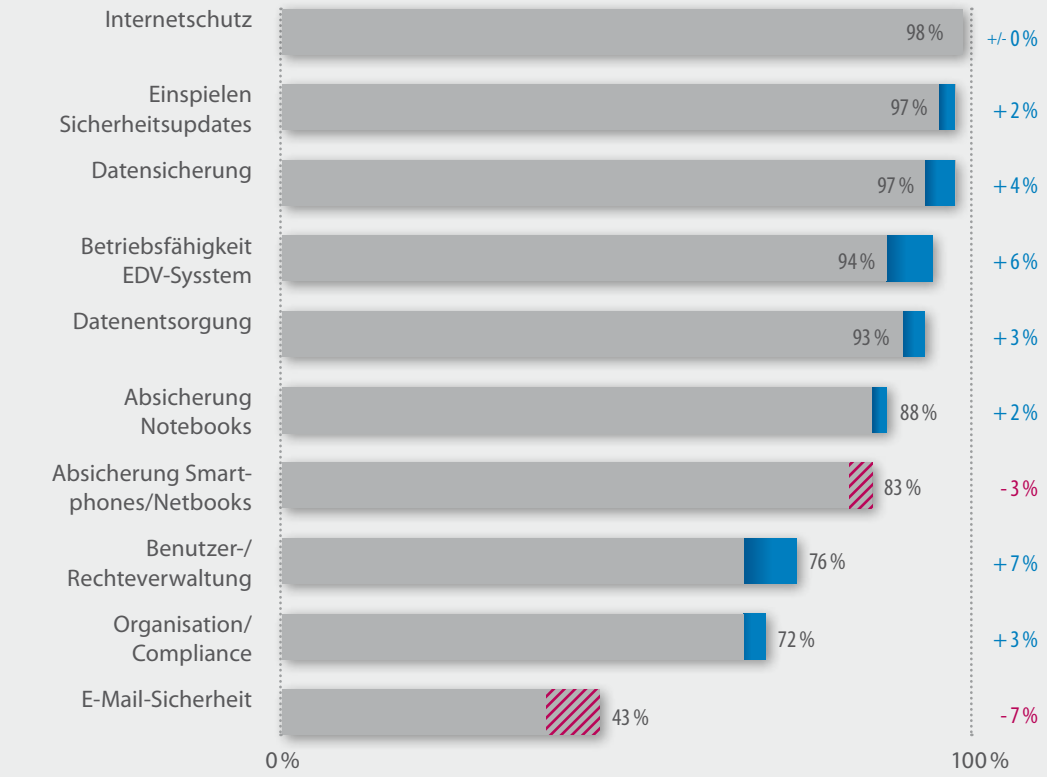
Einer teilweise erfreulich hohen Verbreitung von IT-Sicherheitsmaßnahmen stehen deutliche Defizite gegenüber. Daraus leitet sich die Frage ab, inwieweit die Maßnahmen einem ganzheitlichen IT-Sicherheitskonzept entspringen und aufeinander abgestimmt sind.

Erfreulich ist, dass die Datensicherung sowie auch das Einspielen von Sicherheitsupdates mit 97 % heute nahezu vollständig verbreitet ist (2011: 93 bzw. 95 %). Auch der reine Internet-Schutz etwa durch Firewalls liegt unverändert hoch bei 98 %. Eine sichere Datenentsorgung im Unternehmen geben 93 % an – eine Steigerung um 3 % gegenüber 2011.

Alarmierend ist hingegen die schwache Verbreitung sicherer E-Mail-Kommunikation mit nur 43 %. Sie ist gegenüber den Vorjahren sogar rückläufig (2011: 50 %). Auch die organisatorischen Maßnahmen für IT-Sicherheit zeigen mit 72 % erheblichen Nachholbedarf (2011: 69 %). Dasselbe gilt für die Einhaltung von sicherheitsrelevanten Rechtsvorschriften.

Insgesamt weist das Lagebild auf eine Vernachlässigung ganzheitlicher IT-Sicherheitskonzepte hin. Dieser Eindruck wird bestärkt, da ein von der Geschäftsleitung getragenes gesamtheitliches IT-Sicherheitskonzept in nur 32 % der Unternehmen gegeben ist. 57 % der Unternehmen haben die Verantwortlichkeit geregelt (siehe Grafik 7, S. 13). So entsteht der Eindruck, dass die Unternehmen fälschlicherweise glauben, das Thema damit gelöst zu haben.

Vorhandene IT-Schutzmaßnahmen



Grafik 5 03/2014 03/2014 Zunahme 03/2014 Abnahme

-7%

Die E-Mail-Kommunikation verläuft nur noch bei 43 % aller befragten Unternehmen in sicheren Bahnen.

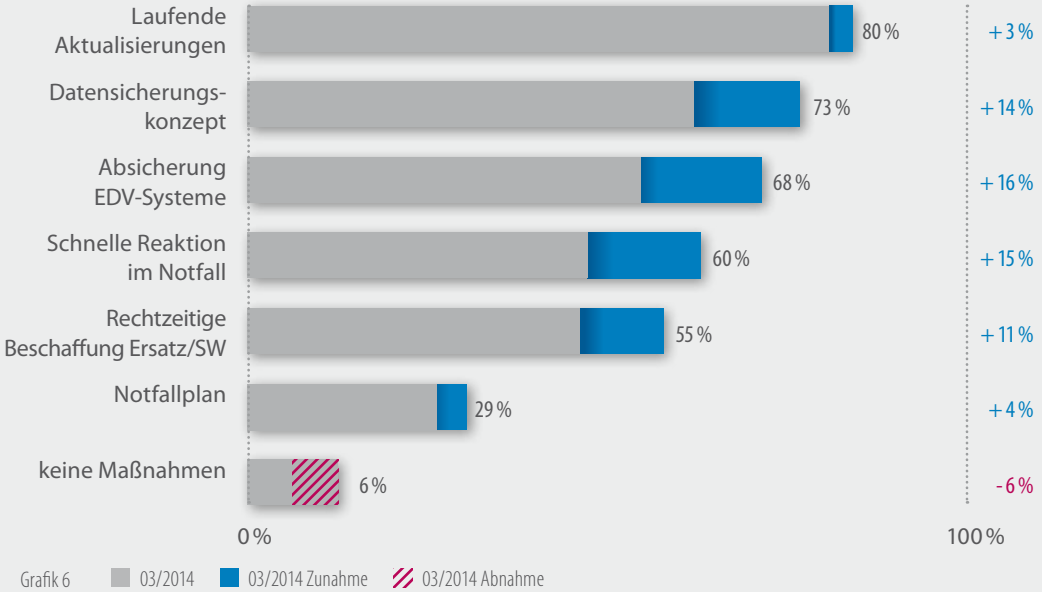
Schwerpunkt: Datensicherungskonzept:

Bei näherer Betrachtung der Betriebe, die eine vorhandene Sicherung ihrer Daten angeben (97 %) ergibt sich ein differenziertes Bild. Zwar gab es gegenüber 2011 in allen Bereichen Zuwachs. Dennoch verharrt die Anzahl derer, die ein Notfallkonzept vorhalten, bei unter 30 %. Auch die Reaktionszeiten im Notfall geben nur 60 % der Betriebe als „schnell" an. Über eine allgemeine Absicherung der EDV-Systeme verfügen nur zwei Drittel der Unternehmen.

80%

der Befragten, die über ein Datensicherungskonzept verfügen, erklären, die Daten täglich oder permanent zu sichern. Die Prüfung der Funktionsfähigkeit der Datensicherung erfolgt hingegen nur zu 41 % regelmäßig, knapp die Hälfte (48 %) prüft die Funktionsfähigkeit nur teilweise, 11% verzichten.

Maßnahmen zur Erhaltung der Betriebsfähigkeit der EDV



Grafik 6 03/2014 03/2014 Zunahme 03/2014 Abnahme

2 Sensibilisierung der Mitarbeiter

Kaum Verbesserung der organisatorischen Maßnahmen in Unternehmen

1/3

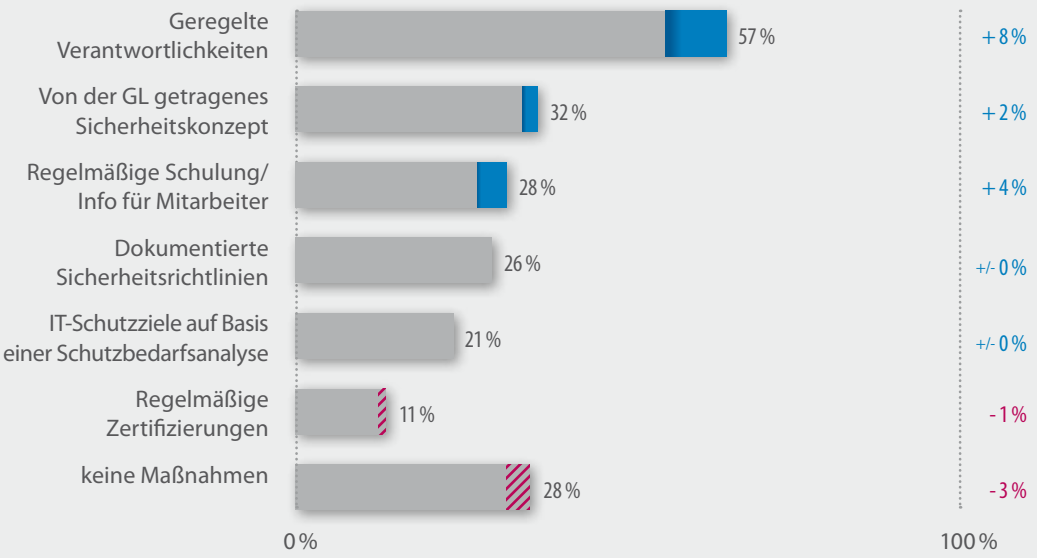
der Unternehmen haben keine Personen mit der Verantwortung für IT-Sicherheit betraut

Die Vorkehrungen für eine Sensibilisierung von Mitarbeitern verharren auf relativ niedrigem Niveau mit starken Defiziten bei organisatorischen Vorkehrungen

Nur 28 % der Unternehmen bieten regelmäßige Informationen und Schulungen zum sicherheitsbewussten Verhalten für ihre Mitarbeiter an (2011: 24 %). Über dokumentierte Sicherheitsrichtlinien verfügen nur 26 %. Dies kommt einem Stillstand seit 2011 gleich. Ins Gewicht fällt zudem, dass 28 % der Unternehmen angeben, überhaupt „keine organisatorischen Maßnahmen" zu ergreifen (2011: 31 %).

Aber auch bei Unternehmen, die über ganzheitliche Sicherheitskonzepte mit Mitarbeitermaßnahmen verfügen, fällt auf, dass sie nur ausnahmsweise von der Geschäftsführung getragen werden (2014: 32 %, 2011: 30 %). Hingegen sorgen inzwischen mehr Unternehmen für geregelte Verantwortlichkeiten, z.B. durch Berufung eines Datenschutzbeauftragten. Der Wert stieg um 8 Prozentpunkte auf 57 %. Damit verfügen heute ein Drittel der Unternehmen aber immer noch über keine geregelte Verantwortlichkeiten.

Organisatorische Maßnahmen zu Datenschutz und IT-Sicherheit



Grafik 7 03/2014 03/2014 Zunahme 03/2014 Abnahme

Die Rolle der Mitarbeiter wird unterbewertet.

Die Defizite bei der Sensibilisierung von Mitarbeitern werden durch die Tatsache untermauert, dass sich die Vorkehrungen für Compliance im Unternehmen mit 72 % kaum verbessert haben (Grafik 5, S. 11). Diese dienen der Einhaltung sicherheitsrelevanter Regeln und Gesetze.

Insgesamt wird die Rolle der Mitarbeiter für IT-Sicherheit im Unternehmen als zentraler Sicherheitsfaktor damit deutlich unterschätzt. Dies kann enorme Sicherheitsrisiken im Unternehmen verursachen. Denn praktisch jeder Mitarbeiter kommt in seiner täglichen Arbeit mit sensiblen Daten in Berührung.

Mögliche Gründe können ein mangelndes Bewusstsein der Unternehmensleitung sein, dass Mitarbeiter eine der größte Gefahrenstelle für Angriffe von außen sowie auch von innen sind. Auch entsteht der Eindruck, dass Unternehmen mit der Berufung von Verantwortlichen möglicherweise schon glauben, das Thema ausreichend behandelt zu haben.

Vor allem aber könnten Unternehmen schlichtweg überfordert sein, geeignete Maßnahmen für eine ausreichende Mitarbeitersensibilisierung über organisatorische Vorkehrungen zu treffen. Sowohl bei der Bewusstseinsbildung auf Entscheider- und Mitarbeiterebene als auch in der Umsetzungskompetenz bestehen damit erhebliche Aufklärungsaufgaben.

89 %

aller befragten Unternehmen verzichten auf regelmäßige Zertifizierungen.

Sichere Kommunikation und E-Mail-Verkehr

Deutliche Verschlechterung: Mehr als die Hälfte der Unternehmen ohne Schutz

ø10 %

beträgt die Steigerung des E-Mail-Versands kritischer Geschäftssachen insgesamt.

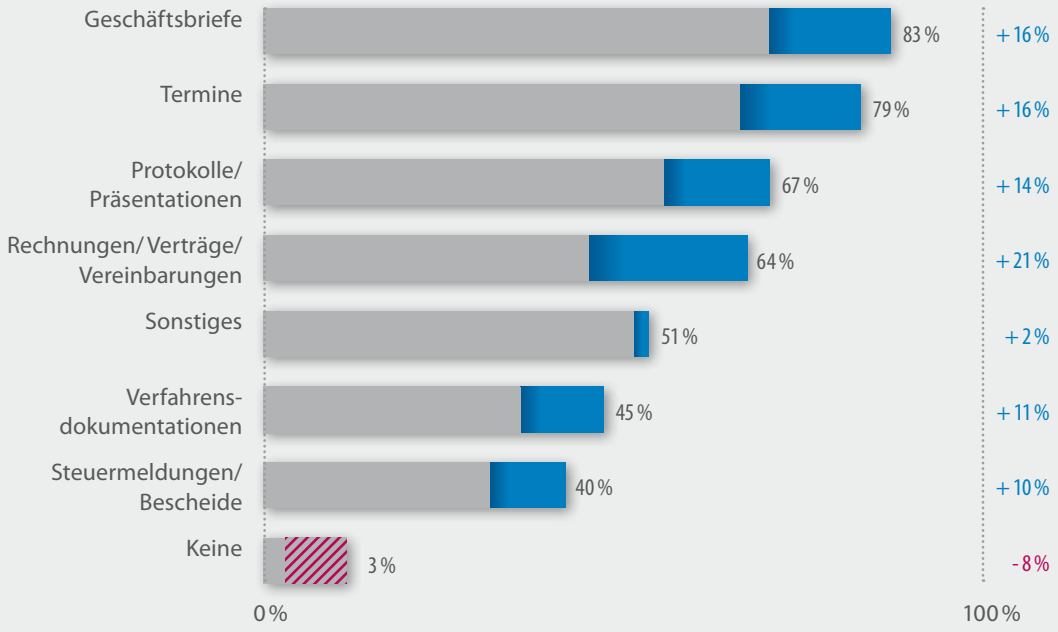
Die E-Mail ist das meist genutzte Kommunikationsmedium im Unternehmen. Auch die Intensität der versandten Unterlagen hat nochmals deutlich zugelegt. So sind in fast allen Bereichen zweistellige Zuwachsraten zu verzeichnen. Allein bei Rechnungen/Verträgen/Vereinbarungen beträgt der Zuwachs 21 Prozentpunkte auf 64 % (Grafik 8).

Ungeachtet der zunehmenden Relevanz des geschäftlichen E-Mail-Verkehrs sind Sicherheitsvorkehrungen teilweise rückläufig. Mehr als die Hälfte der Unternehmen (57 %) versenden ihre E-Mails ungeschützt. Unverändert 12 % der Befragten geben an, sich über Risiken bei der E-Mail-Nutzung keine Gedanken zu machen.

Die Hälfte der Unternehmen kommuniziert ohne Absicherung der E-Mail.

Damit fällt ein Paradox ins Auge: Trotz des Bewusstseins zum Umgang mit vertraulichen Informationen bleiben praktischen Sicherheitsmaßnahmen aus. Damit zeigt die Sicherheit des E-Mail-Verkehrs einen akuten Handlungsbedarf auf.

Geschäftssachen, die per E-Mail versandt werden



Grafik 8 03/2014 03/2014 Zunahme 03/2014 Abnahme

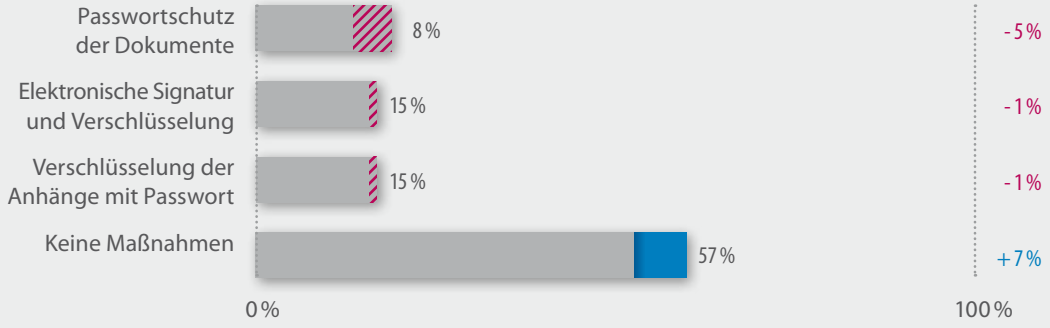
Die Absicherung der E-Mails zeigt einen gravierenden Bruch zwischen der Mehrheit der Unternehmen (57 %), die keine Sicherheitsmaßnahmen treffen und solchen, die die Kommunikation mit Passwörtern, elektronischen Signaturen oder Verschlüsselungen der Anhänge schützen. Insgesamt zeigt der Beobachtungszeitraum von 2011 bis 2014 einen Rückgang der Schutzmaßnahmen auf 38 % (Grafik 9).

Es ist zu vermuten, dass viele Unternehmen bei dieser Thematik schlichtweg überfordert sind. Teilweise herrscht aber auch die Vorstellung, der Schutz des Internet-Zugangs beinhalte eine Absicherung von E-Mails. Tatsächlich ist der Zugang zum Internet bei fast allen Unternehmen abgesichert, teilweise sogar mehrfach – eine separate Maßnahme zur E-Mail-Sicherheit besteht hingegen nicht.

57 %

der Unternehmen treffen keine Sicherheitsmaßnahmen zur Absicherung der E-Mails.

Sichere Kommunikation per E-Mail



Grafik 9 03/2014 03/2014 Zunahme 03/2014 Abnahme

Schutzmaßnahmen für mobile Geräte

Effektivität der getroffenen Maßnahmen unzureichend.

4

57 %

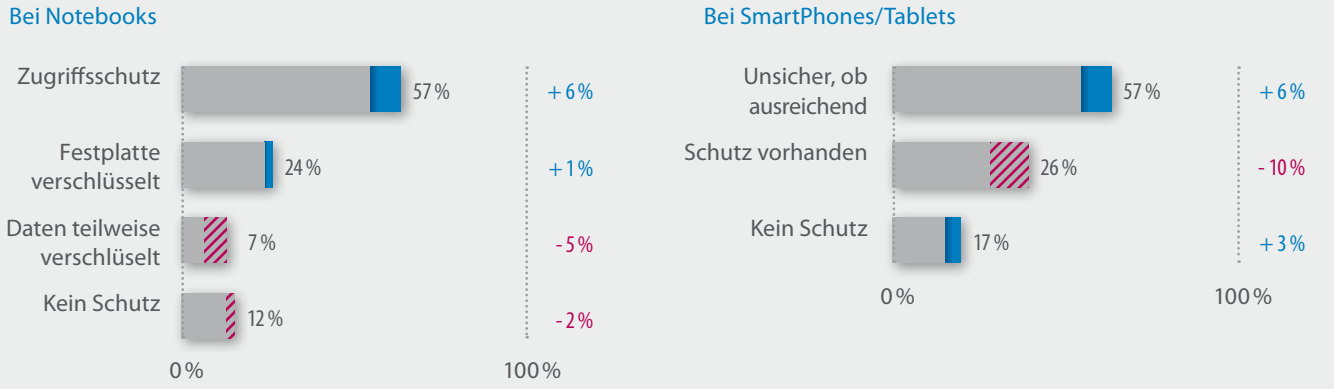
verwenden einen Zugriffschutz für Notebooks, genauso viele sind unsicher, ob die Maßnahmen auch bei Smartphones / Tablet-PCs ausreichen

Der mobile Zugriff auf die Unternehmensdaten von unterwegs zeigt eine deutliche Zunahme. Entsprechend konnten Sicherheitsmaßnahmen bei Notebooks gegenüber 2011 zwar leicht zulegen – wenngleich auf recht niedrigem Niveau. Bei Smartphones, Tablet PC und Netbook waren die Schutzmaßnahmen hingegen sogar rückläufig:

- Der Zugriffsschutz bei Notebooks verharrt auf niedrigem Niveau bei 57 % und hat sich auch nur um 6 Prozentpunkte seit 2011 verbessert. Effektive Sicherungsmaßnahmen wie Festplattenverschlüsselung, auch die teilweise Verschlüsselung von Daten haben eher Ausnahmecharakter. Hier liegt eine Stagnation oder sogar Verschlechterung der Vorkehrungen vor (Grafik 11).
- Im Bereich der Smartphones und Tablets ist ein Rückgang relevanter Sicherheitsmaßnahmen wie Zugriffsschutz zu verzeichnen. Hier geben nur noch 26 % an, entsprechende Maßnahmen im Betrieb zu ergreifen. Das ist ein Rückgang von 10 Prozentpunkten.

Auffällig ist, dass sich 57 % der Befragten bewusst sind, dass ihre Maßnahmen möglicherweise nicht ausreichen („Bin mir nicht sicher“). Dieser Aussage liegen zwei mögliche Ursachen zu Grunde. Entweder fehlt das Bewusstsein darüber, welche Risiken bestehen und wie die getroffenen Maßnahmen wirken. Oder es besteht eine Unkenntnis über die Optionen, die einen höheren Schutz bewirken können.

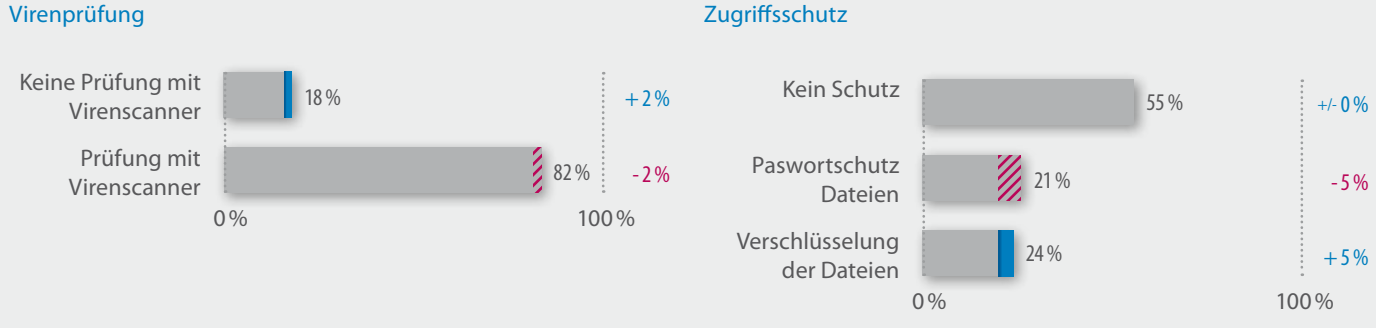
Vorhandene Schutzmaßnahmen für mobile Geräte



Grafik 10 03/2014 03/2014 Zunahme 03/2014 Abnahme

Über die Verwendung von mobilen Geräten hinaus spielt auch der Austausch mit mobilen Datenträgern eine relevante Rolle. Auch hier sind die getroffenen Sicherheitsmaßnahmen kaum gestiegen oder rückläufig: So gaben 55 % der Unternehmen an, ihre IT bei der Verbindung mit mobilen Datenträgern überhaupt nicht zu schützen. Eine Sicherung der Daten mit Passwörtern ist sogar rückläufig - von 26 % (2011) auf 21 % (2014). Lediglich bei der Verschlüsselung der Daten gibt es Steigerung um 5 Prozentpunkte – auf nunmehr 24 % etabliert.

Welche Sicherungsmaßnahmen werden beim Datenaustausch über mobile Datenträger ergriffen?



Grafik 11 03/2014 03/2014 Zunahme 03/2014 Abnahme

Supertrend Cloud Computing

Unsicherheit bei Sicherheitsfragen beeinflusst die Cloud-Verbreitung

5

2012

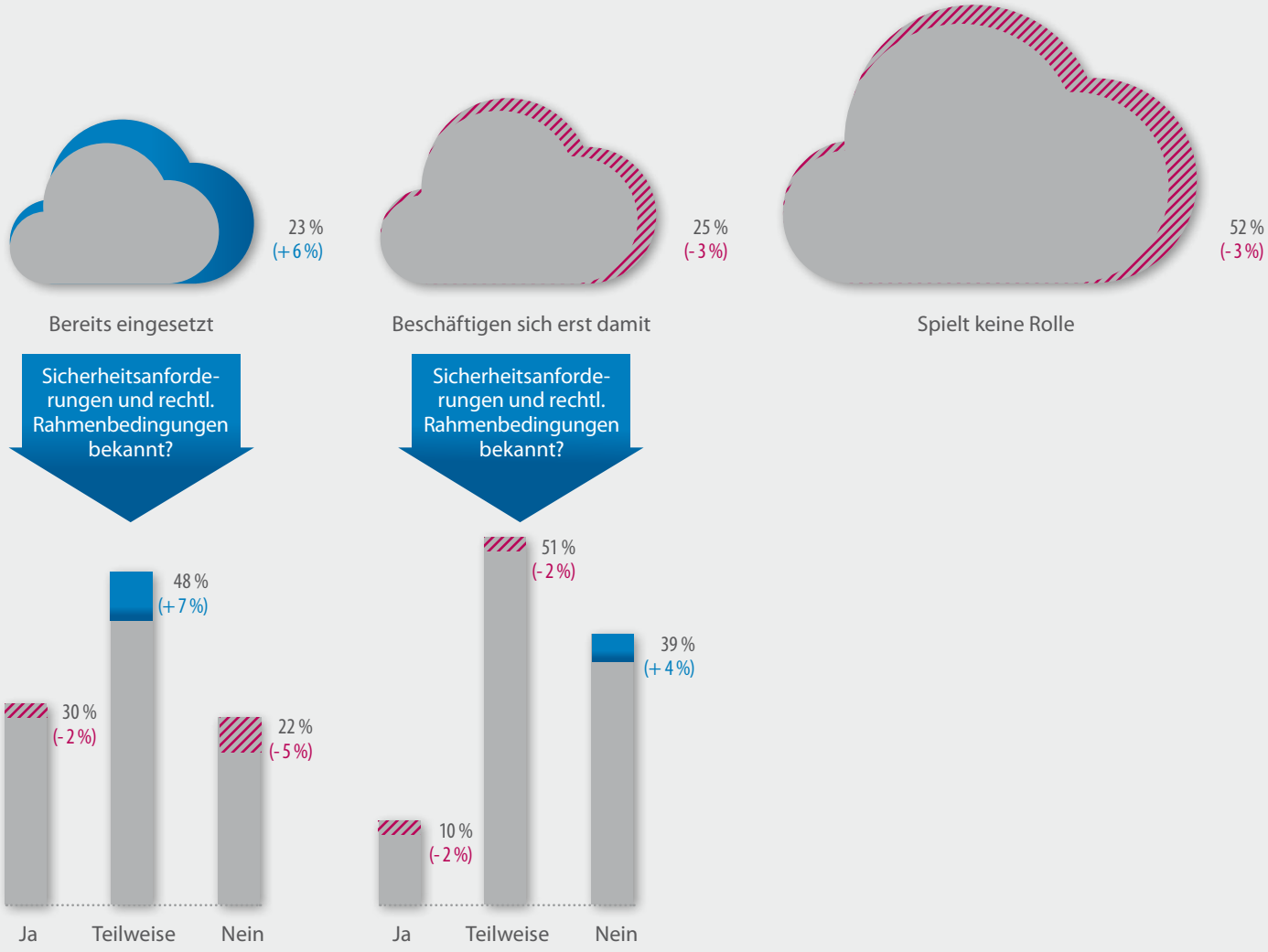
Seit 2012 hat die Nutzung von Cloud-Anwendungen deutlich zugelegt.

Seit 2012 wird der Umgang mit Cloud Computing im DsiN-Sicherheitsmonitor unter Sicherheitsaspekten behandelt. In dieser Zeit hat die Nutzung von Cloud-Anwendungen deutlich zugelegt. Fast jedes vierte Unternehmen gibt an, mit Diensten in der Cloud zu arbeiten. Für mehr als die Hälfte der befragten mittelständischen Unternehmen spielt Cloud Computing hingegen noch „keine Rolle".

Eine Mikroanalyse aus den vergangenen 12 Monaten ergab, dass die Befassung mit Cloud-Computing bei mittelständischen Unternehmen in der Zeit abnahm, wodurch auch die bislang steigende Nutzung etwas abebben könnte. Eine mögliche Ursache könnte in der aktuellen Sicherheitsdebatte liegen.

Auffällig ist, dass 70 % der Unternehmen, die sich in der Cloud befinden, Sicherheitsanforderungen und rechtlichen Rahmenbedingungen nur teilweise oder gar nicht kennen. Das ist ein Zuwachs von 2 Prozentpunkten. Nur 30 % geben an, diese zu kennen. Demgegenüber meinen über 90 % der Befragten, die nicht in der Cloud sind, keine oder nur teilweise Kenntnis über die Sicherheitsanforderungen zu besitzen. Die Anforderungen zu kennen, meinen hingegen davon nur 10 %.

Cloud-Einsatz und Wissen über Sicherheitsanforderungen



Grafik 12 03/2014 03/2014 Zunahme 03/2014 Abnahme

Mit 25 % ist die Anzahl der Unternehmen rückgängig, die eine Nutzung der Cloud in Betracht ziehen (2012: 28 %). In Verbindung damit, dass nur 10 % der Unternehmen die Sicherheitsanforderungen kennen, würde der überwältigende Teil der cloudinteressierten Unternehmen über (kein ausreichendes) Wissen zu den Sicherheits- und Rechtsanforderungen in der Cloud verfügen.

Insgesamt weist das Ergebnis auf eine erhebliches Aufklärungsbedürfnis der kleinen und mittelständischen Unternehmen im sicheren Umgang mit der Cloud hin. Dabei ist zu vermuten, dass Basiswissen sowie – darauf aufbauend – praktische Anleitungen im Umgang mit der Cloud und bei der Auswahl von Cloud-Diensten der notwendige erste Schritt sind, um Unternehmen zum sicheren Umgang mit der Cloud zu befähigen.

32 %

aller Cloud-Anwender sind mit den Sicherheitsaspekten vertraut. Bei den Unternehmen, die noch darüber nachdenken, sind dies 18 % weniger.

Im Fokus: Ausgesuchte Entwicklungen seit 2011

Der Sicherheitsmonitor stellt Entwicklungen in den Fokus, die im Jahresvergleich 2011 bis 2014 eine besondere Relevanz für die IT-Sicherheitslage aufweisen. Dadurch werden Trends sichtbar, die auf relevante Handlungsfelder für künftige Aufklärungsmaßnahmen hinweisen. Im Zentrum stehen Fragestellungen, die im IT-Sicherheitscheck eine besondere Rolle aufweisen:

- IT-Infrastruktur und digitale Arbeitslabläufe
- E-Mail und sichere Kommunikation
- Verwendung mobiler Datenträger
- Datenschutz und IT-Sicherheitsmanagement

IT-Infrastruktur und digitale Arbeitslabläufe

Die Sicherung der IT-Infrastruktur in ihrer Gesamtheit ist eine ständige Herausforderung, die heute nur wenige Unternehmen im Mittelstand voll erfüllen. Dabei steigt die Komplexität mit einer zunehmenden Digitalisierung und Vernetzung der Arbeitsabläufe.

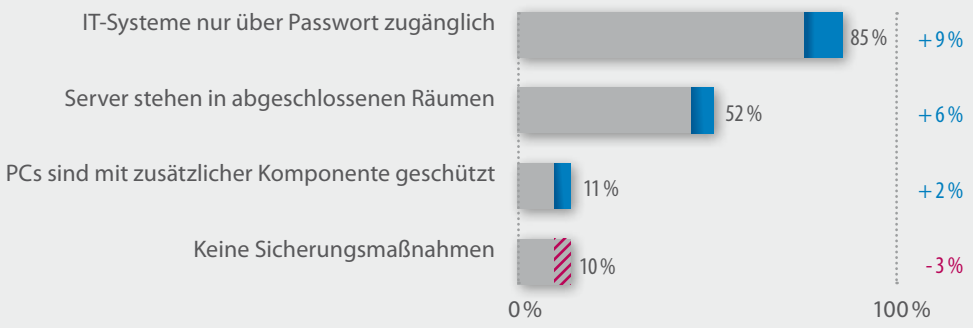
Bei einigen Sicherheitsfaktoren der IT-Infrastruktur ist eine Verbesserung zu erkennen, wenn gleich das Gesamtniveau noch nicht ausreichend ist. So erfolgt heute in 85 % der Unternehmen eine Sicherung der IT-Systeme mit Passwörtern (Grafik 13), ein Zuwachs um 9 Prozentpunkte. Immerhin die Hälfte der Unternehmen, 52 % (2011: 46 %) sichert seine Server in abgeschlossenen Räumen, zu denen ausschließlich autorisierte Personen Zugang haben.

Der Schutz der PCs mit zusätzlichen Komponenten (Besitz und Wissen, z.B. Smartcard) legt mit 11 % (vorher 9 %) hingegen nur leicht zu, ist jedoch weiterhin von eher untergeordneter Bedeutung. Dies ist angesichts millionenfachen Diebstahls von Zugangsdaten wie aktuell über die OpenSSL-Lücke eher verwunderlich. Erfreulich aber nicht befriedigend ist der leichte Rückgang von 13 % auf 10 % derer, die keinerlei Sicherungsmaßnahmen zur Nutzung der IT-Systeme in den Unternehmen treffen.

11 %

Mangelnder PC-Schutz mit zusätzlichen Komponenten angesichts wiederkehrender Vorfälle wie zuletzt die OpenSSL-Lücke eher verwunderlich.

Welche Sicherungsmaßnahmen zur Nutzung Ihrer IT-Systeme (Server und PCs) setzen Sie ein?



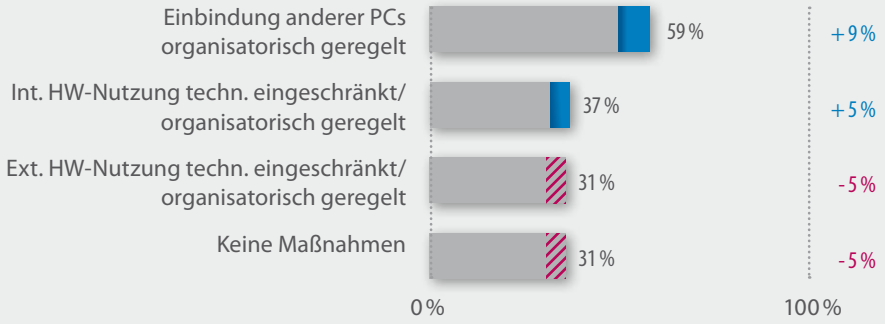
Grafik 13 03/2014 03/2014 Zunahme 03/2014 Abnahme

Eine weitere Sicherheitslücke ist der unerlaubte Transfer von Daten aus IT-Systemen. Eine leichte Mehrheit der Unternehmen von 59 % trägt Vorkehrung, dass Daten aus den IT-Systemen nicht unerlaubt transferiert werden, in dem sie die Einbindung anderer PCs organisatorisch regeln (2011: 50 %). Immer noch aber trifft fast jedes dritte Unternehmen (31 %), gar keine Vorkehrung gegen den unerlaubten Datentransfer (2011: 36 %).

Sicherstellung, dass nicht unerlaubt Daten aus IT-Systemen transferiert werden

31 %

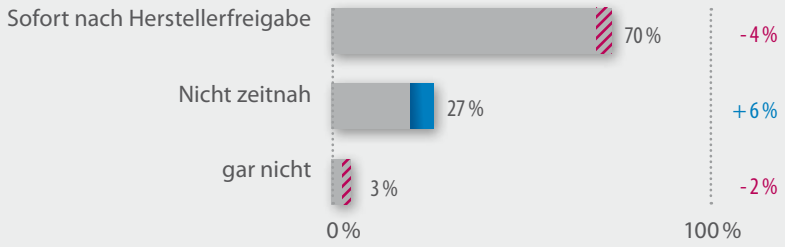
verfügen über keine Maßnahmen. Insgesamt halten sich positive und negative Entwicklungen zum Schutz vor Datendiebstahl die Waage.



Grafik 14 03/2014 03/2014 Zunahme 03/2014 Abnahme

Die Unternehmen haben die Sicherheits-Updates im Blick. Positiv zu bewerten ist, dass nur noch 3 % der Unternehmen gar keine Vorkehrungen zur Installation von Sicherheits-Updates treffen und immerhin 70 % unmittelbar nach der Herstellerfreigabe ihre Systeme aktualisieren (Grafik 15).

Wann werden IT-Systeme mit den relevanten Sicherheits-Updates aktualisiert?



Grafik 15 03/2014 03/2014 Zunahme 03/2014 Abnahme

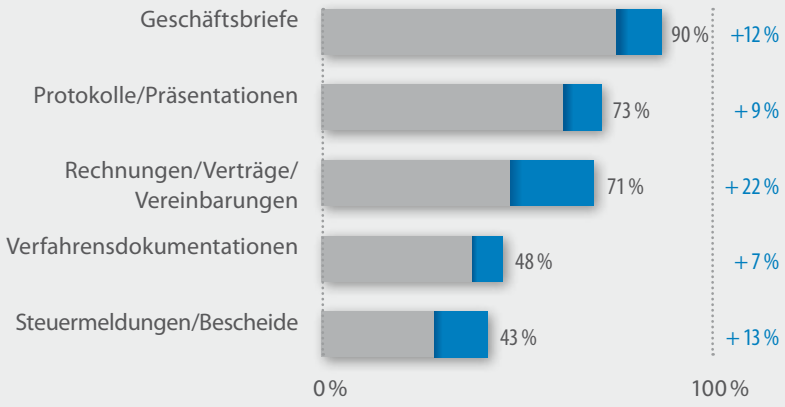
Umso erforderlicher erscheint es, auf die zunehmende Komplexität und Vernetzung mit der einfachen Vermittlung von praktikablem Sicherheitswissen zu reagieren, welches die Unternehmen zu konkreten Maßnahmen befähigt.

E-Mail und sichere Kommunikation

Die Übertragung von – auch vertraulichen – Dokumenten über E-Mail ist ein allgemeiner Trend im geschäftlichen Alltag. Dem steht gegenüber, dass Maßnahmen für ihre Sicherung kaum verbessert wurden und teilweise sogar rückläufig sind (Grafik 9, S. 15).

Im Lichte dieser Entwicklung ist bemerkenswert, dass das Bewusstsein für die Sensibilität der Dokumente vorhanden ist, gleichwohl eine Sicherung ausbleibt. Gegenwärtig verwenden 90 % der Unter-nehmen wissentlich einen ungesicherten Kommunikationskanal für ihre Geschäftskorrespondenz – ein Anstieg um 12 %. Bei potentiell hochsensiblen Verträgen und Vereinbarungen sieht es nicht besser aus: Hier ist ein Anstieg um 22 Prozentpunkte zu verzeichnen auf heute 71 %. Damit werden drei von vier E-Mails in diesem Bereich ungesichert übermittelt.

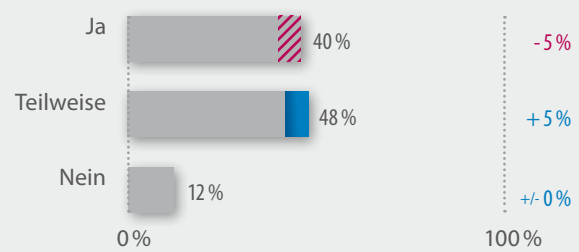
Welche Informationen werden per E-Mail ohne Schutzmaßnahmen versendet?



Grafik 16 03/2014 03/2014 Zunahme 03/2014 Abnahme

Mit dieser Entwicklung korrespondiert, dass 60 % der Unternehmen sich gar nicht oder nur teilweise mit Risiken für Internet- und E-Mail-Kommunikation beschäftigen (Grafik 17). Dies gilt auch für die rechtlichen Anforderungen hinsichtlich der E-Mail-Schutzmaßnahmen gegen unberechtigte Einsichtnahme, Missbrauch oder Manipulation; hier besteht weiterhin großer Aufklärungsbedarf.

Auseinandersetzung mit Risiken und rechtlichen Anforderungen bei der Internet- und E-Mail-Nutzung



Grafik 17 03/2014 03/2014 Zunahme 03/2014 Abnahme

+/-0

Die Auseinandersetzung mit Risiken bei Internet und E-Mail stagniert.

Verwendung mobiler Datenträger

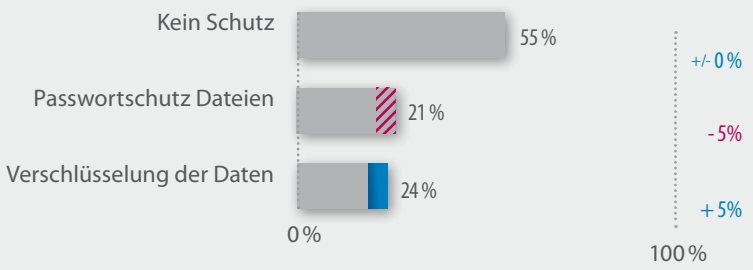
-5

Um 5 Prozentpunkte verschlechtert sich der Schutz mobiler Datenträger. Dazu zählen Passwortschutz für einzelne Dateien aber auch Verschlüsselung.

Der Austausch von Unternehmensdaten mit mobilen Datenträgern hat seit 2011 stark zugenommen. Dafür mitverantwortlich ist der Trend, dass private Geräte und Datenträger für berufliche Zwecke verwendet werden, die dann mit Trägern des Unternehmens in Verbindung gebracht werden (Bring your own device).

Auffällig ist, das im Beobachtungszeitraum die Sicherheitsmaßnahmen für den Datenaustausch stagnieren oder rückläufig sind. Wie schon 2011, gaben auch 55 % der Unternehmen an, beim Austausch überhaupt keine Schutzvorkehrungen vorzunehmen (Grafik 18). Ein wirksamer Passwortschutz wird nur noch in 21 % der Fälle verwendet (2011: 26 %), eine Verschlüsselung in 24 % mit immerhin einer leichten Verbesserung (2011: 19 %). Insgesamt verharrt der Schutz der IT beim Austausch mobiler Datenträger aber auf niedrigem Niveau und sollte dringend verbessert werden.

Sicherheitsmaßnahmen für Informationen beim Austausch über mobile Datenträger



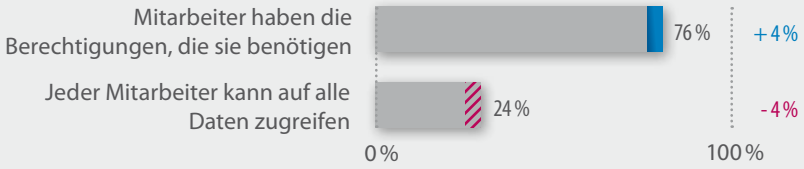
Grafik 18 03/2014 03/2014 Zunahme 03/2014 Abnahme

Datenschutz und IT-Sicherheitsmanagement

Die Vorkehrungen im Bereich des Datenschutzes und des IT-Sicherheitsmanagements weisen im Vergleich zu 2011 die geringsten Zuwächse aus. So geben immer noch 28 % (Grafik 7, S. 13) an, keinerlei organisatorische Maßnahmen im Unternehmen festgelegt zu haben. Dies ist weiterhin als relativ hoch zu bezeichnen.

In nahezu jedem vierten Unternehmen können alle Mitarbeiter auf sämtliche Daten zugreifen. Dieser Wert verbesserte sich um lediglich 4 Prozentpunkte im Vergleich zu 2011 (Grafik 19).

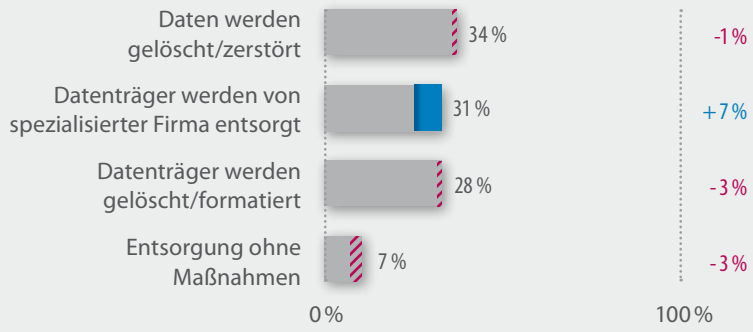
Regelung für Nutzungsrechte der Mitarbeiter



Grafik 19 03/2014 03/2014 Zunahme 03/2014 Abnahme

Positiv hat sich hingegen der Umgang mit vertraulichen Daten auf nicht mehr benötigten Datenträgern entwickelt. Hier entsorgen nur noch 7 % (2011: 10 %) Medien sorglos ohne besondere Maßnahmen (Grafik 20). Bemerkenswert ist, dass die Entsorgung verstärkt über externe Spezialisten erfolgt. Dieser Wert stieg im Vergleich zu 2011 um 7 Prozentpunkte auf 31 %.

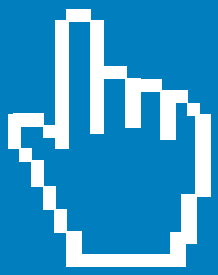
Entsorgung von Datenträgern mit vertraulichen Daten



Grafik 20 03/2014 03/2014 Zunahme 03/2014 Abnahme

+ 7 %

beträgt die Steigerung bei der Beauftragung spezialisierter Firmen zur Datenträgerentsorgung.



Handlungsempfehlungen – Engagement stärken

Die IT-Sicherheitslage im Jahre 2014 zeigt eine steigende Verbreitung von IT in allen Geschäftsprozessen, ohne dass die notwendigen Sicherheitsmaßnahmen Schritt halten: In vielen Bereichen ist eine Stagnation, wenn nicht sogar eine geringere Verbreitung der Aktivitäten für IT-Sicherheit in Unternehmen zu verzeichnen.

Obwohl Sicherheitsfragen in Unternehmen subjektiv als wichtig empfunden werden, mangelt es an einer wirksamen Umsetzung. Eine Mischung aus Unkenntnis, organisatorischen Defiziten sowie Überforderung spielen eine Rolle – von der Sicherung des elektronischen Mail-Verkehrs bis zum mobilen Internet.

Um dieser Entwicklung entgegenzuwirken, sind alle Beteiligten gefragt: Die IT-Wirtschaft in koordinierender Rolle, die Politik in unterstützender Funktion und die IT-Anwender selbst mit Offenheit und Verbesserungswillen. Das ist ein Prozess, der ein geduldiges, aber konsequentes und nachhaltiges Handeln erfordert.

Erforderlich sind Maßnahmen, die das Risiko-Bewusstsein innerhalb der Unternehmen steigern. Es geht aber auch um die Stärkung von Kompetenzen, konkrete Maßnahmen zu ergreifen. Dazu werden nachfolgend fünf Schwerpunktbereiche skizziert.

Aufklärungsarbeit und praktische Anleitungen: Fünf Handlungsfelder für mehr IT-Sicherheit

- Empfehlung 1: IT-Risikobewusstsein stärken
- Empfehlung 2: Lösungs- und Umsetzungskompetenz verbessern
- Empfehlung 3: Mitarbeiter nachhaltig sensibilisieren
- Empfehlung 4: Technische Expertise verankern
- Empfehlung 5: Unterstützung beim Cloud Computing

1.

IT-Risikobewusstsein ganzheitlich stärken

Die Ergebnisse der Studie zeigen, dass das Sicherheitsbewusstsein im Vergleich zur Basismessung 2011 nicht mit dem Digitalisierungszuwachs Schritt hält. Die Folge sind nachlässige Sicherheitsaktivitäten. Teilweise erfolgen aber Sicherheitsmaßnahmen, die nicht an den eigentlichen Schwachstellen wirken und daher ins Leere laufen.

Daher sollte das Verständnis für IT-Risiken und Schwachstellen im Unternehmen gezielt verstärkt werden sowie auch das Bewusstsein für mögliche Folgen und Schäden – sowohl für Mitarbeiter als auch für verantwortlichen Entscheider. Es geht nicht um eine einseitige Darstellung von Risiken, sondern vielmehr um eine gezielte Betrachtung von IT-Sicherheitsfragen.

Spezielle Themenfelder der IT sollten in einer ganzheitlichen Betrachtung erfolgen. Auch sollte auf branchen- und sektorspezifische Besonderheiten eingegangen werden. In der Folge eines verbesserten, ganzheitlichen Risikobewusstseins wird ein Prozess ermöglicht, der auf Seiten der Unternehmen selbst mitgestaltet und vorangetrieben wird.

Aufgabe ist es daher, eine gesteigerte Wahrnehmung der Gesamtproblematik zu schaffen und den negativen Trend umzukehren. Dies betrifft in erster Linie kleine und mittlere Unternehmen und ihre Entscheider. Ein gestärktes Risikobewusstsein wird bei verantwortlich handelnden Unternehmern die Frage nach zu ergreifenden Maßnahmen hervorrufen, die es im weiteren ebenfalls zu beantworten gilt.

2.

Lösungs- & Umsetzungskompetenz verbessern

Einfache, aber wirksame Maßnahmen zur Steigerung der IT-Sicherheit haben in kleinen und mittelständischen weiterhin nur untergeordnete Bedeutung – wie der Schutz von PCs mit zusätzlichen Komponenten. Dies gilt erst Recht für anspruchsvollere Lösungen wie die sichere Anbindung mobiler Endgeräte, sichere E-Mail-Kommunikation oder Notfallkonzepte.

Die Entscheidungsebenen in KMU sollten dazu befähigt werden, die richtigen Maßnahmen auf identifizierten Risiken im Unternehmen zu ergreifen. Es muss gegengesteuert werden, dass etwa 57 % (2011: 51 %) der Unternehmen für die Risiken durch mobile Endgeräte wie Smartphones, Netbooks und WLAN vorliegen, jedoch Unkenntnis den Erlass wirksamer Maßnahmen verhindern.

Es sollte auch deutlich werden, dass nicht jede Maßnahme für jedes Unternehmen geeignet ist. An Stelle von Einzelmaßnahmen, die oftmals nicht erforderlich sind und keinen zusätzlichen Schutz bewirken, sollten Entscheider befähigt werden, aufeinander abgestimmte Sicherheitsmaßnahmen zu veranlassen, insbesondere in kritischen Feldern wie der E-Mail-Sicherheit und dem mobilen Internet.

Für die Stärkung der Lösungs- und Umsetzungskompetenz sollten Unternehmen mit den gängigen Instrumenten vertraut gemacht werden, insbesondere Sicherheitstests. Zudem sind praktikable Anleitungen erforderlich, die konkrete Kriterien bei der Auswahl und Durchführung von IT-Dienstleistungen im eigenen Unternehmen umfassen.

Ausgesuchte DsiN-Angebote:

- Die DsiN-Aufklärungsfilme geben Mitarbeitern von Unternehmen eine Anleitung zu einigen grundlegenden Verhaltensregeln im Umgang mit IT.
- DsiN-Mitarbeitersensibilisierung im Projekt „Freie Berufe als Brückenbauer“
- Der DsiN-Sicherheitscheck bietet als Einstieg für kleine und mittlere Unternehmen Hinweise zur IT-Sicherheitslage, die über einfache verständliche Grundlagenfragen generiert werden: www.sicher-im-netz.de/dsin-sicherheitscheck
- www.dsin-blog.de vermittelt praxisorientierten Hinweise bei der Planung konkreter Sicherheits maßnahmen.
- Leitfaden Sichere E-Mail-Kommunikation

3.

Mitarbeiter nachhaltig sensibilisieren

Maßnahmen zur Sensibilisierung von Mitarbeitern in kleinen und mittleren Unternehmen stagnieren bei unter 25 %. Es mangelt in weiten Teilen an einem Grundverständnis für die Informationssicherheit auf allen Ebenen. Damit sind Unternehmen nicht allein durch Angriffe von außen auf die IT bedroht, sondern auch mittels Social-Engineering-Attacken oder Mitarbeiter selbst.

Unternehmen sollten daher befähigt werden, ihre Mitarbeiter zum sicherheitsbewussten Umgang mit Informationen zu motivieren, indem diese aktiv beteiligt und eingebunden werden. IT-Risiken müssen klar kommuniziert werden und allen Mitarbeitern bewusst sein. Verbindliche Richtlinien in Form von Verfahrensanweisungen für Ihre Mitarbeiter können dazu einen wichtigen Beitrag leisten.

Dieses Verständnis sollten auch die Entscheider selbst vorleben. Denn wenn Mitarbeiter sorglos und nachlässig mit Daten, Programmen und Rechnern umgehen, nützen technische Schutzmaßnahmen nur wenig. Die Mitarbeiter müssen also im sicheren Umgang mit technischen Lösungen und sensiblen Unternehmensdaten im Alltag geschult werden.

Aufgabe ist es daher, die Entscheider in Unternehmen zu nachhaltigen Maßnahmen der Sensibilisierung von Mitarbeitern auf allen Ebenen zu unterstützen und einen selbsttragenden Lernprozess in Gang zu setzen. Diese Problematik sollte Teil von Mitarbeiterschulungen sein und auch bereits in der Ausbildung Platz erhalten. Darüber hinaus sollte auch der Diskurs außerhalb der Unternehmenswelt auf die Herausforderungen der IT-Sicherheit besser eingehen.

4.

Technische Expertise verankern

Die Studie weist darauf hin, dass heute schon einfache technische Anforderungen wie verschlüsselte E-Mail-Kommunikation die technische Expertise der meisten Unternehmen übersteigt. Unbeschadet ganzheitlicher Betrachtungen sowie organisatorischer und rechtlicher Vorkehrungen sollte daher jedenfalls ein technisches Grundwissen gewährleistet sein.

Ein Schwerpunkt sollte auf der Vermittlung von E-Mail-Verschlüsselungskompetenzen liegen. So ist bei der E-Mail-Sicherheit im Beobachtungszeitraum die Tendenz eines Rückgangs der Schutzmaßnahmen feststellbar. 43 % der befragten Unternehmen verfügen derzeit über keinerlei Sicherungsvorkehrungen. Maßnahmen sollten unberechtigte Einsichtnahme, Missbrauch oder Manipulation der E-Mails vorbeugen und sich in vorhandene Geschäftsprozesse einbinden lassen.

Es sollte gewährleistet sein, dass Festplattenverschlüsselung für Notebooks zum Standard wird sowie ein intelligentes Rechtemanagement und stärkere Authentifizierungsmechanismen sich in der Fläche durchsetzen. Eine Risiko-Nutzen-Analyse für die Synchronisation von mobilen Geräten sollte durchgeführt werden.

Aufgabe ist daher die Vermittlung von IT-Sofort-Maßnahmen für kleine und mittlere Unternehmen, die einfach und praktikabel das „Grundwerkzeug“ einer technischen Expertise vermitteln. Wichtig ist, einen nachhaltigen Ansatz zu wählen, der die betroffenen Unternehmen zu kontinuierlichen Verbesserungen und Optimierungen für die Zukunft befähigt.

Ausgesuchte DsiN-Angebote:

- Leitfaden Verhaltensregeln zur Informationssicherheit für Mitarbeiter
  (Verfügbar ab 25.07.2014 auf www.dsin.de)
- Passwortkarte zum DsiN-Jahreskongress
- Leitfaden Mobiles Arbeiten
- Leitfaden E-Mail-Verschlüsselung
- Gut-zu-Wissen, ein DsiN-Handlungsversprechen

5.

Unterstützung beim Cloud-Computing

Die Migration der IT von Unternehmen in die Cloud gehört zu den wichtigsten IT-Trends. Er ermöglicht enorme Vorteile für Unternehmen und ist auch Voraussetzung für veränderte Wertschöpfungsprozesse in der gesamten Wirtschaft. Aber nur 22% der Cloud-Nutzer geben an, die Sicherheitsanforderungen und rechtlichen Rahmenbedingungen zu kennen, 48 % kennen sie nur teilweise. Bei Unternehmen, die nicht in der Cloud sind, liegt dieser Prozentsatz sogar bei 90 %.

Um die Vorteile der Cloud zu nutzen und mögliche Risiken zu vermeiden, sollten Unternehmen mit den Sicherheitsanforderungen sowie den rechtlichen Bedingungen zügig vertraut gemacht werden. Dies gilt für Unternehmen, die in der Cloud sind (und möglicherweise ihr Engagement verstärken möchten) sowie auch für Betriebe, die einen Umzug erst noch in Betracht ziehen.

Erforderlich ist es, dass grundlegendes Wissen einfach vermittelt wird sowie auch praktische Anleitungen mitgegeben werden, die eine konkrete Auseinandersetzung mit einer „sicheren Cloudlösung“ ermöglichen. Sie sollte alle Ebenen des Cloud Computing umfassen sowie auch die Befähigung, zu eigenständiger Wahl und Entscheidung für Cloud-Dienste.

Unternehmen sollten Kriterien für die Auswahl geeigneter Cloud-Dienste sowie auch eines zuverlässigen Cloud-Anbieters erhalten – mit praktikablen Anleitungen. Produktunabängig und herstellerneutral sollten die Risiken dargestellt und Szenarien von der Migration bis zum Wechsel zwischen Cloudanbietern erläutert werden – flächendeckend und auch vor Ort über die lokalen IT-Dienstleister.

Ausgesuchte DsiN-Angebote:

- Nützlicher Hinweis für Auseinandersetzung mit Sicherheitsfragen in Sachen Cloud Computing: DsiN-Cloud-Scout.de
- Ab Juli wird der DsiN Cloud Scout auch für Europäische Nachbarländer verfügbar unter www.cloudwatchhub.eu

Deutschland sicher im Netz

Die Mission von DsiN ist, das Sicherheitsbewusstsein von Verbrauchern im Internet durch konkrete Hilfestellungen zu verbessern – im Verbund mit Unternehmen, Verbänden und Nichtregierungsorganisationen. Dafür bieten wir praktische Anleitungen und Orientierungshilfen, beispielsweise mit der Passwort-Wechsel-App für Verbraucher oder dem Cloud-Scout für Unternehmen.

Als Reaktion auf die NSA-Enthüllungen und steigende Cyberkriminalität verstärkt DsiN seine Angebote für Verbraucher und Unternehmen durch neue bundesweite Projekte. Für Unternehmen stehen die Aufklärung von Mitarbeitern, die Verbreitung von Sicherheitstests sowie das Thema Cloud Computing und digitale Vernetzung von Betriebsabläufen im Mittelpunkt.

Gegründet wurde DsiN als gemeinnütziger Verein im Nationalen IT-Gipfelprozess der Bundesregierung und steht seit 2007 unter der Schirmherrschaft des Bundesministeriums des Innern. Im Acht-Punkte-Programm der Bundesregierung für einen besseren Schutz der Privatsphäre von 2013 wird DsiN mit verstärkter Aufklärungsarbeit zu IT-Sicherheitsfragen in der breiteren Öffentlichkeit betraut.

Impressum

DsiN-Sicherheitsmonitor Mittelstand 2014
Eine Studie von Deutschland sicher im Netz

Verantwortlich:
Dr. Michael Littger

Redaktion:
Stefan Brandl
Katrin Böhme

Gestaltung:
ideengut I Agentur für Kommunikation.

Deutschland sicher im Netz e.V.
Albrechtstr. 10 a
10117 Berlin
Telefon +49 30 27576 - 310
Telefax +49 30 2757651 - 310
www.sicher-im-netz.de
info@sicher-im-netz.de

Ein Handlungsversprechen von:

Gemeinsam mit: