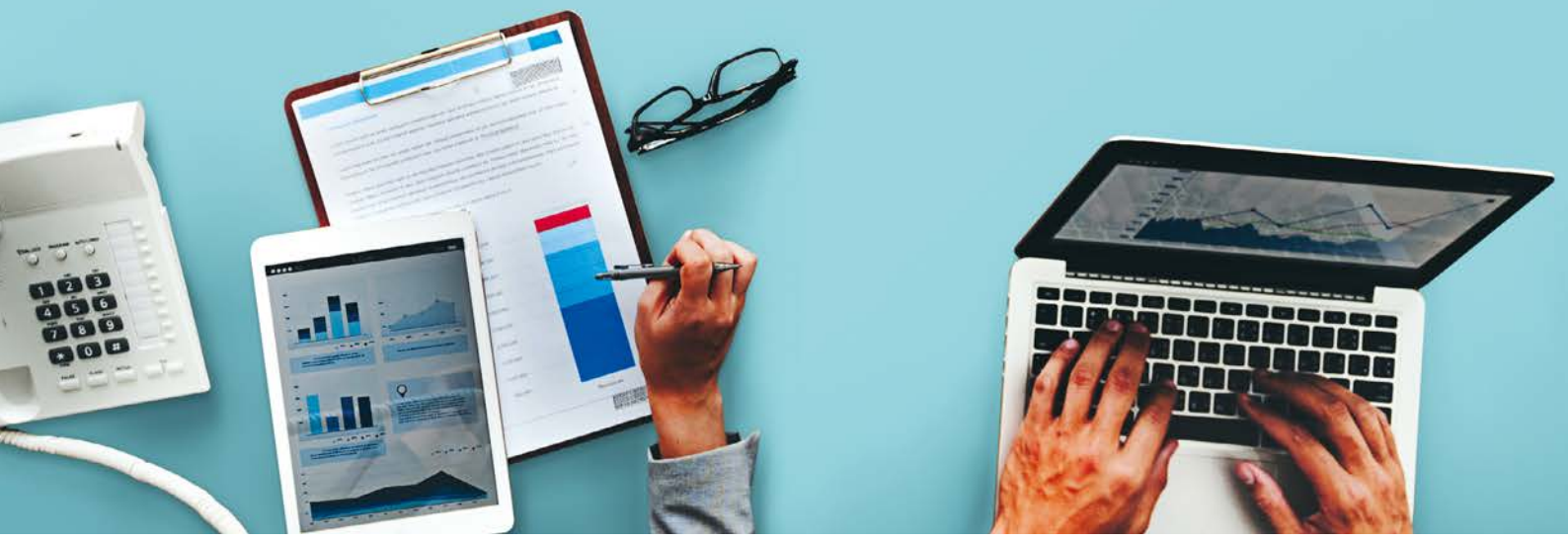
# DsiN SicherheitsMonitor 2016 Mittelstand

## IT-Sicherheitslage in Deutschland



Schirmherrschaft:

Bundesministerium des Innern

DsiN Deutschland sicher im Netz

Dr. Peter Krug

Dr. Michael Littger

# Sicherheit durch Verantwortung stärken

Wir freuen uns, dass bis heute rund 8.600 Unternehmen den kostenfreien IT-Sicherheitscheck genutzt haben, um einen fundierten Einstieg in Sicherheitsfragen zu erhalten – sowie als Grundlage für die vorliegende Erhebung. Nach sechs erfolgreichen Jahren wird Deutschland sicher im Netz e.V. den IT-Sicherheitscheck in wenigen Monaten neu aufstellen, um die wandelnden Anforderungen an Sicherheitsfragen im Mittelstand zu berücksichtigen.

Seit 2011 ist die Digitalisierung in kleinen und mittleren Unternehmen (KMU) im betrieblichen Alltag stetig gewachsen, während die Schutzvorkehrungen dahinter zurückblieben. Adäquate Gesamtkonzepte für die IT-Sicherheit gehören auch im Jahre 2016 noch immer nicht zur „IT-Sicherheitskultur“ in der Mehrheit der KMU. Auch die die öffentlichen Diskussionen über Sicherheitsvorfälle und die tägliche Berichterstattung über Angriffe von Cyberkriminellen, z.B. mit Erpressersoftware, hat daran wenig verändert.

Bemerkenswert ist, dass es gleichwohl erste Hinweise auf ein Umdenken in Unternehmen gibt, die sich zeitversetzt auch in den wichtigen, weil wirksamen organisatorischen Maßnahmen andeuten. Diese Anzeichen sind mit Vorsicht zu interpretieren und ihr vorhandenes Potential bedarf eines aktiven Ausbaus und einer Verstärkung entsprechender Aufklärungsangebote und Initiativen.

Auch in Zukunft sind innovative Angebote gefordert, die den Mittelstand zum Handeln motivieren, um eine ganzheitliche Sicherheitskultur zu etablieren. Dies fängt beim Bewusstsein und der Motivation der Mitarbeiter an – und schließt auch die Chefebenen mit ein.

Für DsiN und unsere Partner ist das ein klarer Handlungsauftrag: mit neuen Methoden und Ansätze zielen wir darauf ab, Treiber und Hemmnisse für das erkannte Sicherheitsverhalten bei KMU zu identifizieren und Lösungen anzubieten. Unser Ziel sind passgenaue Aufklärungsangebote für den Mittelstand. Diesem Ziel widmet sich Deutschland sicher im Netz e.V künftig mit einer Neuausrichtung der IT-Sicherheitsstudie, basierend auf den Erfahrungen der letzten sechs erfolgreichen Jahre.

Eine anregende Lektüre wünschen Ihnen

**Dr. Peter Krug**
Beiratsmitglied Deutschland sicher im Netz e.V.
Vorstand Entwicklung, DATEV eG

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

# Studienziel und Design

Der DsiN-Sicherheitsmonitor Mittelstand untersucht seit 2011 die IT-Sicherheitslage in kleinen und mittleren Unternehmen (KMU) und ermittelt Schwachstellen, um wirksame Aufklärungsmaßnahmen für den digitalen Schutz zu entwickeln.

Grundlage für die Untersuchung ist der *DsiN-Sicherheitscheck*, mit dem sich KMU einen Überblick über ihren IT-Sicherheitsstatus verschaffen können und mittels eines Online-Fragebogens Auskunft über ihr Sicherheitsniveau erhalten. Um die Sicherheitslage abzubilden, werden Fragen zur Nutzung digitaler Anwendungen aber auch zu getroffenen technischen sowie organisatorischen Schutzmaßnahmen gestellt. Der standardisierte und anonymisierte Online-Fragebogen wurde von DsiN mit seinen Mitgliedern BITKOM, DATEV, SAP und Sophos entwickelt. Für die Auswertung wurden nur vollständig abgeschlossene Fragebögen berücksichtigt.

Seit 2011 haben 8.600 Unternehmen am DsiN-Sicherheitscheck teilgenommen, davon 1.320 Unternehmen im aktuellen Erhebungszeitraum von Juni 2015 bis März 2016. Der Untersuchungszeitraum über nunmehr sechs Jahre ermöglicht eine zuverlässige Betrachtung von Trends der IT-Sicherheit in KMU, die auch die Einordnung von kurzfristigen Ausschlägen erleichtert.

Größte Teilnehmergruppe der vorliegenden Erfassung sind mit 34% Unternehmen mit bis zu 10 Mitarbeitern[1], gefolgt von Unternehmen mit bis zu 50 Beschäftigten mit insgesamt 26%. Die restlichen Unternehmensgruppen mit Mitarbeitern von über 50 teilen sich auf die verbliebenen 40% auf.

Die aktuellen Ergebnisse ermöglichen ein fundiertes Gesamtbild zur IT-Sicherheitslage im Mittelstand, um wirksame Aufklärungsstrategien abzuleiten und sind wichtige Grundlage für die Arbeit von DsiN.

[1] Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben stets auf Angehörige aller Geschlechter.

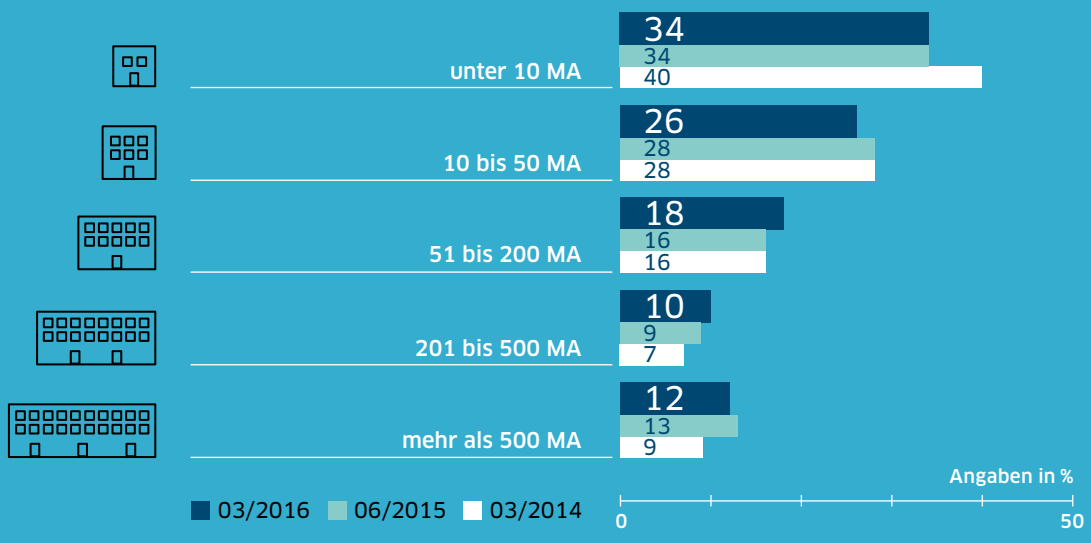
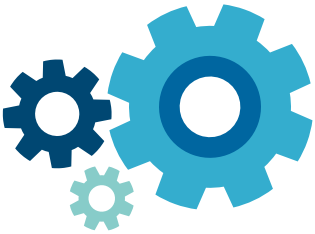



**Abb. 1: Befragte Unternehmen nach Anzahl der Mitarbeiter**

# Inhalt







# Zentrale Ergebnisse

**Positive Ansätze jetzt verstärken – bestehende Maßnahmen überprüfen**

**Der DsiN-Sicherheitsmonitor bestätigt in seiner diesjährigen Erhebung in Teilen die Stagnation bei IT-Schutzvorkehrungen in kleinen und mittleren Unternehmen (KMU) der vergangenen Jahre. Zugleich deuten sich Anzeichen von Fortschritten im Sicherheitsbewusstsein an. Der Einsatz bestehender Schutzvorkehrungen sollte sich dabei an zertifizierten Anforderungen wie dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutz messen lassen.**

Die seit Studienstart beobachteten Entwicklungen der IT-Sicherheitslage in KMU haben sich in der diesjährigen Fassung größtenteils bestätigt. Dabei hat sich die geschäftliche Internetnutzung im vergangenen Jahr auf einem hohem Niveau weitgehend stabil gezeigt – mit einer teilweisen leichten Abschwächungstendenz. Diese Abschwächung könnte eine Folge der Datensicherheitsdiskussionen der vergangenen Monate sein.

Es konnten keine bedeutenden Verbesserungen der organisatorischen Maßnahmen zu Datenschutz und Sicherheit bei den KMU festgestellt werden, weiterhin auch insbesondere im Bereich *Social Engineering*: Nach wie vor wird nur rund ein Viertel der Mitarbeiter zu diesem Thema geschult.

Die an der Umfrage beteiligten KMU lassen weiterhin ganzheitliche Ansätze von Sicherheitskonzepten vermissen. Oftmals kommen Einzellösungen zum Einsatz, die nur unzureichend aufeinander und auf die tatsächlichen Anforderungen der Unternehmen abgestimmt sind.

Die Ergebnisse dieser Studie werfen die Frage auf, ob bereits implementierte Sicherheitskonzepte und Lösungen in den Unternehmen den Anforderungen beispielsweise eines IT-Grundschutzes des BSI genügen.

Eine fatalistische Grundhaltung wird dort erkennbar, wo vorhandenes Bewusstsein für nötige Sicherheitsmaßnahmen keine Berücksichtigung in der Umsetzung eines ganzheitlichen Sicherheitsansatzes findet. Dies gilt trotz zum Teil einer verstärkten Kommunikation zur Bewusstseinsbildung für IT-Angriffsvektoren.

Bespielhaft dient hier die *Benutzer-/Rechte-Verwaltung*, die neben *Organisation* und *E-Mail* weiterhin eine der Schutzmaßnahmen mit dem größten Nachholbedarf darstellt. Im Hinblick auf den sich verstärkenden Digitalisierungsprozess bedarf die Notwendigkeit der Benutzerverwaltung bei den Unternehmen einer deutlicheren Platzierung.

Bei den Themen *Cloud Computing* und *E-Mail* zeichnet sich bei vielen Unternehmen ebenfalls Unsicherheit darüber ab, ob getroffene Maßnahmen ausreichend sind und ob Sie umfassend genug über die rechtlichen Anforderungen Bescheid wissen.

Neben diesen weiterhin bestehenden Defiziten sind aber auch positive Entwicklungen zu mehr Sensibilität und ganzheitlichen Sicherheitskonzepten im Ansatz erkennbar. Hier gilt es weiter mit geeigneten und neuen Initiativen diese zu forcieren und die Mittelständler dadurch zum stärkeren Handeln zu motivieren.

## Kapitel 1

# Digitalisierter Geschäftsalltag

Die Digitalisierung des Geschäftsalltags in der Wirtschaft und damit auch im Mittelstand hat seit der ersten Erhebung der Studie stetig zugenommen. Der Digitalisierungsdruck im Mittelstand wird durch weitere gesetzliche Regelungen, E-Governance, steuerrechtliche Änderungen und auch durch ein geändertes Kundenverhalten im E-Commerce verstärkt.

Die Nutzung digitaler Dienste durch kleine und mittlere Unternehmen über den Betrachtungszeitraum der Studie verhält sich über die vergangenen Jahre betrachtet stabil – so allerdings auch die Unsicherheiten in der Anwendung solcher Dienste, die Risiken in deren Nutzung sowie die rechtlichen Anforderungen an KMU.

# Digitalisierung des Geschäfts-alltags nimmt zu

**Die geschäftliche Internetnutzung sowie auch die Nutzung von E-Mail für geschäftliche Zwecke sind stabil auf hohem Niveau. Verlagerungen gibt es bei der Nutzung von Notebook zu Smartphone und Tablet. Die Nutzung von Cloud Computing erfährt eine leicht positive Tendenz, auch wenn der Gesamtwert immer noch auf einem recht geringen Niveau verharrt.**

**+3**

Prozentpunkte bei der Smartphone-Nutzung.

Die starken Zuwächse bei *Notebook-Nutzung (on-/offline)* aus dem vorigen Jahr sind durch einen rückläufigen Trend dieses Jahr teilweise wieder aufgebraucht. Stieg der Wert 2015 gegenüber 2014 um satte sechs Prozentpunkte, erleidet er mit 77% in der aktuellen Erhebung ein Minus von drei Prozentpunkten. Zur selben Zeit stieg die *Smartphone-/Netbook-Nutzung* um drei Prozentpunkte auf nunmehr insgesamt 68% (2014: 64%, 2015: 65%). Diese Entwicklung lässt eine Verlagerung in der geschäftlichen Nutzung von Notebooks zu Gunsten von Smartphones und Tablets vermuten.

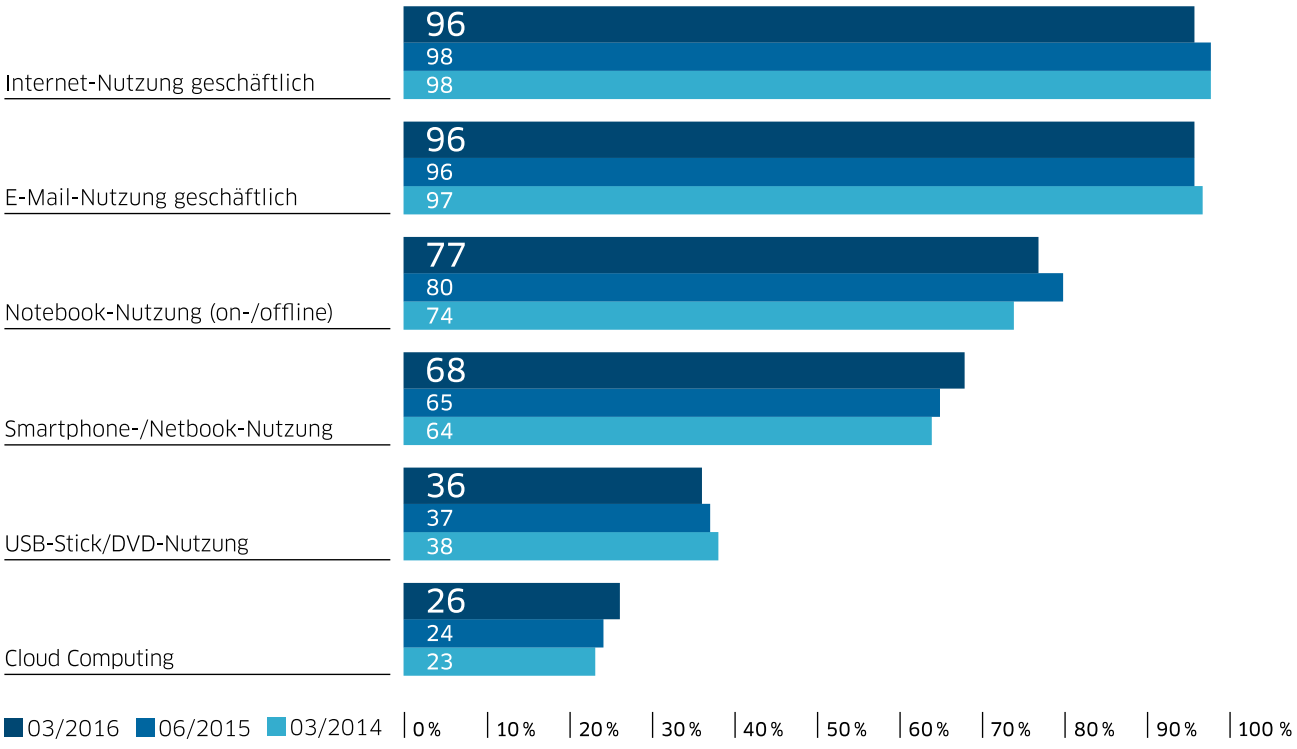



**Abb. 2: Digitalisierung im Geschäftsalltag**

Die oben erwähnte Verlagerung macht sich auch durch eine leicht erhöhte Nutzungstendenz der *Synchronisation von Mail- und Kalenderdaten* auf Smartphones und Netbooks um vier Prozentpunkte auf insgesamt 69% (2014: 64%, 2015: 65%) im Vergleich zum Vorjahr bemerkbar.

**+4**

Prozentpunkte bei der Synchronisation Postfach/Kalender mit Smartphone/ Netbook.

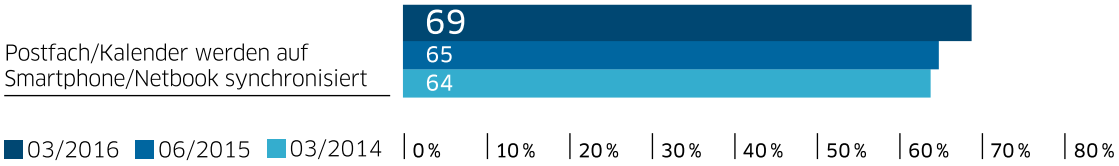



**Abb. 3: Auszug: Externe Datenzugriffe auf das Unternehmensnetzwerk**

## Abwärtstrend geschäftliche Nutzung Online-Banking bestätigt

Wie in beiden Erhebungsjahren zuvor wird das Internet von den befragten Unternehmen mit 91% am häufigsten zur Informationsbeschaffung und Recherche genutzt (2014 und 2015: 92%), gefolgt von der Bereitstellung einer eigenen Homepage, eines Shops bzw. Kundenportals mit 72% (2014: 72%, 2015: 73%).

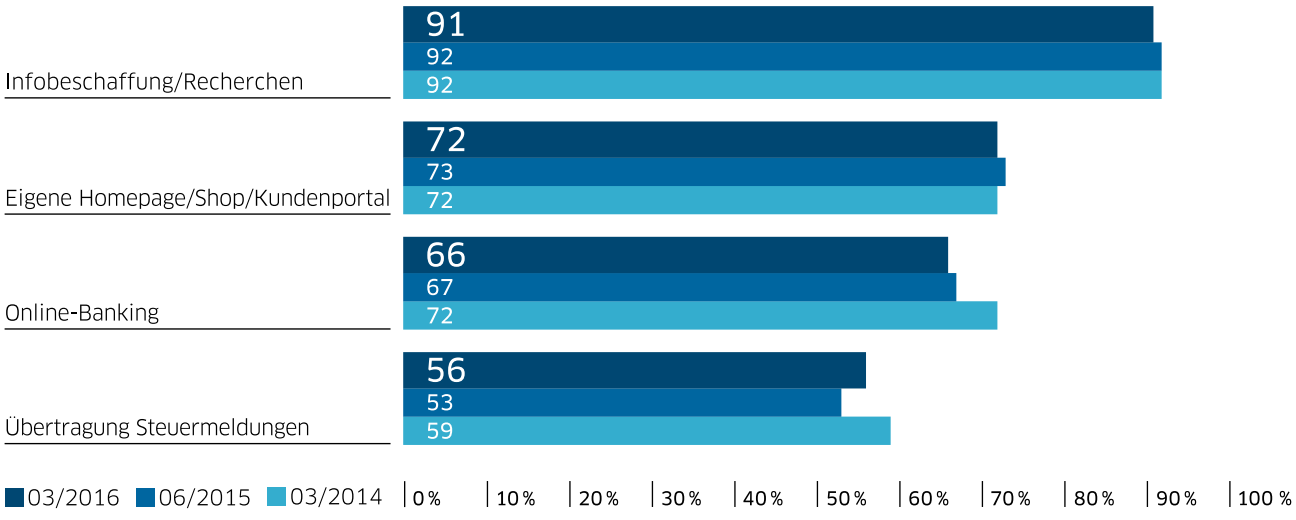



**Abb. 4: Auszug: Geschäftliche Nutzung Internet**

Die Nutzung von *Online-Banking* ist dagegen rückläufig: Der Rückgang im letzten Jahr – von 72% in 2014 um satte fünf Prozentpunkte auf 67% in 2015 – setzt sich tendenziell fort. Der Vertrauensverlust aus dem Vorjahr hat sich in 2016 mit 66% bestätigt. Die Hintergründe für den relativ niedrigen Akzeptanzwert von gut zwei Dritteln sind nicht eindeutig.

*Übertragung Steuermeldungen* hingegen kann nach einem Rückgang im letzten Jahr (2014: 59%, 2015: 53%) wieder einen Zuwachs verzeichnen: der Wert stieg um drei Prozentpunkte auf einen Gesamtwert von 56%. Dies könnte durch die verstärkte Nutzung des Elsterportals begründet sein: Die Vorteile der elektronischen Steuermeldung wurden anscheinend erkannt, während das Thema Datensicherheit durch den nicht vermeidbaren Fortschritt der Digitalisierung hier in den Hintergrund zu rücken scheint. Diese Entwicklung zeichnet sich auch bei der Häufigkeit des Versandes von Steuermeldungen und Bescheiden per E-Mail ab, welche nach einem Rückgang von 40% in 2014 auf 37% in 2015 nun um vier Prozentpunkte auf 41% gestiegen ist.

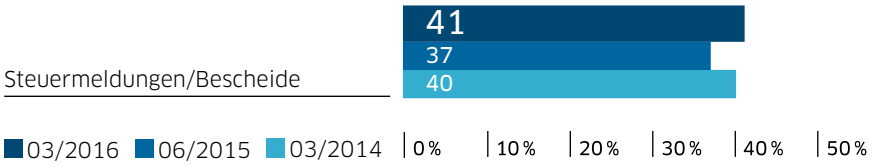



**Abb. 5: Versand vertraulicher/geschäftskritischer Informationen per E-Mail**

**Die Vorteile einer elektronischen Steuermeldung wurden von KMU anscheinend erkannt – Bedenken hinsichtlich der Datensicherheit bei der Digitalisierung treten hier in den Hintergrund.**

## Cloud Computing bleibt weiter hinter Potential zurück

Die Bedeutung von Cloud Computing stieg in der neuerlichen Erhebung zwar um jeweils zwei Prozentpunkte in den Kategorien *Wird bereits eingesetzt* auf 26% (2014: 23%, 2015: 24%) und *Beschäftigen sich damit* auf 28% (2014: 25%, 2015: 26%). Die Implementierung bleibt dabei hinter dem langjährig vorhergesehenen Potential weiter zurück; die bestehenden Hürden konnten anscheinend noch nicht abgebaut werden. Der Wert für KMU, bei denen Cloud Computing noch keine Rolle spielt, fiel demnach um vier Prozentpunkte auf 46% (2014: 52%, 2015: 50%) und damit zum ersten Mal unter die 50%-Marke.

Somit ist Cloud Computing im Geschäftsalltag für viele kleine und mittlere Unternehmen weiterhin von nachrangiger Bedeutung, auch wenn der Trend eine leicht positive Tendenz aufweist. Ein Grund dafür dürften die im folgenden Unterkapitel beschriebenen Unsicherheiten hinsichtlich der rechtlichen Bedingungen eine Rolle spielen.

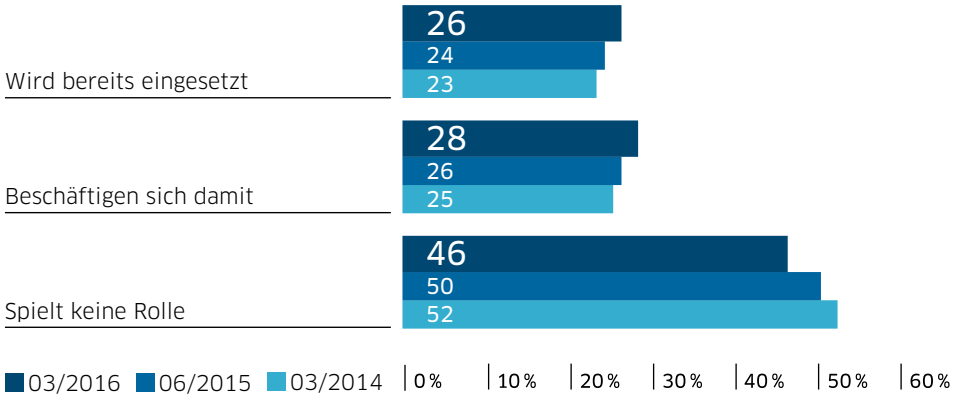



**Abb. 6: Rolle Cloud Computing im Unternehmen**

## Ausgesuchte DsiN-Angebote

→ **DsiN-Cloud Scout**
Online-Fragebogen zur Befassung mit Sicherheits- und Rechtsfragen beim Cloud Computing.
www.dsin-cloudscout.de

→ **Leitfaden Sicheres Arbeiten von unterwegs**
Hinweise für Mitarbeiter und IT-Verantwortliche (mit DATEV).
www.dsin.de/downloads/sicheres-arbeiten-unterwegs

# Anhaltende Unsicherheit bei rechtlichen Anforderungen und den Risiken

**Unternehmen verspüren im Zuge der Digitalisierung sowie teilweise in den einhergehenden rechtlichen Anforderungen eine auffällige Unsicherheit: Es geht um die Frage, ob die getroffenen Schutzmaßnahmen ausreichend sind und ob sie über die rechtlichen Anforderungen und Risiken ausreichend informiert sind. Diese Unsicherheit hat in den vergangenen Jahren angehalten.**

**60 %**

der KMU sind Risiken und rechtliche Anforderungen von E-Mail und Internet immer noch nicht bekannt.

Weniger als die Hälfte (46%) der befragten KMU gibt an, sich jedenfalls teilweise mit den genannten Risiken auszukennen (2014: 48%, 2015: 51%). Dies ist ein Rückgang um fünf Prozentpunkte innerhalb eines Jahres. Obwohl diese Entwicklung positiv anmutet, deutet der Gesamtanteil derer, denen die Risiken immer noch nicht bekannt sind mit insgesamt 60% auf eine weiterhin hohe Verunsicherung, und damit auch auf bestehenden Handlungsbedarf hin.

Der Anteil der Unternehmen, die angeben, die Risiken und rechtlichen Voraussetzungen bei der Nutzung von E-Mail und Internet zu kennen, steigt um drei Prozentpunkte im Vergleich zum Vorjahr auf 40% (2014: 40%, 2015: 37%). Zugleich steigt die Unsicherheit, über alle Anforderungen ausreichend informiert zu sein, um zwei Prozentpunkte auf nun 14% (2014 und 2015: 12%).

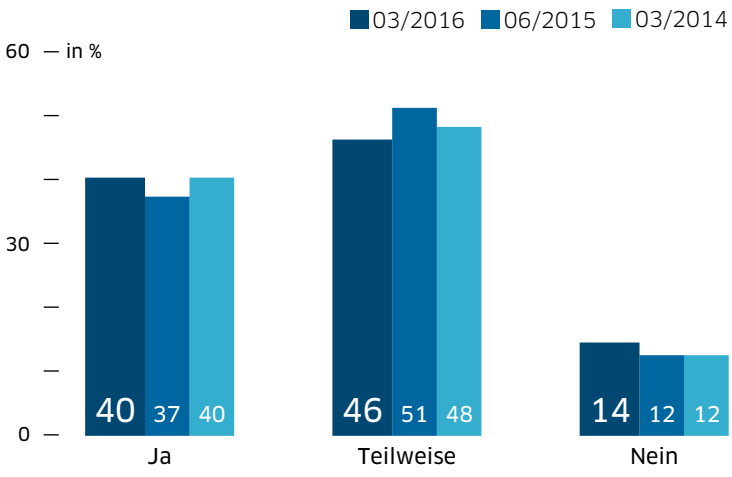



**Abb. 7: Bekanntheit von Risiken und rechtlichen Anforderungen bei der geschäftlichen Nutzung von E-Mail und Internet**

## Bedarf an Unterstützungsmaßnahmen für mobile Endgeräte

Die Digitalisierung des Arbeitsalltags hält insbesondere auch beim Einsatz von mobilen Endgeräten an: Smartphones und Netbooks erfreuen sich steigender Beliebtheit.

Hingegen gibt die Mehrheit der Befragten mit 57% an, dass Maßnahmen zur Sicherheit dieser Geräte ergriffen wurden, aber Unsicherheit besteht, ob diese Maßnahmen am Ende ausreichen (2014: 58%, 2015: 57%).

Die Anzahl der mit keinerlei Maßnahmen geschützten Smartphones, Tablets oder Netbooks beläuft sich auf immerhin noch 17% (2014 und 2015: 19%). Dieser Wert kann trotz leichter Verbesserung nicht zufrieden stellen, denn: über mobile Endgeräte fließen auch wegen des weiteren Wachstums in diesem Bereich immer häufiger sehr sensible Unternehmensdaten. 17% der mobilen Endgeräte sind überhaupt nicht gesichert und stellen damit für viele KMU eine ernstzunehmende Schwachstelle der IT-Sicherheit dar.

Rund

**17 %**

der Smartphones in KMU sind überhaupt nicht abgesichert.

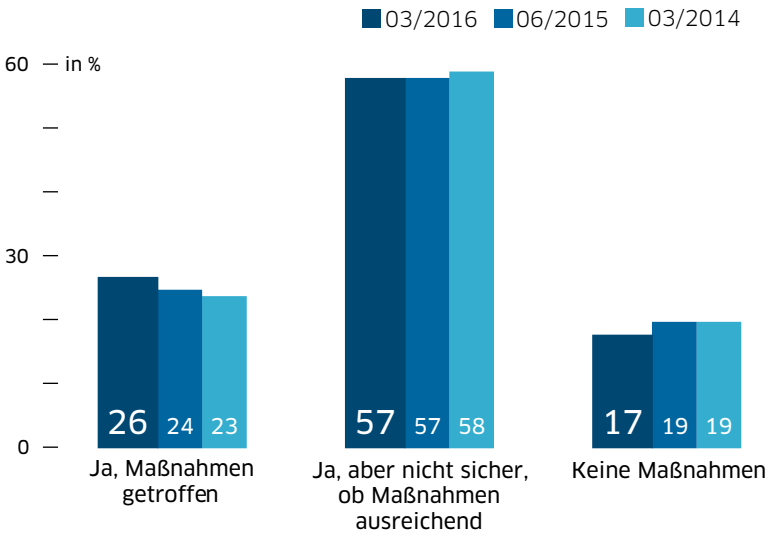



**Abb. 8: Maßnahmen gegen Gefahren im Umgang mit Smartphones, Tablets und Notebooks**

## Rechtliche Anforderungen Cloud Computing – 2016 besser bekannt

Die Unsicherheiten hinsichtlich der rechtlichen Nutzung von E-Mail und Internet sowie der zu ergreifenden Maßnahmen zur Absicherung von Smartphones und anderen mobilen Endgeräten setzen sich auch beim Thema Cloud Computing fort.

Nach einem Zuwachs um 3 Prozentpunkte kennen sich weiterhin nur 29% der befragten Unternehmen, die Cloud Computing bereits einsetzen, mit den Sicherheitsanforderungen und rechtlichen Rahmenbedingungen aus (2014: 27%, 2015: 26%). Auch der Anteil der Unternehmen, dem die rechtlichen Anforderungen immerhin „teilweise“ bekannt sind, steigt um 3 Prozentpunkte und liegt mit 49% (2014: 46%, 2015: 47%) immer noch unter der Hälfte der Befragten.

Der Anteil der Unternehmen, der Cloud Computing bereits einsetzt und dem die Sicherheitsanforderungen und rechtlichen Rahmenbedingungen weiterhin nicht bekannt sind, reduziert sich damit insgesamt um 6 Prozentpunkte auf nunmehr 22% (2014: 28%, 2015: 27%). Dieses insgesamt immer noch geringe Sicherheitswissen bei Unternehmen, die Cloud Computing bereits einsetzen, zeigt die Notwendigkeit zu weiterer Aufklärungsarbeit, um die Sicherheitskultur der KMU gerade auch beim Einsatz von Cloudlösungen zu stärken.

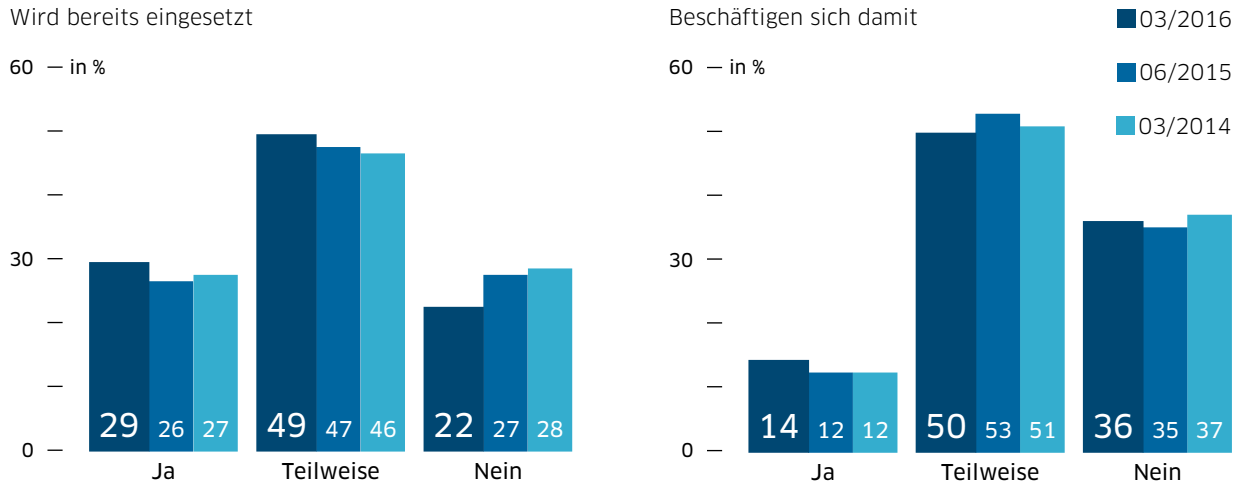



**Abb. 9: Bekanntheit Sicherheitsanforderungen/rechtl. Rahmenbedingungen von Cloud Computing**

## Ausgesuchte DsiN-Angebote

→ **Leitfaden Sicher im Netz**
Grundlagen für einen ganzheitlichen IT-Schutz in KMU (mit DATEV).
www.dsin.de/downloads/sicher-im-netz

→ **Leitfaden Sichere E-Mail Kommunikation**
Verständliche Handlungsempfehlungen zur Verbesserung der E-Mail-Sicherheit (mit Datev)
www.dsin.de/downloads/sichere-e-mail-kommunikation

→ **Überblickspapier IT-Consumerisation und BYOD**
Hinweise und Empfehlungen zum geschäftlichen Einsatz privater Geräte (vom BSI).
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.html

## Kapitel 2

# Technische Einzellösungen versus organisatorische Maßnahmen

Leichte Verbesserungen bei der E-Mail-Sicherheit und Verschlüsselung in den vergangenen Monaten deuten positive Verhaltensänderungen bei KMU an. Die Verstetigung der positiven Ansätze im digitalen Geschäftsalltag bedarf zusätzlicher, motivierender Ansprache.

Ebenso finden Sicherheitsrichtlinien und IT-Schutzzielen auf Basis von Schutzbedarfsanalysen Verbreitung. Dennoch: Grundlagen der IT-Sicherheit wie Notfallpläne geben nur ein Drittel der befragten KMU an. Auch bleibt die regelmäßige Prüfung vorhandener Maßnahmen auf Ihre Wirksamkeit erforderlich.

# IT-Sicherheitslage zeitstabil

**Die Digitalisierung der Wirtschaft schreitet weiter voran, während die IT-Sicherheitslage im Sinne von eingesetzten Schutzmaßnahmen dabei recht zeitstabil bleibt. Auffällig ist, dass die bisher weniger eingesetzten Schutzmaßnahmen tendenziell aufholen, allerdings teilweise noch große Verbesserungspotentiale ausweisen.**

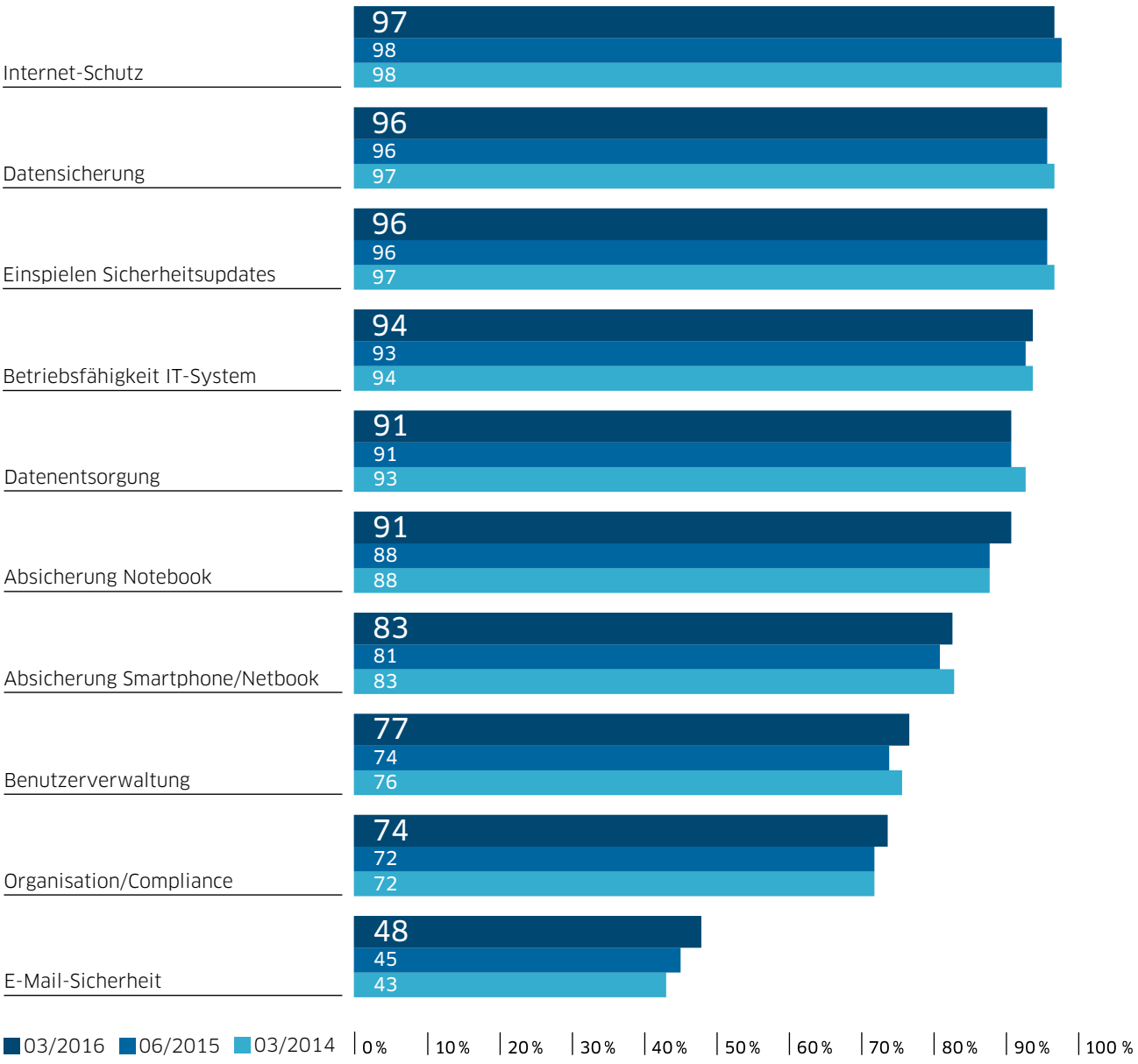



**Abb. 10: IT-Sicherheitslage: vorhandene Schutzmaßnahmen**

Die vorhandenen IT-Schutzmaßnahmen bei kleinen und mittleren Unternehmen zeigen nahezu annähernd gleiche Werte über den dreijährigen Vergleichszeitraum: Sowohl der *Internet-Schutz* (97%), die *Datensicherung* (96%) als auch *Einspielen Sicherheitsupdates* (96%) weisen allesamt hohe und konstante Werte auf. Hingegen lassen sich bei Maßnahmen wie *Benutzerverwaltung* (77%) und *Organisation/Compliance* (74%) weiterhin deutliche Verbesserungspotentiale erkennen. Insbesondere auch bei der *E-Mail-Sicherheit* (48%), das seit Jahren größte Sorgenkind.

Die Schutzmaßnahme *Absicherung Smartphone/Netbook* weist einen Wert von 83% auf. Betrachtet man im Zusammenhang mit diesem Wert das anhaltende Wachstum beim Einsatz von Smartphones und Tablets im betrieblichen Alltag, verlangt dies eine weitere Stärkung dieser Schutzmaßnahme. *E-Mail-Sicherheit* verzeichnet im Vergleich zum Vorjahr einen erfreulichen Anstieg um 3 Prozentpunkte, findet allerdings mit nun 48% immer noch bei weniger als der Hälfte der befragten Unternehmen Berücksichtigung (2014: 43%, 2015: 45%). Diese Entwicklung legt die Vermutung nah, dass die Informationsbemühungen zu den bekannten Hürden beim Thema E-Mail-Sicherheit (besonders bei der Verschlüsselung) im Ansatz greifen, ein entscheidender Schritt nach vorne allerdings noch nicht vollzogen wurde.

**+3**

Prozentpunkte beim Aspekt E-Mail-Sicherheit.

**Schutzmaßnahmen für E-Mail-Sicherheit finden weiterhin bei weniger als der Hälfte der KMU Berücksichtigung.**

## Ausgesuchte DsiN-Angebote


→ **DsiN-Sicherheitsblog**
Hintergrundinformationen zum Schutz vor Cyberkriminalität und zu digitalen Entwicklungen.
www.dsin-blog.de

→ **Leitfaden „Cloud Computing. Was Entscheider wissen müssen“**
Bietet Hinweise zur Einführung des Cloud Computings im Unternehmen (von BITKOM).
www.bitkom.org/Bitkom/Publikationen/Publikation_4365.html


→ **DsiN-Cloud Studie**
Schafft einen Überblick über den Status der Cloud-Nutzung im Mittelstand.
www.dsin.de/downloads/dsin-cloud-scout-report-2015

→ **Sicherheitsbarometer: SiBa-App**
Stellt Meldungen zu aktuellen IT und Internet-Risiken mit passenden Sicherheitstipps für den digitalen Alltag bereit.
www.dsin.de/siba

# Technische Einzellösungen überwiegen nach wie vor

**Technische Einzellösungen dominieren die IT-Sicherheitskultur der KMU. Trotz teilweiser Stagnation bei Schutzvorkehrungen sind kaum mehr Betriebe komplett ungeschützt. Hier ist der Schutz durch Passwörter eine zentrale Sicherheitsvorkehrung. Auch URL-Filter, Monitoring und Webnutzung verzeichnen Zuwächse. E-Mail-Vorkehrungen bleiben die größte Schwachstelle.**

Noch

**9 %**

der Notebooks ohne jeglichen Schutz vor unberechtigter Einsichtnahme.

Der Einsatz von Passwörtern ist die populärste Sicherheitsvorkehrung zum Schutz von IT-Systemen und stagniert auf einem relativ hohen Niveau von 84% (2014: 85%, 2015: 84%).

Ebenso ist beim Schutz vor unberechtigter Einsichtnahme des geschäftlich genutzten Notebooks die Einrichtung eines *Zugriffsschutzes* mit 56% die am meisten genutzte Maßnahme. Doch auch hier deuten sich keine weiteren positiven Entwicklungen im Dreijahresvergleich an (2014: 57%, 2015: 56%). Eine leicht positive Tendenz zeichnet sich dahingegen bei der Verschlüsselung von Festplatten mit 26% (2014 und 2015: 24%,) und von Daten auf Notebooks mit 9% (2014: 7%, 2015: 8%) ab.

Insgesamt liegen die Werte damit in einem Bereich, der ein realistisches Verbesserungspotential aufweist und mit weiteren Bemühungen zur Sensibilisierung wesentlich zur Stärkung der IT-Sicherheit in KMU beitragen kann. Der leichte Zuwachs lässt auf erste Einstellungsänderungen bei Unternehmen hoffen.

Auch die Zahlen zu Unternehmen, die keinen Schutz in Anspruch nehmen, haben sich leicht verbessert: Während in den Vorjahren jeweils 12% keine Schutzvorkehrungen getroffen hatten, um ihr Gerät vor unberechtigter Einsichtnahme zu schützen, sind es 2016 immerhin nur noch 9%. Die positive Tendenz könnte – analog zu den bereits erwähnten Entwicklungen beim Thema E-Mail-Sicherheit – einen weiteren Hinweis liefern, dass sich die anhaltende Aufklärungsarbeit erst zeitverzögert in der Organisation der Unternehmen bemerkbar macht.

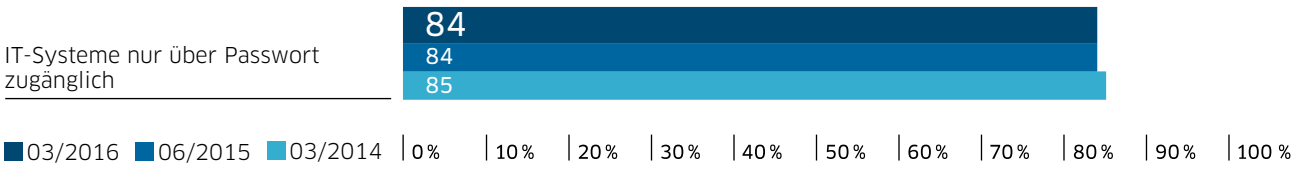



**Abb. 11: Auszug: Sicherungsmaßnahmen zur Nutzung der IT-Systeme**

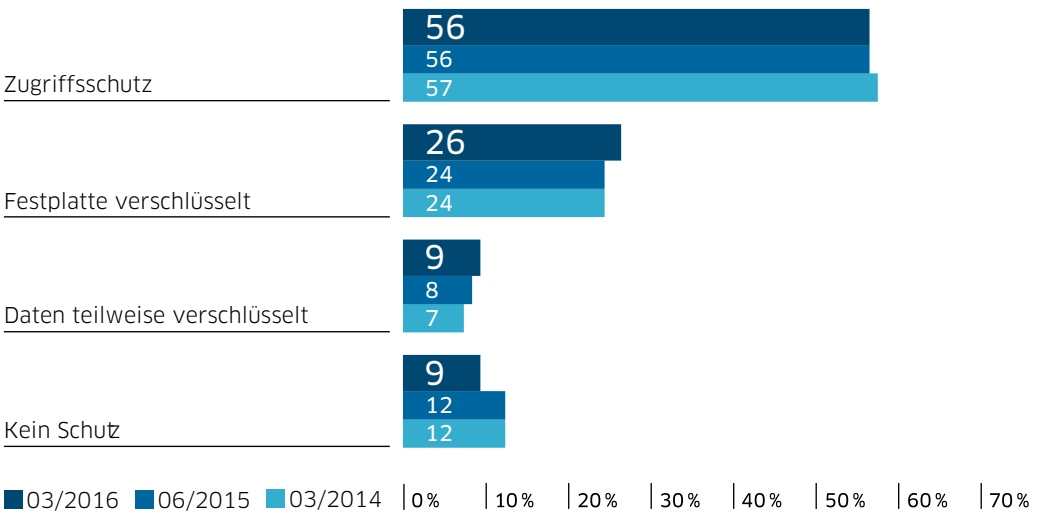



**Abb. 12: Notebookschutz vor unberechtigter Einsichtnahme**

## URL-Filter und Monitoring Webnutzung erfreuen sich größerer Beliebtheit

Bei den Maßnahmen zur Absicherung des Internetzugangs gibt es folgende Entwicklungen: der *URL-Filter* als Sicherungsmaßnahme legt um drei Prozentpunkte im Vergleich zum Vorjahr (2014: 35%, 2015: 36%) auf insgesamt 39% zu. Grundsätzlich lassen sich URL-Filter von Unternehmen einsetzen, um das Aufrufen von illegalen oder mit Malware (Schadsoftware) infizierten Webseiten vom Arbeitscomputer aus zu unterbinden (häufige Gefahr: Drive-by-Downloads, siehe Kasten). Auch bei *Reporting/Monitoring Webnutzung* ergibt sich ein Anstieg, hier sogar um satte fünf Prozentpunkte auf insgesamt 38% (2014: 32%, 2015: 33%). Die weiteren Sicherungsmaßnahmen stagnieren hingegen in ihrer Akzeptanz und Anwendung.

Diese Entwicklung lässt vermuten, dass durch die bekannten Unsicherheiten auf Anwenderseite (hier insbesondere die Mitarbeiter eines Unternehmens) bei der Identifizierung vertrauenswürdiger Webseiten durch URL-Filter und dem Monitoring der Webnutzung größerer Schaden abgewendet werden soll.

Erklärung: Ein **Drive-by-Download** ist ein vom Internetnutzer unbewusstes und unbeabsichtigtes Herunterladen einer Datei (in der Regel Schadsoftware) beispielsweise durch das alleinige Aufrufen einer infizierten oder manipulierten Website.

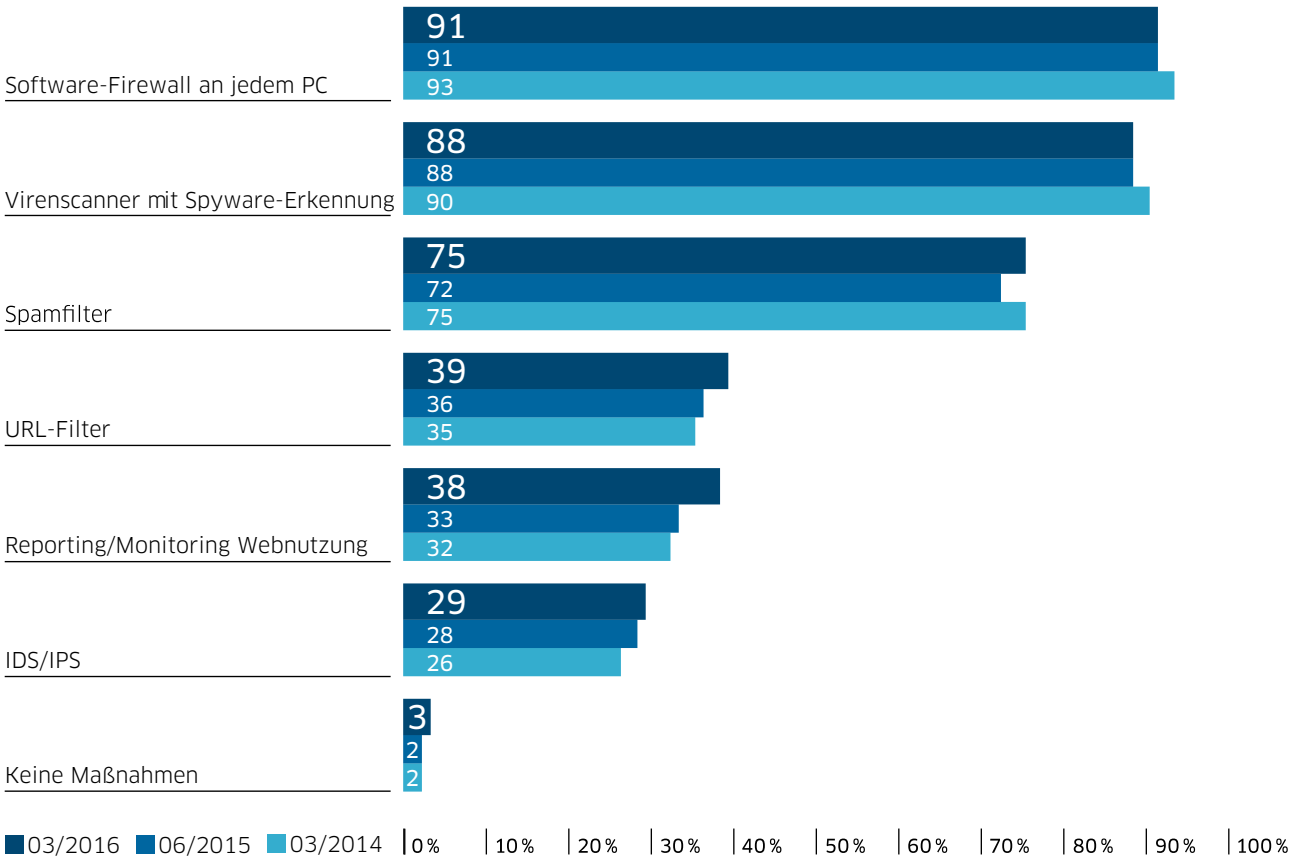



**Abb. 13: Maßnahmen zur Absicherung des Internetzugangs**

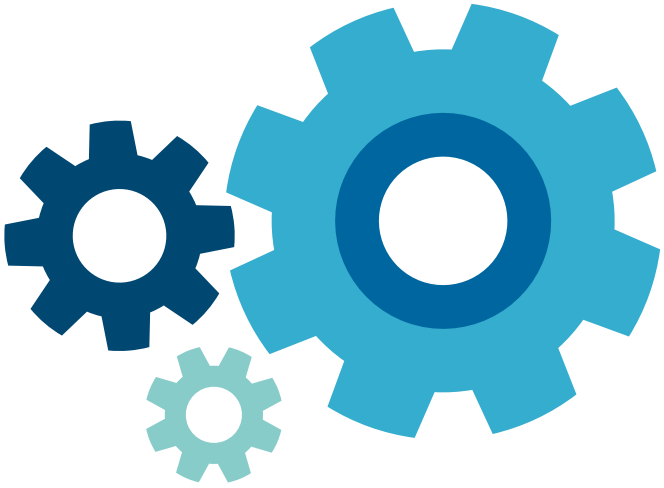
**+3**

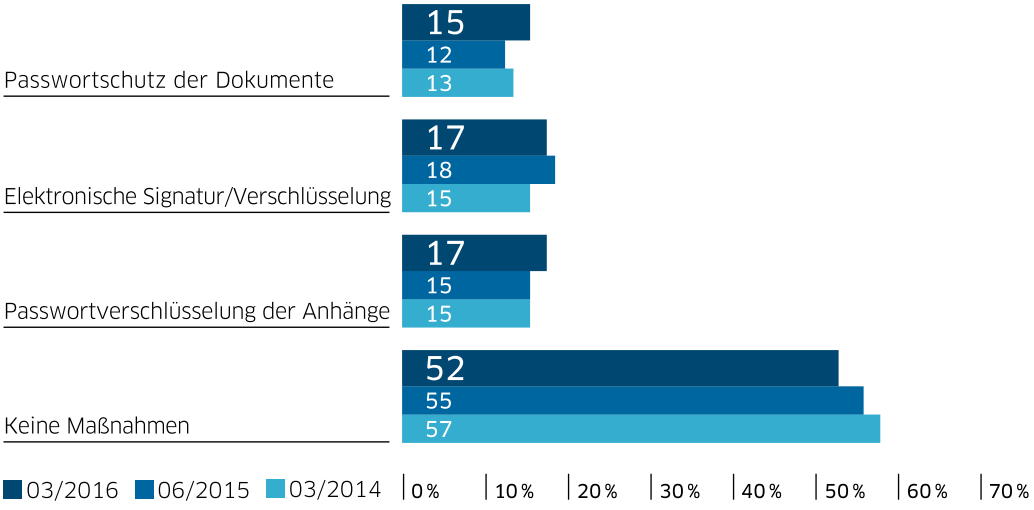
Prozentpunkte beim Passwortschutz von Dokumenten bei E-Mail-Übertragung.

## Nach wie vor größte Schwachstelle: E-Mail-Sicherheit

Das Thema der Datensicherheit bei der Übertragung durch E-Mails erhält mehr Aufmerksamkeit von den befragten KMU: von *Keine Maßnahmen* (minus drei Prozentpunkte) hin zu einem *Passwortschutz der Dokumente* (plus drei Prozentpunkte) und einer *Verschlüsselung der Mail-Anhänge* um zwei Prozentpunkte. Trotz dieser leichten Aufwärtstendenz bleibt E-Mail-Sicherheit im Rahmen dieser Umfrage die größte Schwachstelle mit dem dringendsten Handlungsbedarf.

Die anhaltende und leichte Verlagerung bei der Datensicherung während der E-Mail-Übertragung von *Keine Maßnahmen* (2014: 57%, 2015: 55%, 2016: 52%) hin zu einem *Passwortschutz der Dokumente* (2014: 13%, 2015: 12%, 2016: 15%) und einer *Passwortverschlüsselung der Anhänge* (2014 und 2015: 15%, 2016: 17%) um je zwei Prozentpunkte nach oben deuten dennoch auf ein gewachsenes Bewusstsein der Anwender für vertrauenswürdige und sichere Kommunikation hin. Diese positive Entwicklung basiert möglicherweise auf den langjährigen Sensibilisierungskampagnen in diesem Bereich, die sich nun mit Verzögerung in den Organisationen bemerkbar machen.






**52%**

der KMU ohne jegliche Datensicherung während der E-Mail Übertragung.

**Abb. 14: Datensicherung während der E-Mail Übertragung**

## Ausgesuchte DsiN-Angebote

→ **Leitfaden Verschlüsselung von E-Mails**
Bietet einen Überblick über die E-Mail-Verschlüsselung (mit DATEV).
www.dsin.de/downloads/verschluesselung-e-mails

→ **Muster-Passwortkarte**
Regelkonforme Passwortbildung einfach gemacht (mit DATEV).
www.dsin.de/dsin-muster-passwortkarte

→ **Leitfaden Social Engineering**
Weist auf konkrete Risiken im Arbeitsbereich hin und gibt Verhaltensregeln zum sicherheitsbewussten Umgang mit Situationen und Personen (mit DATEV).
www.dsin.de/downloads/verhaltensregeln-zum-social-engineering

# Organisatorische Maßnahmen und Gesamtkonzepte

**Positive Tendenzen für den vermehrten Einsatz von Sicherheitsrichtlinien und einer Schutzbedarfsanalyse deuten auf eine Verbesserung des IT-Schutzes hin, während eine große Schwachstelle weiterhin vernachlässigt wird: Nach wie vor wird nur rund ein Viertel der Mitarbeiter zu dem Thema explizit geschult.**

Bei den organisatorischen Maßnahmen zu Datenschutz und Datensicherheit konnte zwar im Jahresvergleich keine signifikante Verbesserung erzielt werden, die Vermutung hinsichtlich eines zeitverzögerten positiven Effekts insbesondere bei organisatorischen und bzw. oder ganzheitlichen Sicherungskonzepten spiegelt sich dennoch in einzelnen Entwicklungen wider.

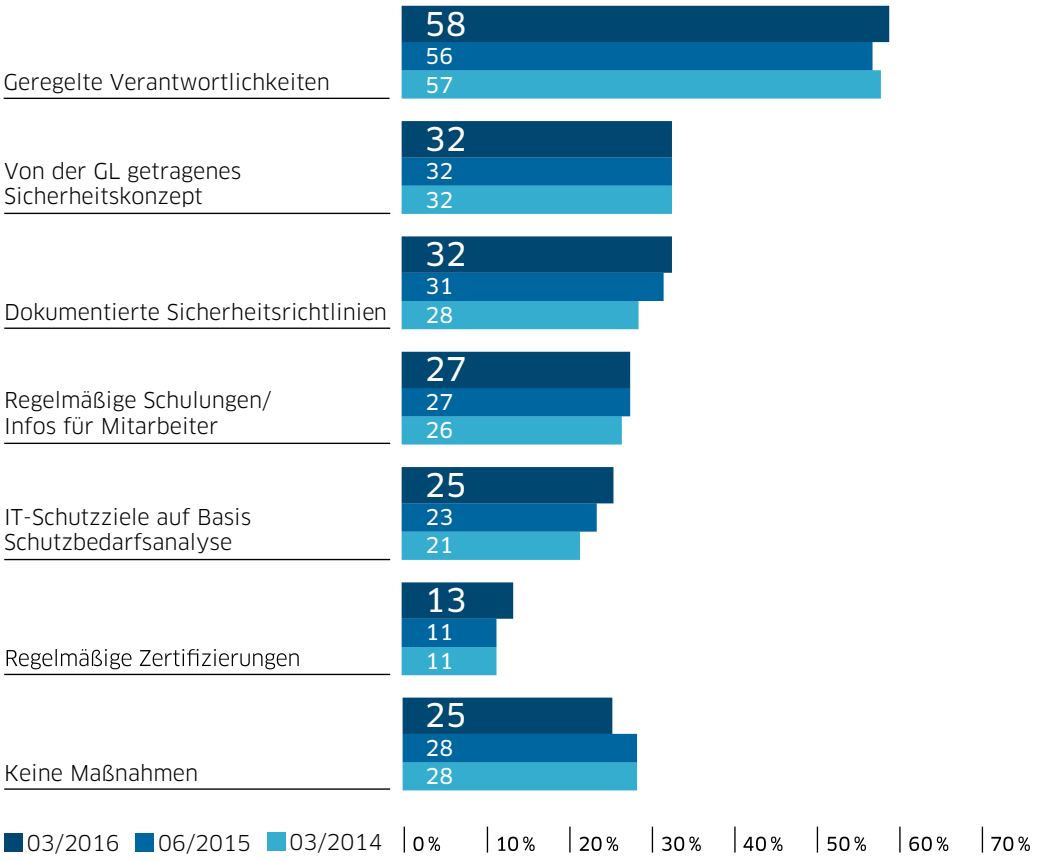



**Abb. 15: Organisatorische Maßnahmen zu Datenschutz und Sicherheit**

Während im Dreijahresvergleich im Hinblick auf die *Regelung von Verantwortlichkeiten* nunmehr mit 58% (2014: 57%, 2015: 56%) kaum Veränderungen zu beobachten sind sowie die Etablierung von *Geschäftsleitung getragenen Sicherheitskonzepten* in allen drei Erhebungsjahren mit 32% konstant bleibt, zeichnet sich eine leicht positive Tendenz bezüglich *Dokumentierter Sicherheitsrichtlinien und IT-Schutzziele auf Basis Schutzbedarfsanalysen* um je plus 4 Prozentpunkte seit 2014 ab. Dies deutet darauf hin, dass sich Unternehmen ihrer Verantwortung vor allem für die für ein Gesamtkonzept unbedingt nötigen organisatorischen Maßnahmen zur Stärkung der IT-Sicherheit in Ansätzen bewusster werden.

## Sicherheitsfaktor Mitarbeiter: Potentiale ausschöpfen

Als organisatorische Maßnahme zu Datenschutz und Datensicherheit und für eine Etablierung einer nachhaltigen Sicherheitskultur in KMU bedarf es regelmäßiger Schulungen und Informationen für Mitarbeiter. Allerdings sind hierbei keine positiven Entwicklungen zu verzeichnen und nur rund ein Viertel (27%) aller Mitarbeiter werden adäquat zu möglichen Gefahren und Schutzmaßnahmen geschult (2014: 26%, 2015: 27%). Diese Stagnation ist vor dem Hintergrund der Zunahme von Angriffen, die auf die Schwachstelle Mitarbeiter ausgerichtet sind, besonders ungünstig. Dabei ist Aufklärung der Mitarbeiter die beste Maßnahme gegen bekannte Angriffsmethoden wie Erpressersoftware oder Social Engineering, also der gezielten Manipulation von Mitarbeitern, um an Daten des Unternehmens zu gelangen.

Lediglich

**58 %**

der KMU verfügen über geregelte Verantwortlichkeiten beim Datenschutz.

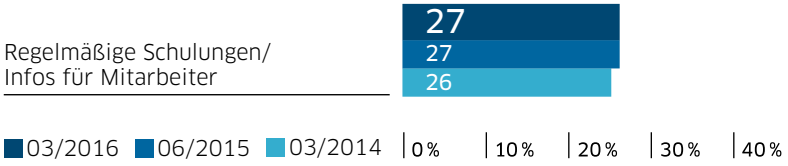



**Abb. 16: Auszug: Organisatorische Maßnahmen zu Schulung von Mitarbeitern**

Der Faktor Mitarbeiter spielt auch bei anderen Schutzvorkehrungen eine Rolle: Die Digitalisierung fordert immer weitere Zugriffe von unterschiedlichsten Endgeräten und Personen auf Unternehmensdaten. Die rechtlichen Regelungen durch Datenschutz und Compliance erfordern daher ein effektives und umfassendes Benutzer- und Rechteverwaltungssystem. Die Notwendigkeit einer *Benutzerverwaltung* sollte bei den Unternehmen daher ausdrücklicher platziert werden. Die derzeitige Entwicklung scheint auch hier zu stagnieren: Benutzerverwaltung als Schutzmaßnahme erfährt im Vergleich zum Vorjahr zwar einen Zuwachs um drei Prozentpunkte auf 77% (2014: 76%); dem gegenüber stehen allerdings immer noch 23%, die diese effektive und wichtige Schutzmaßnahme nicht berücksichtigen und die Datensicherheit im eigenen Unternehmen somit leichtfertig gefährden.

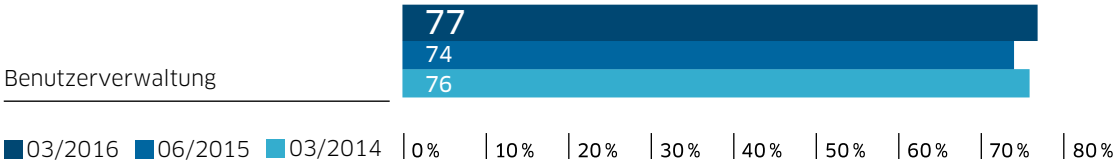



**Abb. 17: Auszug IT-Sicherheitslage: Vorhandene Schutzmaßnahmen Benutzerverwaltung**

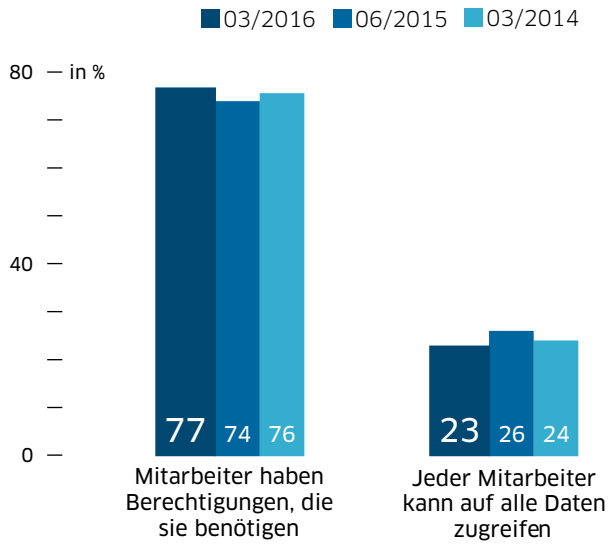



**Abb. 18: Regelung der Nutzungsrechte für Mitarbeiter**

Weiterhin verfügen mit 77% knapp drei Viertel der Mitarbeiter (2014: 76%, 2015: 74%) laut der aktuellen Umfrage über die Berechtigungen, die sie zur Ausübung ihrer Aufgaben benötigen – somit kann in immerhin noch 23% der Unternehmen jeder Mitarbeiter auf alle Daten zugreifen. Damit weist auch dieser Aspekt aus Sicht der IT-Sicherheit noch einen deutlichen Nachholbedarf auf.

**23%**

der Mitarbeiter haben Zugriff auf ALLE Daten.

Eine weiterhin bestehende Schwachstelle deutet sich in diesem Zusammenhang bei der Schutzmaßnahme *Organisation/Compliance* ab. Diese Schutzmaßnahme konnte im Vergleich zu den Vorjahren (2014 und 2015: 72%) um zwei Prozentpunkte zulegen, liegt aktuell bei 76%. Diese Schutzmaßnahme bildet zusammen mit *E-Mail-Sicherheit* und *Benutzerverwaltung* immer noch das Schlusslicht in der Gesamtbetrachtung.

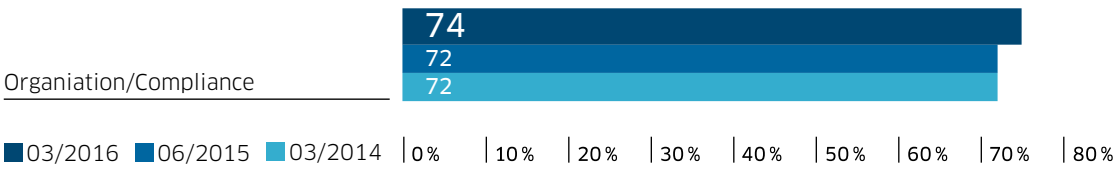



**Abb. 19: Auszug IT-Sicherheitslage: Vorhandene Schutzmaßnahme Organisation/Compliance**

## Mangelndes Bewusstsein für reaktive Maßnahmen und Gesamtkonzepte

Betrachtet man die Entwicklung der Maßnahmen, IT betriebsfähig zu halten, gestalten sich die ermittelten Werte größtenteils ebenso zeitstabil. Hervorzuheben ist der weiterhin niedrige Wert für *Schnelle Reaktion im Notfall*, der bei 61% verharrt (2014 und 2015: 60%). Unabhängig der präventiven Maßnahmen, die von KMU ergriffen werden, deutet dies auf ein fehlendes Bewusstsein für die Bedeutung reaktiver Maßnahmen im Ernstfall hin. Reaktive Maßnahmen zählen zu einer robusten IT-Sicherheitskultur ebenso dazu wie präventive Maßnahmen und bedürfen vor diesem Hintergrund zukünftig besonderer Beachtung.

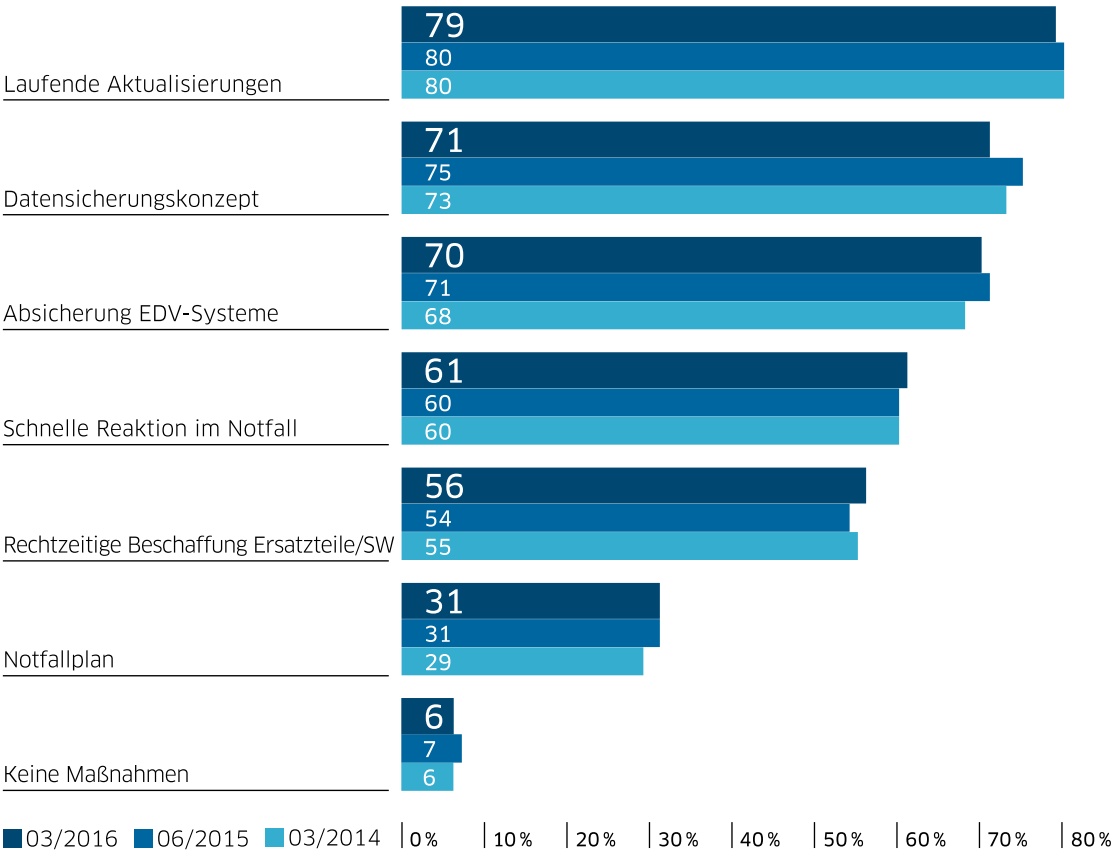



**Abb. 20: Maßnahmen, um IT betriebsfähig zu halten**

Ein Gesamtkonzept bzw. Management (*Notfallplan*) ist wie im Vorjahr nicht im Fokus der Unternehmen: Noch nicht einmal ein Drittel (31%) der befragten KMU gaben an, über einen Notfallplan zu verfügen (2014: 29%, 2015: 31%). Nach wie vor bestimmen Einzelmaßnahmen das Bild, die IT-Lauffähigkeit sicher zu stellen. Einen wirksamen IT-Grundschutz, wie er beispielsweise vom BSI empfohlen wird, bilden die isolierten Anwendungen dabei nicht.

Aber auch bei präventiv ausgerichteten, ganzheitlichen organisatorischen Schutzvorkehrungen herrschen stagnierende bzw. rückläufige Werte. Ungeachtet der vermehrten Sicherheitsvorfälle in den vergangenen Jahren – über die beispielswiese die SiBa-App von DsiN täglich informiert – sind keine signifikanten Veränderungen des Anteils (79%) jener Unternehmen festzustellen, die *laufende Aktualisierungen* durchführen (2014 und 2015: 80%).

Nur

**31 %**

der Unternehmen mit Notfallplan.

**28%**

der KMU führen KEINE zeitnahen Aktualisierungen durch.

Auch im *Aktualisierungsverhalten von Sicherheitsupdates* zeigen sich kaum Veränderungen: rund zwei Drittel (68%) der KMU (2014: 70%, 2015: 69%) installieren sofort nach der Freigabe der Updates durch die Hersteller/Anbieter selbige. Dieser Wert ist über den Betrachtungszeitraum betrachtet allerdings eher rückläufig, was Anlass zur Besorgnis gibt. Gar 28% der Unternehmen (2014 und 2015: 27%) führen eine zeitnahe Aktualisierung gar nicht durch. In Anbetracht der generellen Bekanntheit von Sicherheitslücken in vorhandener Software kann dies als fahrlässig beurteilt werden. Hier ist ein disziplinierteres Verhalten der Unternehmen förderlich.

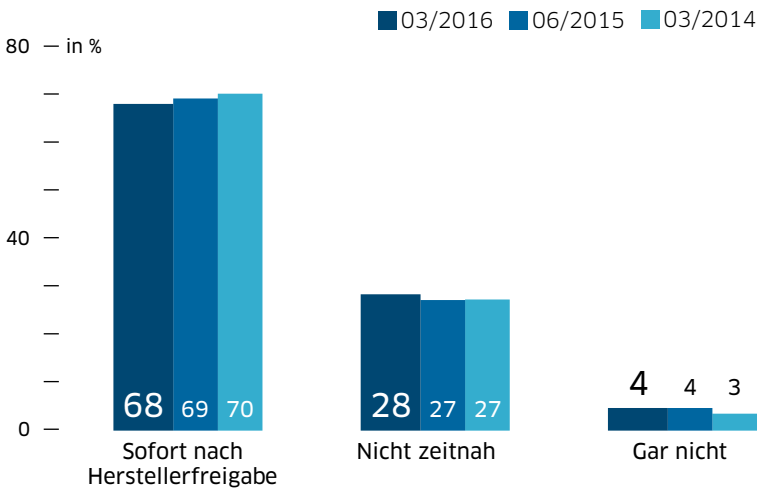



**Abb. 21: Aktualisierung der IT-Systeme mit den relevanten Sicherheitsupdates**

## Ausgesuchte DsiN-Angebote

→ **Leitfaden Sicher im Netz**
Grundlagen für einen ganzheitlichen IT-Schutz in KMU (mit DATEV).
www.dsin.de/downloads/sicher-im-netz

→ **Leitfaden mit Verhaltensregeln zur Informationssicherheit für Mitarbeiter**
Dient als Grundlage für die Entwicklung eines eigenen Sicherheits-Gesamtkonzeptes (mit DATEV).
www.dsin.de/downloads/verhaltensregeln-zur-informationssicherheit

→ **Bottom-Up: Berufsschüler für IT-Sicherheit**
Zielt auf die Schulung von Auszubildenden in KMU ab.
www.dsin-berufsschulen.de

# Sicherungsmaßnahmen versus wirksame Umsetzung

**Sicherungskonzepte sollten für einen effektiven Schutz selbstverständlich den entwickelten Standards und Vorgaben der entsprechenden Einrichtungen und Experten folgen. Die aktuellen Ergebnisse der Studie deuten an, dass die Umsetzung in den Unternehmen diesen Empfehlungen und Vorgaben oftmals nicht zu folgen scheint. Als Ursachen kommen bislang unzureichende Aufklärung und Informationen über die entsprechenden Anforderungen an Betriebe in Betracht.**

Das Vorhandensein eines *Datensicherungskonzepts* weist einen Rückgang um 4 Prozentpunkte im Vergleich zum Vorjahr auf (2014: 73%, 2015: 75%) und liegt aktuell bei 71 % der befragten kleinen und mittleren Unternehmen. Diese Umkehr ist in mehrfacher Sicht bedenklich: Die Bedeutung von Daten und damit auch die Risiken für Unternehmen nehmen mit der fortschreitenden Digitalisierung zu. Die zunehmende Verbreitung von Erpressersoftware verdeutlicht diesen Trend. Weitere Aufklärungsarbeit verspricht in diesem Bereich eine zeitnahe Dividende für die Sicherheitslage.

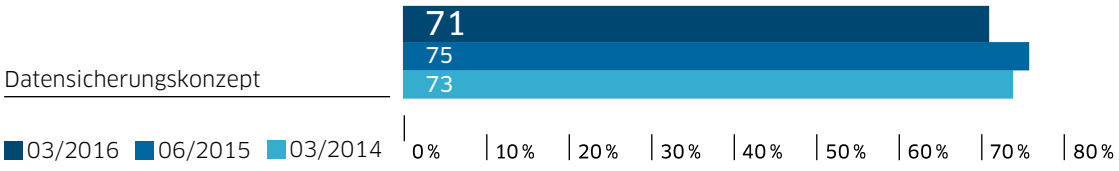



**Abb. 22: Maßnahme Datensicherungskonzept, um IT betriebsfähig zu halten**

Grundsätzlich wird eine positive Entwicklung bezüglich der Sicherungshäufigkeit und der Prüfung der Funktionsfähigkeit der Datensicherung im Dreijahresvergleich sichtbar. Deutlich wird, dass ein vorhandenes Datensicherungskonzept nachweislich positiven Einfluss auf beide Aspekte nimmt: Während von Unternehmen ohne Datensicherungskonzept im Jahr 2016 lediglich 57% eine Sicherung täglich bzw. 19% permanent durchführen sowie 49% teilweise und 36% regelmäßig die Funktionsfähigkeit prüfen, sind es bei Unternehmen mit Datensicherungskonzept immerhin 64%, die täglich und 21% die permanent ihre Daten sichern sowie 49%, die teilweise und 40%, die regelmäßig ihre Datensicherung auf Funktionsfähigkeit überprüfen.

## Datensicherungskonzepte effektiv umgesetzt?

Allerdings fallen die positiven Effekte eines vorhandenen Datensicherungskonzepts auf das Verhalten der Unternehmen nicht so eindeutig aus, wie man es vermuten würde, sehen doch gerade die bestehenden IT-Sicherheitskonzepte in puncto Permanenz und Regelmäßigkeit eindeutige Anforderungen vor, die sich bei einer effektiven Implementierung entsprechend in den Ergebnissen widerspiegeln müssten: Für die permanente Durchführung einer Datensicherung beläuft sich der Unterschied auf lediglich 2 Prozentpunkte. Dies wirft die Frage auf, inwieweit Unternehmen ihre Datensicherungskonzepte entlang der Vorgaben wie die des BSI hinsichtlich eines IT-Grundschutzes ausrichten und diese auch so umsetzen.

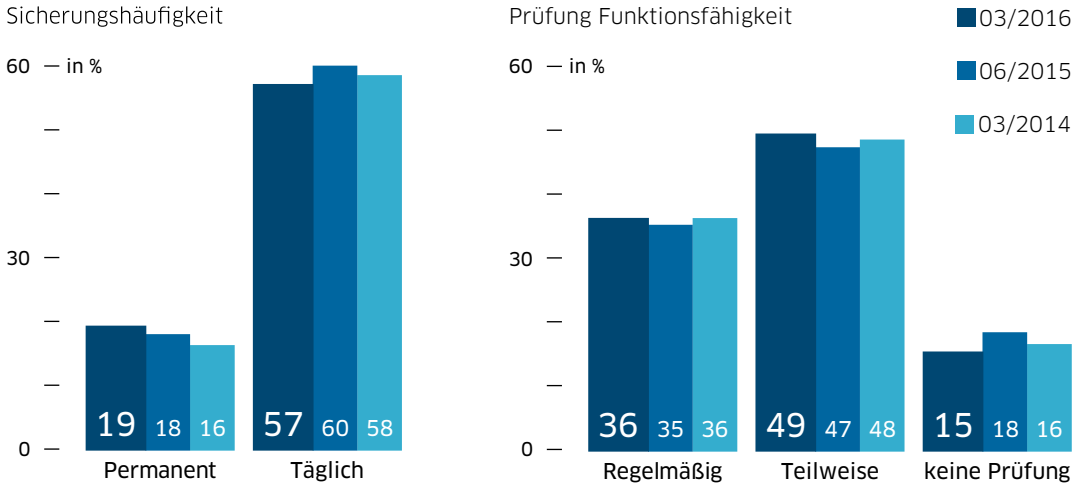



**Abb. 23: Datensicherung, wenn kein Datensicherungskonzept vorhanden ist**

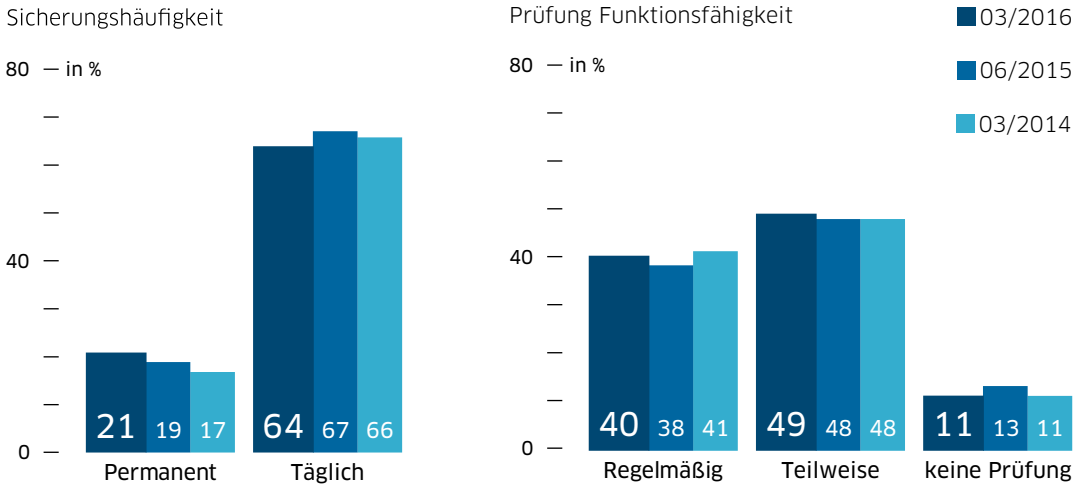



**Abb. 24: Datensicherung bei vorhandenem Datensicherungskonzept**

# Verantwortungs-bewusstsein für IT-Sicherheit bei KMU verzeichnet Anstieg.

Generell bleibt ein Anstieg des Verantwortungsbewusstsein für die IT-Sicherheit bei Unternehmen zu verzeichnen, der sich an einer weiteren Stelle ankündigt: weiterhin werden mehr Spezialfirmen beauftragt (35%), Datenträger fachgerecht zu entsorgen (2014: 31%, 2015 35%). Im Dreijahresvergleich macht dies immerhin ein Plus von vier Prozentpunkten aus. Allerdings bleibt festzuhalten, dass der Gesamtwert mit knapp über einem Drittel noch keinen Anlass zur Zufriedenheit gibt und weitere Anstrengungen nötig sind, Unternehmen auf die Notwendigkeit eines bewussten Umgangs mit Daten und Datenträgern aufmerksam zu machen.

**35%**

der KMU lassen Datenträger von Spezialfirmen entsorgen.

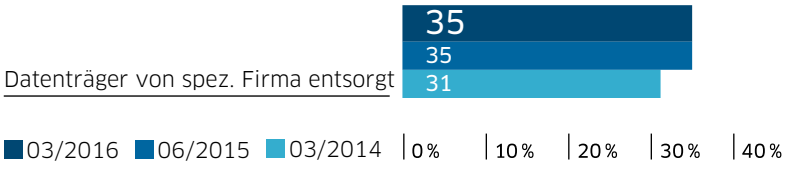



**Abb. 25: Auszug: Entsorgung von Datenträgern mit vertraulichem Inhalt**

## Ausgesuchte DsiN-Angebote

→ **Workshopreihe „IT-Sicherheit@ Mittelstand“**
Praxisvorträge zur IT-Sicherheit für KMU-Entscheider in IHKs (mit DIHK).
www.dsin.de/it-sicherheit-mittelstand


→ **IT-Grundschutz des BSI**
Der IT-Grundschutz vom BSI ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.
www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

## Kapitel 3

# Im Fokus: IT-Sicherheit durch Verantwortung verstärken

Die stagnierenden Sicherheitsvorkehrungen bieten Cyberkriminellen viele Angriffsvektoren. Um die IT-Sicherheit nachhaltig zu stärken, reichen Einzellösungen alleine nicht aus. Gesamtheitliche Sicherheitskonzepte können durch Aufklärungs- und Informationskampagnen vermittelt werden. Maßnahmen wie Mitarbeiterschulungen können einfach implementiert werden – mit großer Wirkung für die IT-Sicherheit.

**Handlungsbedarf bei Aufklärungsmaßnahmen für Erstellung von Gesamtkonzepten erkennbar.**

# Fazit

Die Studie zeigt hier einen Handlungsbedarf bei Sicherheitsmaßnahmen in allen Gruppen von kleinen und mittleren Unternehmen. Dies reicht von grundlegenden Aufklärungsmaßnahmen für die individuelle Planung und die strategische Ausrichtung bei der Erstellung eines Gesamtkonzepts für die IT-Sicherheit und erstreckt sich bis auf die Hilfestellung in der konkreten Umsetzung der Pläne. Zudem müssen auf die konkreten Anforderungen an die einzelnen Schutzmaßnahmen sowie die Gesamtkonzepte für einen nachhaltigen IT-Schutz hingewiesen werden, damit Unternehmen von entsprechenden Umsetzungen in der Praxis in der Tat profitieren.

Die mehrheitlich stagnierenden Werte in der Erhebung zeigen, dass die öffentlichen Diskussionen über Sicherheitsvorfälle und die tägliche Berichterstattung über Angriffe von Cyberkriminellen keine gravierenden Verbesserungen im Sicherheitsverhalten bewirken. Lediglich der Rückgang bei einzelnen Diensten wie dem Online-Banking im geschäftlichen Alltag könnte auf einer gestiegenen Vorsicht von Unternehmen im Hinblick auf IT-Sicherheit beruhen. Entsprechende Informationskampagnen zum sicheren Einsatz von Online-Banking im Geschäftsalltag können hier ansetzen, um Sicherheit und Vertrauen gleichermaßen zu verbessern.

# Schwerpunkt: Organisatorische Maßnahmen

**Vermittlung von Sicherheitswissen an Mitarbeiter Baustein für IT-Sicherheit im Unternehmen.**

Wie den Ergebnissen dieses Berichts zu entnehmen ist, bleiben organisatorische Maßnahmen ein Schwerpunkt, um IT-Sicherheit und Datenschutz zu verbessern: leicht positive Tendenzen sind hier erkennbar. Zu beachten ist, dass organisatorische Maßnahmen tief in die Unternehmensabläufe eingreifen und in der Regel längere Zeit für die Umsetzung erfordern; dies erfolgt dabei meist durch externe Unterstützung (Beratung). Ganzheitliche Sicherheitskonzepte umfassen im Wesentlichen auch die Einbindung der Organisation – hier könnte sich auch zukünftig deutlicher das Vorhandensein von ganzheitlichen Sicherheitskonzepten in Unternehmen abzeichnen.

Aufklärungsmaßnahmen haben weiterhin die Fragen zu Sicherheit und vertraglichen Regelungen sowie Datenschutzanforderungen bis zu Abhängigkeiten zu externen Dienstanbietern zu adressieren. Neben Hinweisen zu präventiven Maßnahmen ist auch die Behandlung reaktiver Maßnahmen im Falle eines Angriffs in ein Gesamtkonzept einzubauen. Die in der letzten Zeit vermehrt stattfindenden Angriffe über Erpressersoftware zeigen, dass Unternehmen oftmals die nötigen Informationen fehlen, was im Falle eines erfolgten Angriffs am besten zu tun ist.

Bestehende Defizite bei den Mitarbeiterschulungen sind bedauerlich, stellen ungeschulte Mitarbeiter doch für viele Unternehmen die wesentliche Sicherheitslücke dar. Dabei zahlen diese Investitionen doppelt in die IT-Sicherheit der Unternehmen ein: Durch die fortschreitende Digitalisierung des Geschäftsalltags steigen die Herausforderungen an Unternehmen weiterhin, ihre Mitarbeiter IT-fit zu halten. Mehr noch: gerade Angriffsvektoren über Social Engineering beweisen, dass Angreifer die Mitarbeiter von heute als Schwachstelle bereits identifiziert haben, und so versuchen, an Daten oder Geld der Unternehmen zu gelangen. Diese Tendenz ist eher ansteigend.

Die Vermittlung von Sicherheitswissen im Unternehmen ist ein Baustein für IT-Sicherheit – neben technologischer Innovation für IT-Schutzvorkehrungen und Regulierungsmaßnahmen. Alle drei Faktoren wirken zusammen: Im Dialog zwischen allen Beteiligten können Anknüpfungspunkte geschaffen werden, um das gemeinsame Ziel einer verbesserten IT-Sicherheitskultur in KMU zu erreichen.

# Was Unternehmen tun können

**Das bereits bestehende Angebot für KMU zur Entwicklung einer resistenten Sicherheitskultur sowie der Weiterbildung der Mitarbeiter ist umfangreich. Auch DsiN bietet hier konkrete Angebote, die zur freien Verfügung stehen und kleinen Unternehmen im geschäftlichen Alltag ein effektives Hilfsmittel sein können.**

## DsiN-Cloud-Scout

Der DsiN-Cloud-Scout bietet vorrangig kleinen und mittleren Unternehmen eine wichtige Online-Orientierungshilfe und deckt dabei wirtschaftliche, technische und rechtliche Aspekte ab. Der Fragebogen dient als erste Orientierung und ersetzt keine individuelle Sicherheitsanalyse. Die Nutzer erhalten in zehn bis fünfzehn Minuten eine individuelle Auswertung und Empfehlung zur Nutzung von Cloud Computing mit Fokus auf IT-Sicherheit und Datenschutz. Dazu werden zusätzlich Links zu verlässlichen Quellen zur Verfügung gestellt.



www.dsin-cloudscout.de

## DsiN-Blog – Der IT-Sicherheitsblog für den Mittelstand

Der Sicherheitsblog bündelt die wichtigsten News zum Thema IT-Sicherheit. Ausgewählte Experten nehmen zu IT-Sicherheitsthemen Stellung und informieren mit ihrem Know-how speziell den Mittelstand. Der Blog ist außerdem eine Kommunikationsplattform, auf der Nutzer Fragen stellen und sich mit Experten und anderen Nutzern austauschen können. Der Sicherheitsblog für den Mittelstand wird vom Verein Deutschland sicher im Netz e.V. angeboten und von DATEV eG betreut.


www.dsin-blog.de


www.sicher-im-netz.de/siba

## SiBa – Das IT-Sicherheitsbarometer

Die kostenfreie SiBa-App stellt Meldungen zu aktuellen IT und Internet-Risiken mit passenden Sicherheitstipps für den digitalen Alltag bereit. Kurz und bündig werden Sofortmaßnahmen sowie konkrete Schutzmöglichkeiten aufgezeigt. Die Nutzerfreundlichkeit der App wird durch verständliche Formulierungen sichergestellt, die auch komplexere Sachverhalten einfach erklärt und einordnet. Meldungen können über eine Teilen-Funktion schnell und einfach an Bekannte und Freunde weitergeleitet werden.


www.sicher-im-netz.de/
it-sicherheit-mittelstand

## Workshopreihe IT-Sicherheit @ Mittelstand

Die Workshopreihe über IT-Sicherheitsfragen im Unternehmen von DsiN und dem Deutscher Industrie- und Handelskammertag (DIHK) richtet sich an Geschäftsführer und Entscheider in KMU. Im Mittelpunkt stehen Motivation, Befähigung und praktische Umsetzung von IT-Sicherheitsmaßnahmen. Erfahrene Referenten vermitteln praxisnahe Tipps für mehr Sicherheit in kleinen und mittleren Unternehmen.

# Deutschland sicher im Netz e.V.

DsiN wurde 2006 im Nationalen IT-Gipfel der Bundesregierung gegründet mit dem Ziel, einen konkreten Beitrag für mehr digitale Sicherheit von Verbrauchern und im Mittelstand zu leisten. Dazu entwickelt der Verein Initiativen und Handlungsversprechen, die er im Verbund mit seinen Mitgliedern und Partnern umsetzt – für mehr Schutz, Sicherheit und Vertrauen.

Mit der Digitalen Aufklärung 2.0 stellt der Verein Aufklärungsangebote bereit, die auf die Bedürfnisse der Anwender eingehen. Als produktunabhängige Plattform für Aufklärungsinitiativen beteiligen sich Unternehmen, Verbände und gesellschaftliche Initiativen bei DsiN. Seit 2007 hat der Bundesminister des Innern die Schirmherrschaft inne.

In der Digitalen Agenda der Bundesregierung wurde ein Ausbau der Zusammenarbeit und Unterstützung von DsiN beschlossen. Schon heute verstärkt DsiN permanent seine Aufklärungsarbeit: Für Unternehmen startete 2015 eine bundesweite Workshopreihe in landesweiter Kooperation mit den IHK unter der Schirmherrschaft des BMWi.

www.sicher-im-netz.de

# Impressum

**DsiN-Sicherheitsmonitor Mittelstand 2016**

Eine Studie von Deutschland sicher im Netz e.V. gemeinsam mit DATEV eG

**Verantwortlich**
Dr. Michael Littger

**Verfasser**
Stefan Brandl und Mara Zimmermann (DATEV)
Nadine Grau, Sascha Wilms, Nils Engler (DsiN)

**Gestaltung**
REUTER × BOBETH GbR

**Stand**
Oktober 2016

Deutschland sicher im Netz e.V.
Albrechtstr. 10 b
10117 Berlin
www.sicher-im-netz.de
info@sicher-im-netz.de

Gemeinsam mit:

DATEV