DsiN SicherheitsMonitor 2015 Mittelstand

IT-Sicherheitslage 2011 bis 2015

Schirmherrschaft:

Bundesministerium des Innern

DsiN Deutschland sicher im Netz

www.sicher-im-netz.de

Prof. Dieter Kempf

Dr. Michael Littger

Digitale Aufklärung 2.0 – wann, wenn nicht jetzt?

Zum fünften Mal stellt Deutschland sicher im Netz im Sicherheitsmonitor die Entwicklung der IT-Sicherheitslage im Mittelstand vor. Wir freuen uns, dass bis heute rund 7.300 Unternehmen das kostenfreie Angebot zum IT-Sicherheitscheck genutzt haben, um einen fundierten Einstieg in Sicherheitsfragen zu erhalten – sowie als Grundlage für die vorliegende Erhebung.

Die diesjährigen Ergebnisse bekräftigen: Die Digitalisierung gehört in kleinen und mittelständischen Unternehmen längst zum betrieblichen Alltag – und nimmt weiter an Fahrt auf. Bedauerlicherweise sind die Vorkehrungen für IT-Sicherheit nicht im gleichen Maße mitgewachsen, sondern stagnieren oder waren sogar rückläufig.

Damit wird klar, dass öffentliche Debatten über Sicherheitsvorfälle, etwa im Bundestag, oder die Enthüllungen über die NSA keine unmittelbaren Auswirkungen auf die Sicherheitspraxis in Unternehmen haben. Die Studie liefert vielmehr Hinweise, dass die öffentliche Wahrnehmung einen „Fatalismus-Effekt“ bewirkt und Schutzbemühungen sogar in Frage stellen kann.

Umso mehr sind Unternehmen, gesellschaftliche Verbünde und auch Verbände aufgefordert, die Anstrengungen für eine digitale Aufklärung gerade jetzt zu verstärken und voranzubringen. Denn es gibt keinen Zweifel: Der Mittelstand trägt einen Großteil der Verantwortung zum digitalen Selbstschutz; darin wollen wir ihn – gemeinsam mit allen Beteiligten aus Wirtschaft, Gesellschaft und Politik – unterstützen.

Mit der Digitalen Aufklärung 2.0 lädt Deutschland sicher im Netz dazu ein, mittelständische Unternehmen bei ihren konkreten Bedürfnissen nach Schutz, Sicherheit und Vertrauen abzuholen und sie zu Sicherheitsmaßnahmen zu motivieren und zu befähigen.

Machen Sie mit und werden Sie Teil des Engagements für digitale Aufklärung – weil es sich lohnt!

Eine anregende Lektüre wünschen Ihnen

Prof. Dieter Kempf
Beiratsmitglied Deutschland sicher im Netz
Vorsitzender des Vorstands DATEV eG.

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

Studienziel und -design

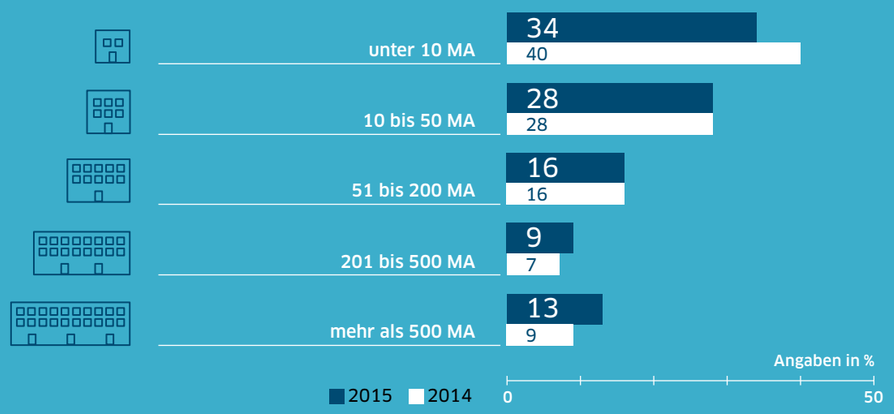
Der DsiN-Sicherheitsmonitor Mittelstand ermittelt seit 2011 die IT-Sicherheitslage in kleinen und mittelständischen Unternehmen (KMU) und identifiziert Schwachstellen, um wirksame Aufklärungsmaßnahmen für digitalen Schutz zu entwickeln.

Der Untersuchungszeitraum über fünf Jahre ermöglicht eine zuverlässige Betrachtung von Trends der IT-Sicherheit, die auch die Einordnung von kurzfristigen Ausschlägen erleichtern. Seit 2011 haben ca. 7.300 Unternehmen am DsiN-Sicherheitscheck teilgenommen, davon 1.308 Unternehmen im aktuellen Erhebungszeitraum April 2014 bis Juni 2015.

Größte Teilnehmergruppe im aktuellen Erhebungszeitraum waren Unternehmen mit bis zu 50 Mitarbeitern (62 %), gefolgt von Unternehmen zwischen 51 und 500 Mitarbeitern mit insgesamt 25 %. Die Gruppe der Unternehmen mit über 500 Mitarbeitern ist gegenüber dem Vorjahr von 9 auf 13 % angestiegen.

Die aktuellen Ergebnisse ermöglichen auch eine fundierte Gesamtsicht auf die IT-Sicherheitslage im Mittelstand, um daraus wirksame Aufklärungsstrategien zu entwickeln. Im Vordergrund stehen Maßnahmen, die Mitarbeiter sensibilisieren und zu Schutzmaßnahmen befähigen und motivieren. Die Ergebnisse sind eine wichtige Grundlage für die Arbeit von DsiN.

Der Untersuchung liegt der DsiN-Sicherheitscheck zu Grunde, mit dem sich kleine und mittelständische Unternehmen einen Überblick über ihren IT-Sicherheitsstatus verschaffen können. Der standardisierte und anonymisierte Online-Fragebogen wurde von DsiN mit seinen Mitgliedern BITKOM, DATEV, SAP und Sophos entwickelt.



↑ Abb. 1: Befragte Unternehmen nach Anzahl der Mitarbeiter

Inhalt

Zusammenfassung

Zentrale Ergebnisse

Stagnation der Schutzvorkehrungen seit 2011

Der DsiN-Sicherheitsmonitor zeigt im fünften Jahr seiner Erhebung eine deutliche Stagnation von Schutzvorkehrungen zur IT-Sicherheit in mittelständischen Unternehmen auf. Er liefert wichtige Anknüpfungspunkte für eine erfolgreiche Aufklärungsarbeit.

Nachdem die Ergebnisse der vergangenen drei Jahre noch eine positive Tendenz vermuten ließen, hat sich diese Entwicklung aktuell nicht fortgesetzt. Angesichts des hohen Digitalisierungsgrades bei den befragten Unternehmen sowie auch verstärkter öffentlicher Diskussionen über Sicherheitsvorfälle könnte dieses Ergebnis widersprüchlich anmuten.

Das vermeintliche Paradox markiert, dass die objektive Relevanz von IT-Sicherheit und subjektives Empfinden allein noch keine Auswirkungen auf die Praxis im Unternehmen entfalten – sondern sogar einer fatalistischen Grundstimmung Vorschub leisten könnten, nach der Sicherheitsmaßnahmen als „ohnehin nicht lohnend“ empfunden werden.

Die wachsende Digitalisierung drückt sich etwa in der stärkeren Nutzung von Sozialen Medien in Unternehmen aus – diese stieg um 4 %-Punkte auf aktuell 42 % – sowie einem nahezu ungehemmten Einsatz von E-Mail für geschäftskritische Korrespondenzen.

Schutzvorkehrungen, die den gestiegenen Risiken im angemessenen Rahmen entgegenwirken könnten, wurden hingegen nicht im gleichen Maße ergriffen. Dies gilt sowohl für technische Maßnahmen der Verschlüsselung oder Authentifizierung wie auch für organisatorische Vorkehrungen. Fast jedes zehnte Unternehmen verzichtete auf jegliche Vorkehrung.

Im Fokus der Untersuchung liegen auch die geschäftliche Praxis von Cloud Computing, die Nutzung mobiler Geräte und die Verschlüsselung der Kommunikation. Auch hier zeigt sich eine gewisse Diskrepanz zwischen den gestiegen Anforderungen an IT-Sicherheit einerseits und der tatsächlich im Unternehmen gelebten Praxis andererseits.

Die Ergebnisse bieten zahlreiche Anknüpfungspunkte für die Aufklärungsarbeit von Deutschland sicher im Netz und seinen Partnern. Sie bestätigen insbesondere die Verschiebung von reinen „Awareness-Kampagnen“ hin zur Vermittlung von konkretem Sicherheitswissen und Unterstützungsangebote zur Umsetzung vor Ort – unter dem Begriff der Digitalen Aufklärung 2.0.

Kapitel 1

Wachsende Digitalisierung – stagnierender IT-Schutz

Die Digitalisierung des Mittelstands ist seit der ersten Erhebung des Sicherheitsmonitors kontinuierlich gewachsen – und mit ihr auch die potentielle Anfälligkeit für Schadensrisiken im Unternehmen. Schutzvorkehrungen, um den Risiken der steigenden Digitalisierung entgegenzuwirken, halten aber nicht Schritt. Tatsächlich stagnierten die Maßnahmen für IT-Sicherheit im vergangenen Jahr überwiegend oder waren sogar rückläufig.

Wachsende Digitalisierung – stagnierender IT-Schutz

Die Digitalisierung hat zur Sättigung bei der Verbreitung einiger Dienste geführt, während andere Bereiche wie Cloud Computing weiter hinterherhinken. IT-Schutzmaßnahmen konnten mit dieser Entwicklung nicht Schritt halten, sondern stagnierten oder waren rückläufig.

In
80 %
der Unternehmen sind Notebooks im Einsatz.

Der Einsatz vernetzter Geräte und Infrastrukturen in Unternehmen konnte im vergangenen Jahr nochmals leicht zulegen. Auffällig ist die gestiegene Verbreitung der Notebook-Nutzung um 6 %-Punkte auf 80 %. Ein geringer Zuwachs war auch bei Smartphones und Netbooks zu verzeichnen, während die meisten anderen Anwendungen konstant blieben.

↑ Abb. 2: Digitalisierung des Geschäftsalltags

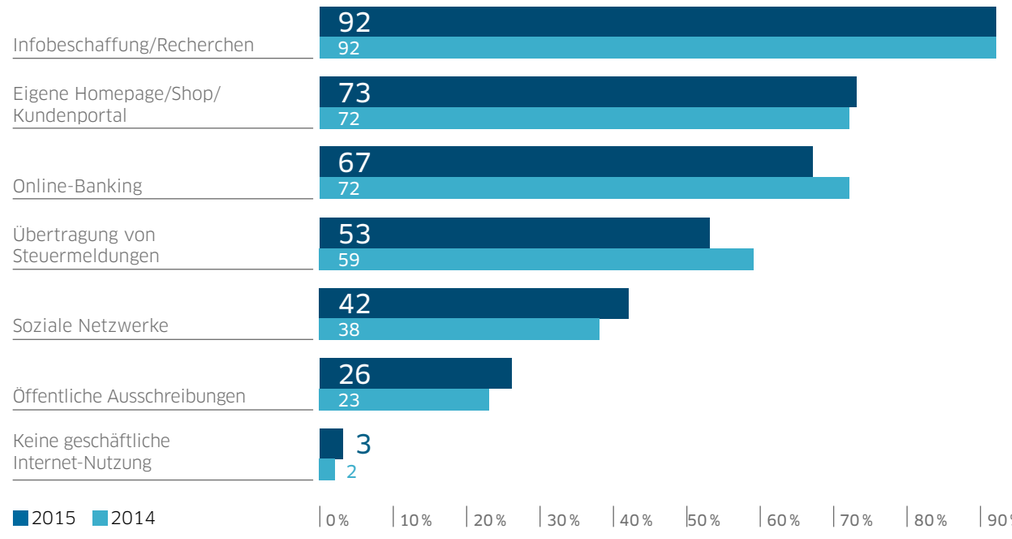
Zu den intensiv genutzten Online-Anwendungen gehörten – gleichbleibend gegenüber 2014 – die Informationsrecherche mit 92 %, gefolgt vom Aufbau eigener Homepages sowie von Einkaufs- und Kundenportalen mit 73 %. Deutlich zugenommen hat die Verwendung Sozialer Netzwerke im Unternehmen um 4 %-Punkte auf 42 %.

Auffällig ist der Nutzungsrückgang bei einigen datensensiblen Diensten, darunter Onlinebanking und Steuermeldungen. Während die Abwicklung von Finanzgeschäften in 2015 um 5 %-Punkte auf aktuell 67 % sank, ging die Übertragung von Steuermeldungen sogar um 6 Punkte auf jetzt nur noch 53 % zurück. Diese Entwicklung könnte auf einer gestiegenen Verunsicherung durch öffentliche Diskussionen über Sicherheitsvorfälle beruhen.

Überraschend ist die weiterhin nur schwache Verbreitung des Cloud Computing im Mittelstand, die auch im vergangenen Jahr auf konstant niedrigem Niveau verharrte (dazu ausführlicher Kapitel 3/ S. 22).

Stagnierender IT-Schutz trotz gewachsener Verunsicherung

Bei einer insgesamt starken Digitalisierung und steigenden Verunsicherung sind die tatsächlich getroffenen Sicherheitsvorkehrungen unzureichend. Deuteten die Zwischenmessungen in den letzten drei Jahren noch eine positive Tendenz an, so hat sich diese



↑ Abb. 3: Geschäftliche Internet-Nutzung

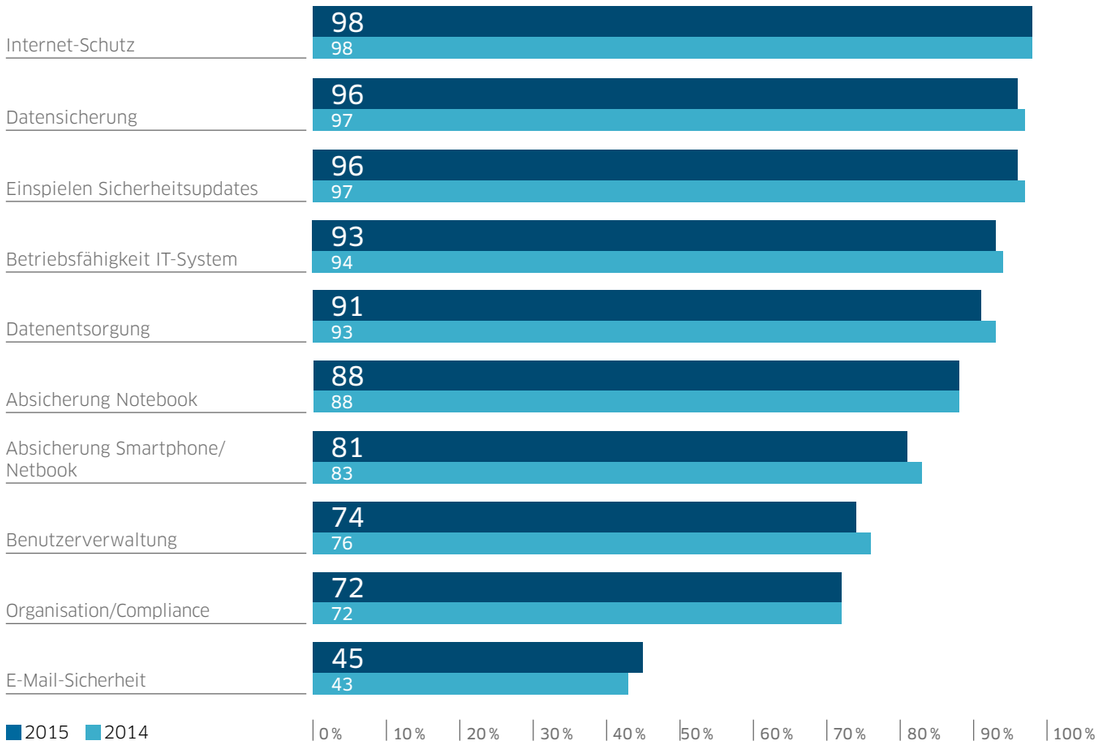
nicht fortgesetzt. Die meisten Werte sind entweder stagnierend oder sogar rückläufig. Dies gilt für Basismaßnahmen wie allgemeine Datensicherung, Internetschutz und Sicherheitsupdates wie auch für weitergehende Maßnahmen wie der Absicherung von mobilen Arbeitsgeräten und Smartphones – letztere wurden bei einem Rückgang um 2 %-Punkte nur noch von 81 % der Befragten gesondert geschützt.
Sorgenkind bleiben die mangelnden Vorkehrungen beim Schutz von E-Mails. Diese verharren auf einem besorgniserregend niedrigen Niveau von 45 %. Besonders erstaunlich ist, dass im Jahr 2011 bereits 50 % der Unternehmen angaben, Schutzvorkehrungen bei E-Mails vorzunehmen – dies entspricht einem Rückgang um 5 %-Punkte in den vergangenen fünf Jahren.

Die Ergebnisse zeigen, dass die Befassung mit digitalen Sicherheitsvorfällen in der Öffentlichkeit keineswegs zu einer höheren Bereitschaft bei der Umsetzung von Schutzmaßnahmen führt. Die öffentlich diskutierten IT-Sicherheitsvorfälle – zuletzt der Hackerangriff auf den Deutschen Bundestag im Juni 2015 – sowie die fortgesetzten Enthüllungen über NSA-Aktivitäten förderten insgesamt eher eine gewisse Passivität in vielen Unternehmen; ein hoher Sicherheitsgrad scheint vielen kaum erreichbar.

Die Notwendigkeit wirksamer Aufklärungsmaßnahmen bleibt damit ungebrochen hoch. Über eine reine Sensibilisierung hinaus müssen die Befähigung und Motivation zur Umsetzung verstärkt im Vordergrund stehen.

-6
%-Punkte der Unternehmen nutzt digitale Steuermeldungen

1 I Wachsende Digitalisierung – stagnierender IT-Schutz



↑ **Abb. 4: IT-Sicherheitslage: vorhandene Schutzmaßnahmen**

Ausgesuchte DsiN-Angebote

→ **DsiN-Workshopreihe „IT-Sicherheit@ Mittelstand“ in Kooperation mit DIHK**
Praxisvorträge zur IT-Sicherheit für KMU-Entscheider in lokalen IHKn
sicher-im-netz.de/it-sicherheit-mittelstand

→ **DsiN-Sicherheitscheck**
Überblick zum Stand der IT-Sicherheit im eigenen Unternehmen mit hilfe eines Online-Fragebogens
sicher-im-netz.de/dsin-sicherheitscheck

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

Kapitel 2

IT-Sicherheit: Gesamtkonzept versus Einzelbausteine

Die steigende Digitalisierung im Mittelstand birgt wachsende Risiken für jedes Unternehmen sowie auch für die Wirtschaft insgesamt – durch Systemausfälle, den Verlust der Vertraulichkeit von Information oder von deren Integrität.

Ein wirksamer IT-Grundschutz, wie er auch vom Bundesamt für Sicherheit in der Informationstechnik verfolgt wird, erfordert zahlreiche Bausteine, deren volle Wirkung sich aber erst im Zusammenspiel entfaltet.

IT-Sicherheit: Gesamtkonzept versus Einzelbausteine

Grundsätzlich begründet die steigende Digitalisierung im Mittelstand neue Verletzlichkeiten für Unternehmen und die Wirtschaft – sei es durch Ausfälle der Verfügbarkeit, den Verlust der Vertraulichkeit von Information oder von deren Integrität.

Einem wirksamen IT-Grundschutz, wie er beispielsweise vom Bundesamt für Sicherheit in der Informationstechnik empfohlen wird, liegen verschiedene Bausteine zu Grunde. Sie erfordern ganzheitliche IT-Sicherheitskonzepte, die mehr als die Summe der Einzelbausteine darstellen.

Gleichwohl verzichten viele Unternehmen auf ein Gesamtkonzept und verlassen sich auf vereinzelte Komponenten, die sich meist technischen oder organisatorischen Maßnahmen zuordnen lassen. Dieser Trend lässt sich über die gesamten fünf Jahre seit der ersten Erhebung erkennen.

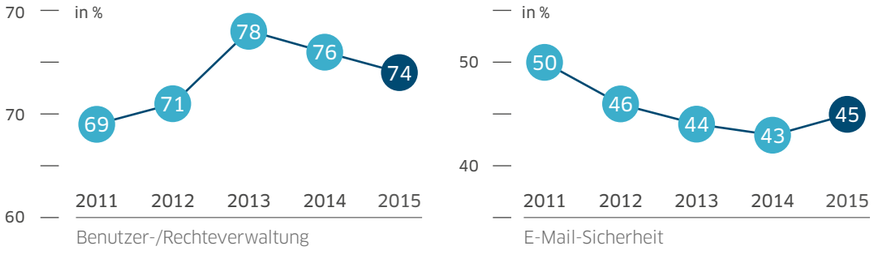
Demnach finden technische Grundmaßnahmen generell eine größere Verbreitung als organisatorische oder mitarbeiterbezogene Vorkehrungen. Hier lag der Internetschutz (2011 und 2015: 98 %) auf konstant hohem Niveau wie auch das Einspielen von Sicherheitsupdates (2011: 95 %, 2015: 96 %).

Organisatorische Maßnahmen wie die Rechteverwaltung im Unternehmen (2011: 69 %, 2015: 74 %) oder Compliance (2011: 69 %, 2015: 72 %) verharrten hingegen auf vergleichsweise niedrigerem Niveau. Vorkehrungen zur E-Mail-Sicherheit wurden lediglich von 50 % (2011) bzw. 45 % (2015) der Befragten getroffen.

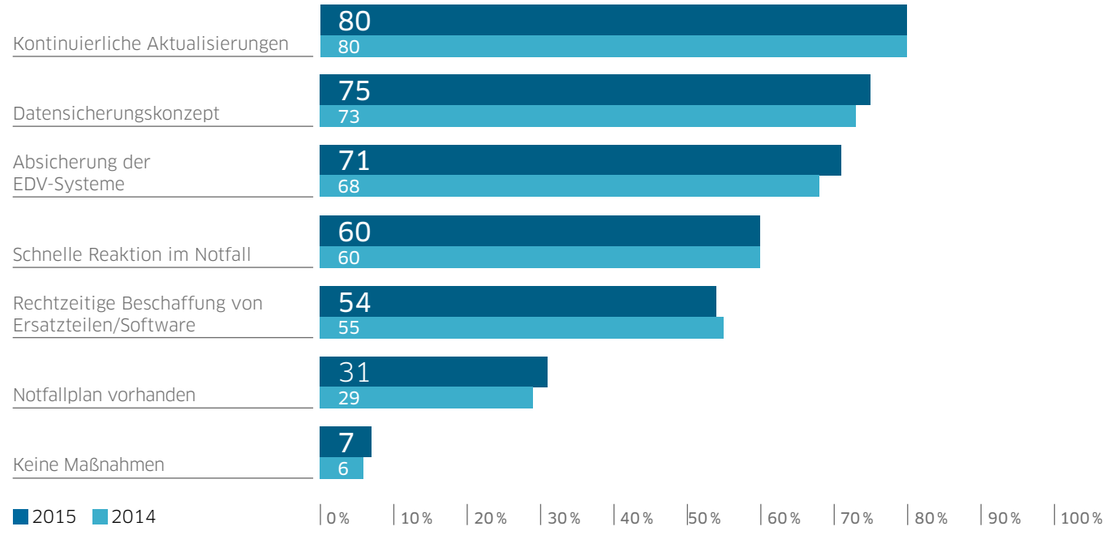
2015: Einzelbausteine überwiegen

Beim Einsatz von Einzelbausteinen stagnieren Art und Umfang der Sicherheitsvorkehrungen. Die rechtzeitige Beschaffung von sicherheitsrelevanten Komponenten verharrte bei 54 %, ebenso wie der Einsatz von Datensicherungskonzepten, der bei 75 % lag. Über eine Absicherung ihrer EDV-Systeme gegen Ausfälle verfügten zwei Drittel der Unternehmen.

Der isolierten Anwendung einzelner Sicherheitskomponenten entspricht, dass zwei von drei Unternehmen auf Notfallpläne



↑ Abb. 5: Fünf-Jahres-Vergleich technischer und organisatorischer IT-Schutzmaßnahmen



↑ Abb. 6: Maßnahmen zur Absicherung der Betriebsfähigkeit der IT

mit einem zusammenhängenden Gesamtkonzept verzichteten; dieser Wert hat sich 2015 mit 31 % nur leicht gegenüber 2014 (29 %) verbessert.

Ganzheitlicher Grundschutz notwendig

Insgesamt weist das Lagebild auf eine Vernachlässigung bzw. mangelnde Bekanntheit ganzheitlicher Ansätze von IT-Sicherheit hin. Die getroffenen Schutzvorkehrungen sind vielfach wohl eher punktuelle Einzelmaßnahmen, die unverbunden nebeneinander stehen, statt gesamtheitliche Konzepte. Aufklärungsangebote sollten daher verstärkt darauf hinwirken, nicht nur Wissen zu Einzelmaßnahmen zu vermitteln, sondern diese auch in eine Gesamtsicht einzubetten. Gerade organisatorische und mitarbeiterbezogene Aspekte von IT-Sicherheit sollten vermehrt Gegenstand von Aufklärung werden.

Ausgesuchte DsiN-Angebote

→ Seiten-Check der Initiative-S
Prüft Internetauftritte von Unternehmen auf Schadsoftware
initiative-s.de

→ DsiN-Sicherheitscheck
Überblick zum Stand der IT-Sicherheit im eigenen Unternehmen mit hilfe eines Online-Fragebogens
sicher-im-netz.de/dsin-sicherheitscheck

→ DsiN-Pocketseminare
Vertiefender Überblick für umfassende Schutzvorkehrungen in KMU
dsin-blog.de/pocketguide

Technische Maßnahmen: Schutz der IT-Systeme

Erfreulicherweise finden technische Basismaßnahmen zur Sicherung der IT-Systeme heute bereits eine gute Verbreitung. Mit einer zunehmenden Komplexität der Maßnahmen nimmt jedoch auch ihr Einsatz erkennbar ab.

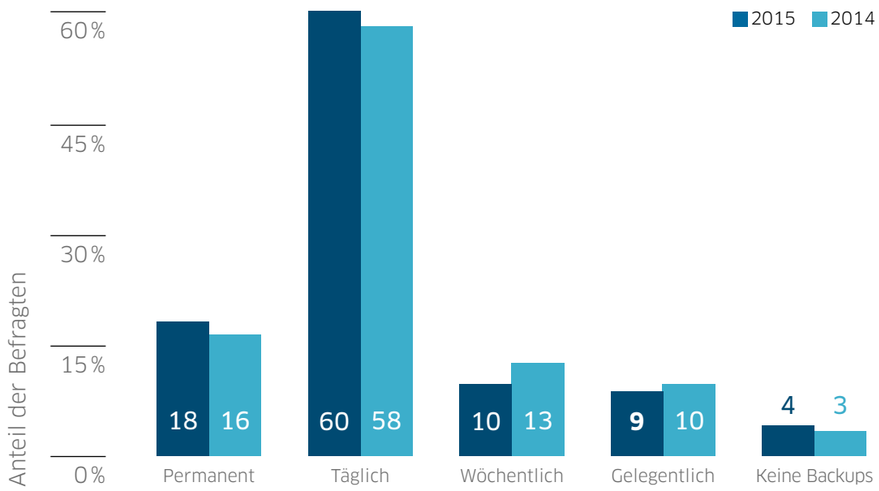
9 %

der Unternehmen sichern ihre IT-Systeme nicht zusätzlich ab.

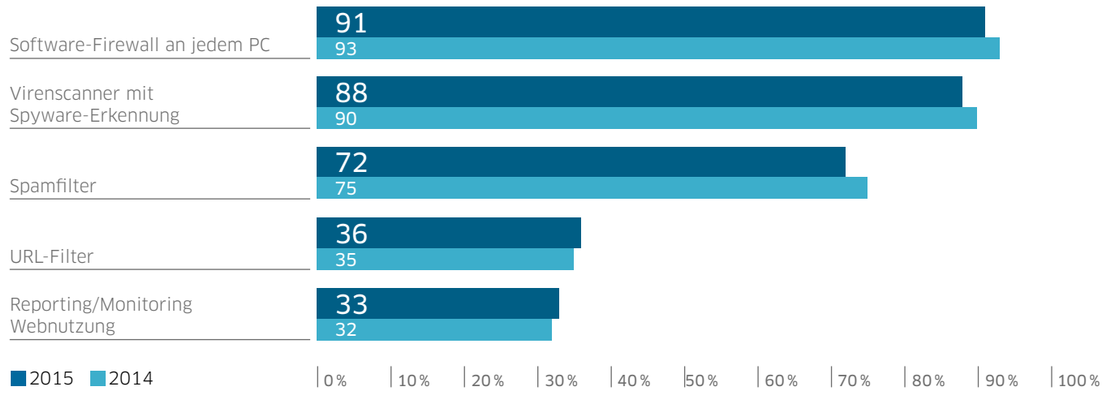
Bei den technischen Schutzmaßnahmen zeigt sich im Jahresvergleich ein insgesamt konstantes Sicherheitsniveau bei leichten Rückgangstendenzen; der Internet-Schutz, die Datensicherung und das Einspielen von Sicherheitsupdates waren bei über 95 % der Unternehmen etabliert. Standardmaßnahmen wie der Einsatz von Passwörtern wurden von konstant 84 % der Unternehmen praktiziert. Das Abschließen des Serverstandorts verblieb hingegen insgesamt auf niedrigerem Niveau (2015: 53 %).

Auffällig ist ein Rückgang komplexerer Sicherheitsmaßnahmen, wie etwa der Einsatz von Smart Cards für einen stärkeren PC-Schutz durch eine zusätzliche Authentifizierung. Dieser Wert ist gegenüber dem Vorjahr um 3 %-Punkte auf jetzt nur noch 8 % zurückgegangen. 9 % der Befragten gaben an, gar keine Sicherungsmaßnahmen für IT-Systeme vorzunehmen.

Die Anzahl der Unternehmen, die keinerlei Sicherung ihrer Datenbestände (Backups) vornehmen, lag bei 4 %. Eine permanente Datensicherung wurde von 18 % der Unternehmen durchgeführt, eine tägliche Sicherung immerhin von einer Mehrheit von insgesamt 59 %.



↑ **Abb. 7: Häufigkeit der Datensicherung in Unternehmen**

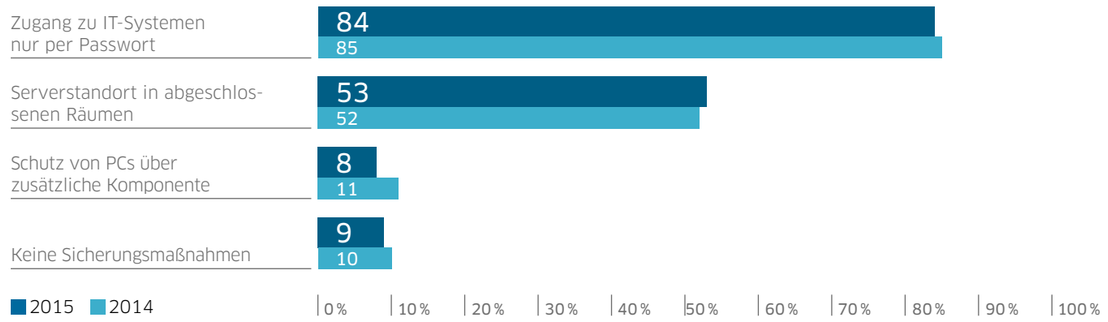


↑ **Abb. 8: Maßnahmen zur Absicherung des Internetzugangs**

Schutz vor Angriffen im Internet

Während Standards wie eine Firewall (91 %), Virenscanner (88 %) oder Spamfilter (72 %) – wenn auch leicht rückläufig – von der Mehrheit der Unternehmen verwendet wurden, kamen komplexere Anwendungen wie URL-Filter, Web-Monitoring oder automatische Angriffserkennung nur bei rund einem Drittel der Unternehmen zum Einsatz.

Obwohl technische Schutzvorkehrungen damit im Mittelstand insgesamt gut verbreitet sind, werden gerade komplexere Maßnahmen zu selten angewendet – und damit ein umfassendes technisches Schutzniveau nicht erreicht. Erforderlich ist daher eine aktive Ansprache, die die Unternehmen zu mehr Initiative befähigt und motiviert.



↑ **Abb. 9: Sicherungsmaßnahmen für IT-Systeme**

Ausgesuchte DsiN-Angebote

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

→ **DsiN-Sicherheitsbarometer**
Bündelt aktuelle Meldungen zur IT-Gefährdungslage für kleine Unternehmen
sicher-im-netz.de/sicherheitsbarometer

Organisatorische Vorkehrungen und Verantwortung

Erst das Zusammenwirken organisatorischer Vorkehrungen mit technischen Maßnahmen ermöglicht ein erhöhtes IT-Schutzniveau. Neben geregelten Verantwortlichkeiten und Mitarbeiterschulungen gehören auch Vorkehrungen zur Compliance zu den Anforderungen.

74 %

der Unternehmen regeln die Vergabe von IT-Nutzerrechten.

Knapp die Hälfte der Unternehmen im Mittelstand verzichtete auf die Regelung von Verantwortlichkeiten für Datenschutz und IT-Sicherheit, 56 % setzen dies bereits um. Nur ein knappes Drittel verfügte über ein Sicherheitskonzept, das von der Geschäftsführung getragen wird (32 %); beide Werte sind seit 2011 kaum verändert.

Überraschend erscheint, dass jedes vierte Unternehmen (28 %) vollständig auf organisatorische Maßnahmen zur IT-Sicherheit verzichtete; dieser Wert ist gegenüber 2014 konstant geblieben. Lediglich 11 % führten regelmäßige Zertifizierungen durch – ebenfalls unverändert gegenüber 2014.

Berechtigungsmanagement unterschätzt

Regelungen, die den Zugriff der Mitarbeiter auf die von ihnen benötigten Programme, Laufwerke und Daten beschränken, fehlten in jedem vierten Unternehmen. Die Anzahl der Unternehmen mit einem geregelten Berechtigungsmanagement ist seit 2014 leicht rückläufig – um 2 Punkte auf 74 %.

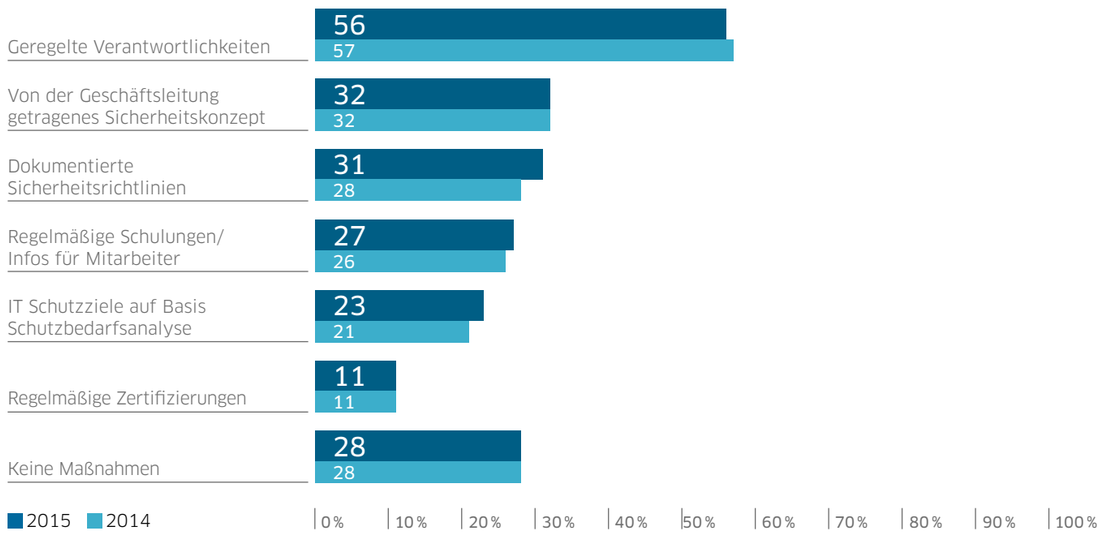


Abb. 10: Organisatorische Maßnahmen für Datenschutz und -sicherheit

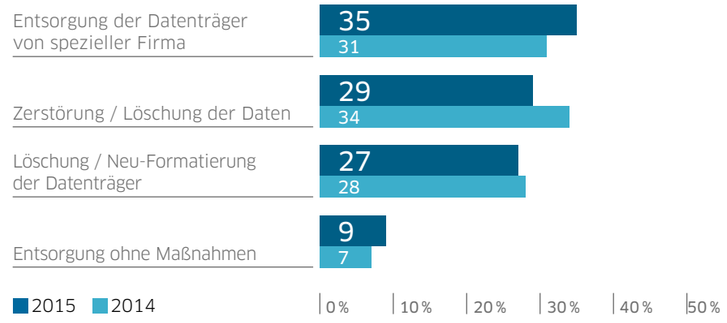


Abb. 11: Entsorgung von Datenträgern mit vertraulichem Inhalt

Die sichere Entsorgung von Datenträgern durch externe Dienstleister hat im letzten Jahr um 4 %-Punkte auf 35 % zugelegt. Fast jedes zehnte Unternehmen (9 %) verzichtete gleichwohl immer noch auf Sicherheitsmaßnahmen bei der Entsorgung von schützenswerten Daten (2014: 7 %).

Risiko durch externe IT-Geräte im Unternehmen

Im Mittelstand werden die Risiken durch die Integration externer Hardware-Komponenten in das Firmennetzwerk oftmals unterschätzt; hier droht etwa die unerlaubte Vervielfältigung von Dokumenten. Im vergangenen Jahr verzichtete mehr als jedes dritte Unternehmen auf Vorkehrungen gegen entsprechenden Missbrauch. Im selben Maße gingen Regelungen der Einbindung externer PCs zurück.

Insgesamt erfordert die Umsetzung organisatorischer Schutzmaßnahmen gut strukturierte Prozesse und klar geregelte Verantwortlichkeiten. Aufklärungsangebote müssen praktikable Lösungswege anbieten – wie Mustervereinbarungen oder Checklisten für die Auslagerung an externe Dienstleister.

Ausgesuchte DsiN-Angebote

→ Aktionsbund Digitale Sicherheit
Bündelt aktuelle Angebote und Initiativen zahlreicher Aktionspartner
aktionsbund.org

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

→ DsiN-Sicherheitsbarometer
Bündelt aktuelle Meldungen zur IT-Gefährdungslage für kleine Unternehmen
sicher-im-netz.de/sicherheitsbarometer

Sicherheitsfaktor Mensch: Social Engineering

Eine wachsende Verbreitung von digitalen Diensten im Unternehmen erhöht die Gefahr von Social Engineering – der Manipulation von Mitarbeitern. Hier greifen auch keine technischen und organisatorischen Vorkehrungen.

Einfallstore zum Social Engineering sind Soziale Netzwerke; sie wurden von 42 % der befragten Unternehmen verwendet – ein Plus von 4 %-Punkten im Vergleich zum Vorjahr. Da über den persönlichen Austausch in Sozialen Netzwerken weiterführende Angriffe erfolgen können, erfordern sie die zusätzliche Aufmerksamkeit der IT-Sicherheit – beispielsweise durch Schulungen der Mitarbeiter. Auch für Phishing-Versuche, bei denen etwa gefälschte E-Mails von vermeintlich vertrauenswürdigen Absendern empfangen werden, sollten Mitarbeiter sensibilisiert werden; ebenso für weitere Einfallstore bei der Nutzung des Internets und anderer Kommunikationskanäle.

Eine weitere potentielle Quelle für Social Engineering-Attacken sind mobile Datenträger, etwa wenn durch die gezielte Weitergabe von infizierten USB-Sticks Schadsoftware in das Unternehmensnetzwerk gelangt. 38 % der Befragten gaben an, mobile Datenträger in das Firmennetzwerk einzubinden. Noch stärker verbreitet ist der direkte Zugriff von außen auf das Firmennetzwerk mit 65 % (2014: 64 %).

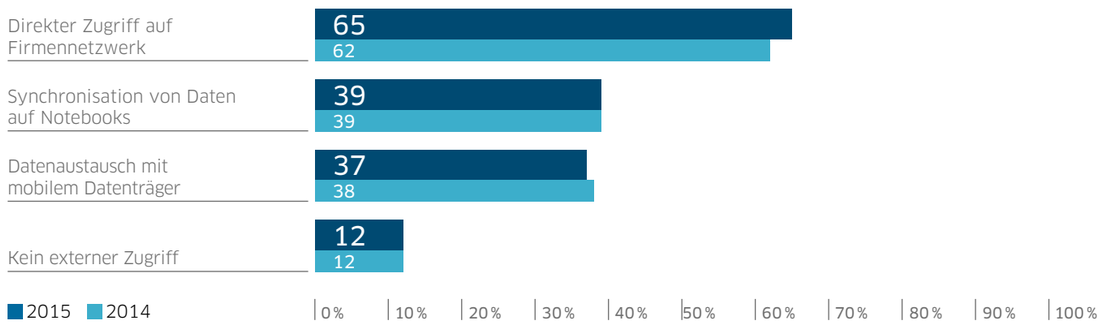


Abb. 12: Einfallstore für Social Engineering: Externer Zugriff auf das Firmennetzwerk

Kaum Gegenmaßnahmen im Unternehmen

Auf Schulungen der Mitarbeiter, um sie u. a. auch gegen Gefahren des Social Engineerings zu rüsten, verzichteten fast drei von vier Unternehmen (73 %). Über 28 % der Unternehmen ergriffen keine Maßnahmen, um Risiken durch menschliches Fehlverhalten vorzubeugen. Ein Blick auf die Entwicklung seit 2011 zeigt, dass sich die Werte in den vergangenen fünf Jahren kaum verändert haben – trotz steigender Digitalisierung. Danach wurden Schulungen im Jahr 2011 von 26 % der Unternehmen durchgeführt.

Wissensdefizite: Praktische Regularien

Die Kenntnisse der Mitarbeiter über rechtliche Anforderungen zu sicherheitsrelevanten Fragen in Unternehmen sind entsprechend schwach ausgeprägt – und sogar rückläufig. Während im Jahr 2011 noch 45 % angaben, die relevanten Regularien für IT-Sicherheit im Arbeitsumfeld zu kennen, waren dies 2015 nur noch 37 %.

Der Grund dafür könnte in der gewachsenen Komplexität von IT-Vorgaben liegen, denen sich Mitarbeiter nicht mehr gewachsen fühlen. Bei der gleichzeitig stagnierenden Vermittlung von Sicherheitswissen ist der Rückgang nahezu zwangsläufig.

73 %
der Unternehmen schulen ihre Mitarbeiter nicht zu IT-Sicherheit.

Nur
37 %
der Befragten kennt sich mit rechtlichen Anforderungen von IT-Sicherheit aus.

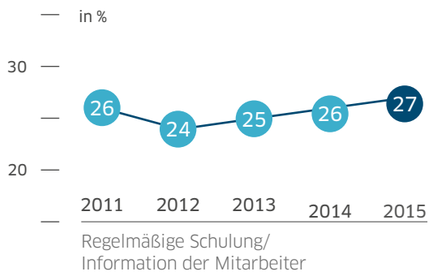
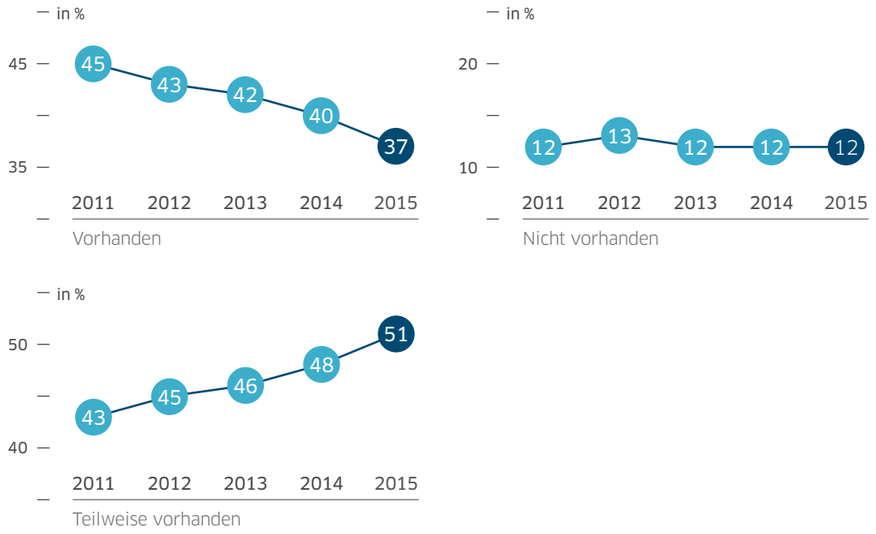


Abb. 13: Fünf-Jahres-Vergleich: regelmäßige Schulunge und Informationen

Insgesamt stellt Social Engineering einen steigenden Risikofaktor für die IT-Sicherheit in Unternehmen dar, dem nicht ausreichend Aufmerksamkeit geschenkt wird. Die Rolle der Mitarbeiter als zentraler Sicherheitsfaktor wird dabei unterschätzt. Erforderlich sind hier umfassendere Maßnahmen – von internen Sicherheitsvorgaben bis hin zur technischen Unterstützung, darüber hinaus aber auch die gezielte Schulung und Bewusstseinsbildung bei Entscheidern und Mitarbeitern.



↑ Abb. 14: Fünf-Jahres-Vergleich: Kenntnisse rechtlicher Anforderungen bei der E-Mail- und Internet-Nutzung

Ausgesuchte DsiN-Angebote

→ **Leitfaden Social Engineering**
weist auf Risiken hin und gibt Verhaltensregeln zum Umgang mit Situationen und Personen (mit Datev)
sicher-im-netz.de/downloads/social-engineering

→ **Social Media – mit Sicherheit**
Tipps zum sicheren Umgang mit sozialen Netzwerken und Blogs
sicher-im-netz.de/downloads/social-media-sicher

→ **Leitfaden mit Verhaltensregeln zur Informationssicherheit für Mitarbeiter**
dient als Grundlage für die Entwicklung eines eigenen Sicherheits-Gesamtkonzeptes (mit Datev).
sicher-im-netz.de/informationssicherheit

Kapitel 3

Im Fokus: Der digitale Geschäftsalltag

Die wachsende Digitalisierung verändert den Geschäftsalltag grundlegend. Dies bleibt nicht ohne Folgen für die IT-Sicherheit im Unternehmen.

→ Cloud Computing – ist die Basis der digitalen Vernetzung von Wertschöpfungsprozessen sowie des vereinfachten Bezugs von IT-Speicherkapazitäten, Software oder IT-Infrastrukturen.

→ Mobile Geräte und Datenträger – mehr Flexibilität für das Arbeiten durch Mobile Devices erfordert zusätzliche Schutzvorkehrungen und einen bewussteren Umgang mit den Risiken des Mobile Business.

→ Kommunikation und Verschlüsselung – der wachsende digitale Austausch auch vertraulicher und geschäftskritischer Informationen erhöht die Relevanz einer wirksamen Verschlüsselung von E-Mails in der Praxis.

Cloud Computing: Vorbehalte versus Potenziale

Cloud Computing wurde 2012 neu in die Erhebung aufgenommen. Die Ergebnisse zeigen Unterschiede zwischen Unternehmensgrößen – sowie auch Zusammenhänge zwischen Sicherheitskenntnissen und Nutzungsverhalten.

Nur

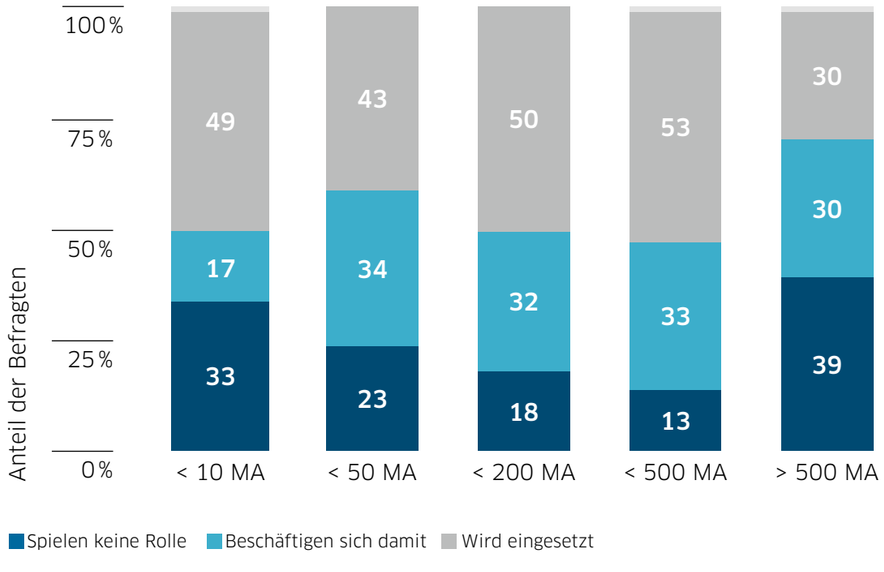
24 %

mittelständischer Unternehmen arbeiten in der Cloud.

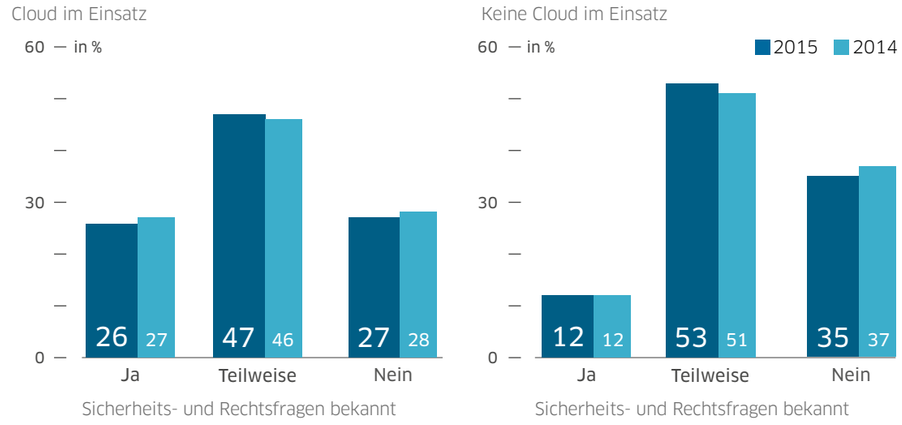
Die Verbreitung der Cloud im Mittelstand verharrte mit 24 % auf niedrigem Niveau und zeigte kaum Veränderungen gegenüber dem Vorjahr (2014: 23 %). Auch die Beschäftigung mit der Cloud ist mit fast 26 % konstant geblieben (2014: 25 %).

Überproportional häufig kamen Cloud-Anwendungen bei Unternehmen mit unter 10 Mitarbeitern zum Einsatz (33 %), wenn auch Unternehmen mit mehr als 500 Mitarbeitern die Cloud noch stärker nutzten. Die geringste Verbreitung fand die Cloud bei Unternehmen zwischen 200 und 500 Mitarbeitern – dafür stehen hier bei jedem dritten Unternehmen Planungen an. Spitzenreiter der Unternehmen, die sich mit dem Cloud-Thema befassen, waren dabei Unternehmen zwischen 10 und 50 Mitarbeitern. Zugleich spielte für knapp die Hälfte der Unternehmen mit unter 500 Mitarbeitern Cloud Computing gar keine Rolle.

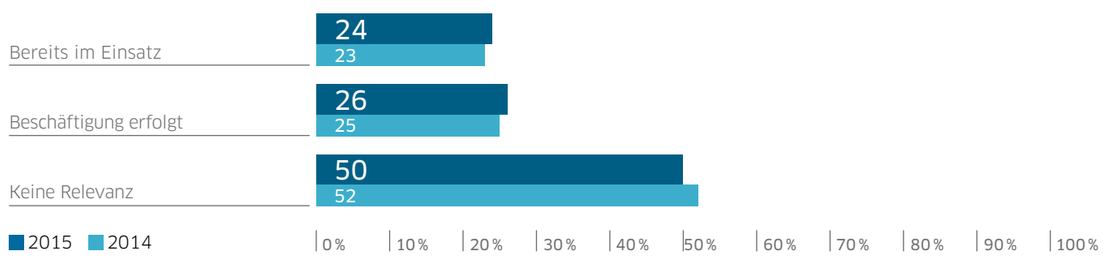
Je intensiver die Befassung mit Cloud Computing, desto stärker die Bereitschaft zur Anwendung: Nur 12 % der Befragten, die nicht in der Cloud arbeiten, hatten Kenntnisse über Sicherheitsanforderungen und rechtliche Bedingungen. Wo die Cloud zum Einsatz kommt, waren Kenntnisse bei 26 % der Befragten mehr als doppelt so stark verbreitet. Umgekehrt verfügten über 27 % der Befragten, die bereits in der Cloud sind, nach eigenen Angaben über keine Kenntnisse zu Sicherheitsanforderungen; 47 % verfügten bestenfalls über „teilweises“ Wissen; hier wird ein enormer Aufklärungsbedarf offensichtlich.



↑ **Abb. 15: Relevanz von Cloud Computing nach Unternehmensgröße**



↑ **Abb. 16: Kenntnisse über Sicherheitsanforderungen bei Cloud-Nutzung**



↑ **Abb. 17: Relevanz von Cloud Computing im Unternehmen**

Ausgesuchte DsiN-Angebote

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

→ BITKOM-Leitfaden
„Cloud Computing. Was Entscheider wissen müssen“
bitkom.org

→ DsiN-Cloud Studie
Schafft einen Überblick über den Status der Cloud-Nutzung im Mittelstand (Erscheint im November 2015)
dsin.de

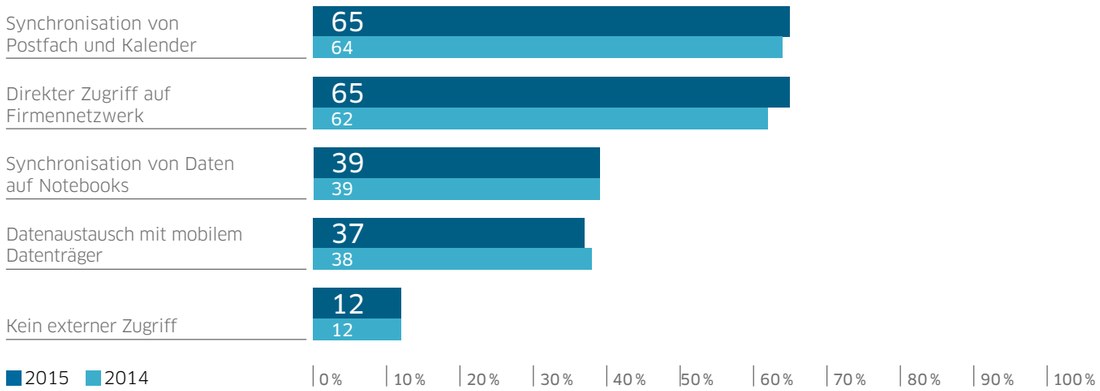
→ Seiten-Check der Initiative-S
Prüft Internetauftritte von Unternehmen auf Schadsoftware
initiative-s.de

Mobile Geräte und Datenträger: Schutz und Flexibilität

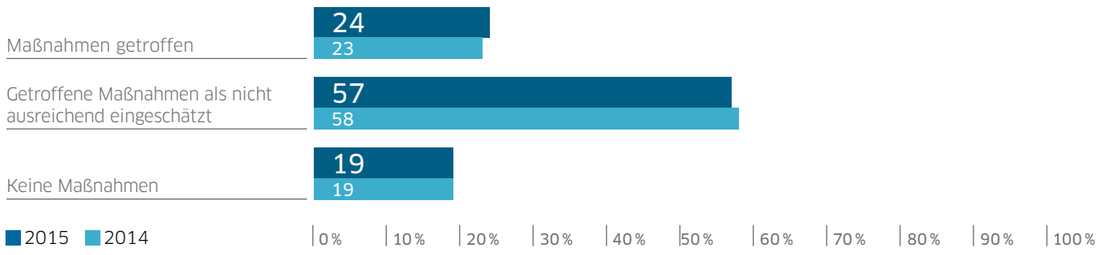
Mobile Endgeräte erleichtern das mobile Arbeiten auf Geschäftsreisen oder im Homeoffice. Zunehmend rücken auch vernetzte Geschäftsprozesse über mobile Anbindungen in den Fokus – beispielsweise die Einbindung externer Daten in Produktionsabläufe.

Externe Datenzugriffe über mobile Geräte auf das Unternehmensnetzwerk steigen weiter an. Knapp zwei Drittel der Unternehmen (65 %) synchronisierten auf diesem Weg Postfächer oder Kalender. Im selben Umfang erfolgte der direkte Zugriff auf das Firmennetzwerk für sonstige Zwecke.

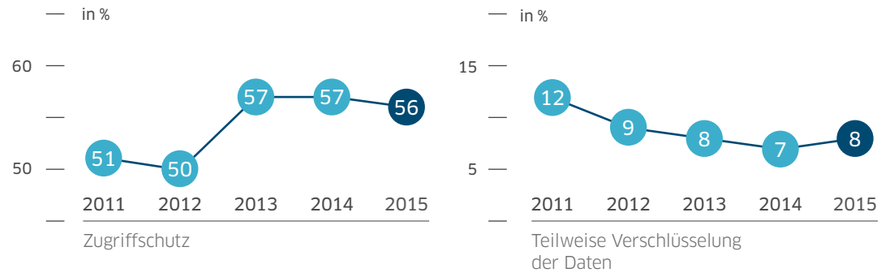
Häufigstes Medium für den Datenaustausch war die Synchronisation über Notebooks (39 %), gefolgt von mobilen Datenträgern wie USB-Sticks (37 %). Lediglich 12 % der Befragten gaben an, über keinen externen Austausch oder Zugriff auf das Unternehmensnetzwerk zu verfügen.



↑ **Abb. 18: Externer Zugriff auf das Unternehmensnetzwerk**



↑ **Abb. 19: Schutzmaßnahmen für Smartphones, Tablets und Notebooks**



↑ **Abb. 20: Fünf-Jahres-Vergleich: Notebook-Schutz vor unberechtigter Einsichtnahme**

Dieser Entwicklung liegt eine relativ hohe Verbreitung von Smartphones und Notebooks (80 %) zu Grunde; eine allgemeine, einfache Absicherung dieser Geräte lag bei 88 % (Notebooks) bzw. 81 % (Smartphones) vor.

Eine Verschlüsselung der Festplatten von Notebooks erfolgte bei nur 24 % der Befragten, eine teilweise Datenverschlüsselung bestätigten 8 % (2014: 7 %). Diese Werte haben sich über die vergangenen fünf Jahre kaum verändert. Rückläufig waren die Werte der teilweisen Verschlüsselung von Festplatten von 12 % (2011) auf 8 % (2015). Der Zugriffschutz auf Notebooks lag mit 51 % 2011 nur 4 %-Punkte unter dem heutigen Wert.

Der teilweise nur rudimentären Absicherung mobiler Geräte entsprach die Einschätzung von 57 % der Befragten, die die getroffenen Sicherheitsmaßnahmen als nicht ausreichend sicher vermuten. 19 % gaben an, gar keine Schutzmaßnahmen zu ergreifen. Diese Werte sind gegenüber dem Vorjahr nahezu unverändert.

Ausgesuchte DsiN-Angebote

→ **Leitfaden Sicheres Arbeiten von unterwegs**
Hinweise für Mitarbeiter und IT-Verantwortliche (mit Datev)
sicher-im-netz.de/downloads/sicheres-arbeiten-unterwegs

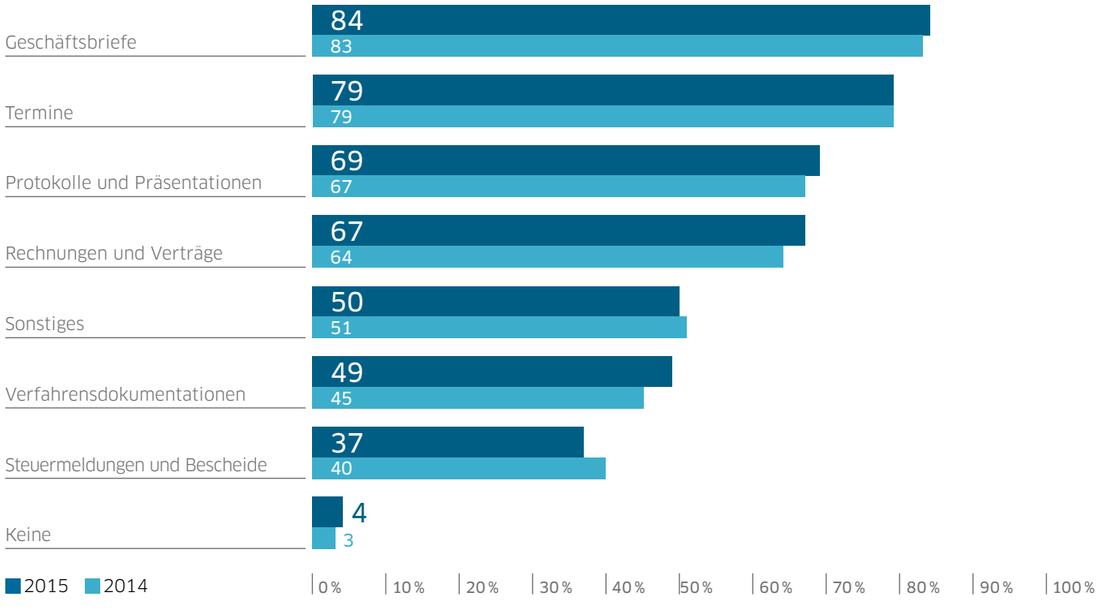
→ **Muster-Passwortkarte**
Regelkonforme Passwortbildung einfach gemacht (mit Datev)
sicher-im-netz.de/dsin-muster-passwortkarte

→ **BSI-Überblickspapier IT-Consumerisation und BYOD**
Hinweise und Empfehlungen zum geschäftlichen Einsatz privater Geräte
sicher-im-netz.de/bring-your-own-device-BSI

Kommunikation und Verschlüsselung

Mit der Digitalisierung nimmt auch die Übermittlung sensibler und geschäftskritischer Informationen zu. Bei der Vermeidung unbefugter Eingriffe kommt der Verschlüsselung von Dokumenten, Datenflüssen und von Geräten eine maßgebliche Rolle zu.

E-Mails sind weiterhin das mit Abstand meist genutzte Medium im Unternehmen, beispielsweise für den Versand von Geschäftsbriefen, Terminen, Protokollen und Präsentationen. Lediglich bei Steuermeldungen und -bescheiden ist im Vergleich zum Vorjahr ein leichter Rückgang um 3 %-Punkte auffällig.
Ungeachtet der zunehmenden Bedeutung betrieblicher Korrespondenzen sind Sicherheitsvorkehrungen in diesem Bereich teilweise stagnierend und sogar rückläufig:

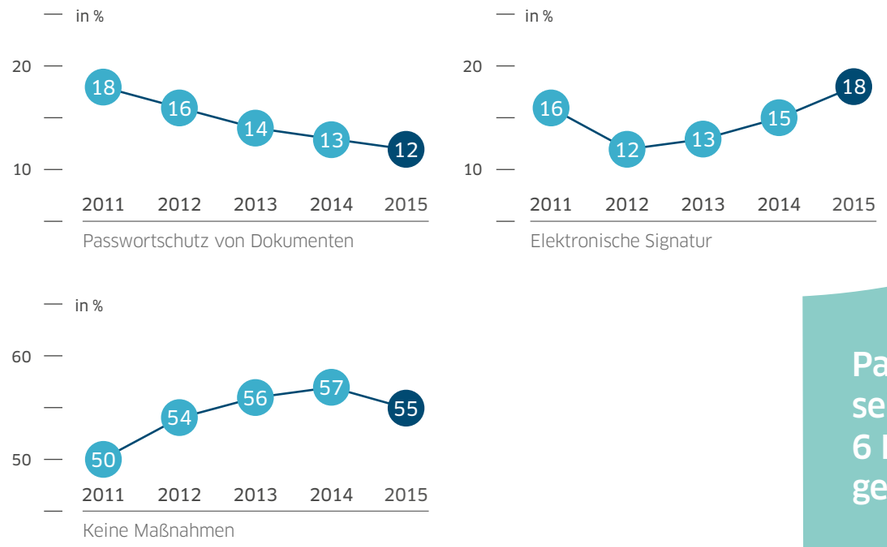


↑ **Abb. 21: Versand vertraulicher Informationen per Email**

Unverändert gaben 63 % der Befragten an, sich gar nicht oder nur teilweise mit Risiken bei der Kommunikation über das Internet zu beschäftigen – ebenso wie mit den rechtlichen Anforderungen gegen unberechtigte Einsichtnahme.

Stagniert: Verschlüsselung in der Unternehmenspraxis

Der Passwortschutz ist gegenüber 2011 (18 %) um 6 %-Punkte zurückgegangen (2015: 12 %).



↑ **Abb. 22: Fünf-Jahres-Vergleich: Datensicherung während der E-Mail-Übertragung**

Passwortschutz seit 2011 um 6 Prozentpunkte gefallen

Mehr als die Hälfte (55 %) der Befragten gab an, bei E-Mails auf jeden Schutz zu verzichten; 2011 lag der Anteil noch bei 50 %. Der Grund dafür könnte sein, dass die Sicherung des Internetzugangs irrtümlich auch als ein Schutz der E-Mails angenommen wird. Positiv ist der leichte Anstieg beim Einsatz elektronischer Signaturen – vermutlich wegen steigender Online-Steuererklärungen.

Insgesamt besteht ein enormer Handlungsbedarf bei der Absicherung von Daten und Informationen durch Verschlüsselung. Dabei geht es um Grundlageninformationen sowie die Befähigung und Motivation zur Umsetzung gleichermaßen.

Ausgesuchte DsiN-Angebote

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

→ **Leitfaden Verschlüsselung von E-Mails**
Bietet einen Überblick über die E-Mail-Verschlüsselung (mit Datev)
sicher-im-netz.de/downloads/verschluesselung-e-mails

→ **DsiN-Handlungsversprechen Verschlüsselung**
Entwickelt Initiativen rund um Verschlüsselung
sicher-im-netz.de/einfach-verschluesseln

Der IT-Sicherheitscheck

Der DsiN-Sicherheitscheck bietet einen einfachen Einstieg in zentrale Fragen der IT-Sicherheit. Der Online-Fragebogen gibt einen Überblick zum Stand der IT-Sicherheit im Unternehmen und informiert über Handlungsbedarfe.

In nur wenigen Minuten können Teilnehmer 20 Fragen rund um digitale Kommunikation mit Geschäftspartnern, die Verfügbarkeit von IT-Systemen und mobile Arbeitsweisen beantworten. Direkt im Anschluss erhalten sie die Auswertung in folgenden vier Themenbereichen:

- IT-Infrastruktur/Management
- Internet- und E-Mail-Nutzung
- Mobile Business
- IT-Sicherheits-Management/Datenschutz

Der jeweilige Handlungsbedarf wird mithilfe eines Ampelsystems signalisiert; die Befragten erhalten konkrete Hinweise, mit welchen Maßnahmen die IT-Sicherheit im Unternehmen erhöht werden kann.
Die Daten der Befragung werden anonym gespeichert; die statische Auswertung dient als Grundlage für den Sicherheitsmonitor. Der IT-Sicherheitscheck wurde in Zusammenarbeit mit den DsiN-Mitgliedern Bitkom, DATEV, SAP und Sophos erarbeitet und wird bei der DATEV gehostet

Kapitel 4

Fahrplan für Digitale Sicherheit im Mittelstand

Die Ergebnisse des DsiN-Sicherheitsmonitors zeigen Handlungsfelder für den Schutz von IT-Sicherheit im Unternehmen auf. Während die Digitalisierung in der Unternehmenspraxis weiter Raum greift, bestehen zugleich Defizite in der Absicherung von digitalen Systemen und Betriebsabläufen.

Die Studie stellt im letzten Kapitel einen Fahrplan auf, der an die konkreten Bedürfnisse von Unternehmern, IT-Verantwortlichen und Mitarbeitern anknüpft. Sie zeigt Perspektiven für eine Vernetzung bestehender Initiativen auf und beleuchtet Grenzen der Digitalen Aufklärung.

Fahrplan Digitale Aufklärung 2.0 im Mittelstand

Während die Zwischenmessungen seit 2011 in den vergangenen drei Jahren noch eine positive Tendenz aufwiesen, hat sich diese nicht weiter fortgesetzt. Damit bestätigt sich, dass die öffentliche Diskussion über Sicherheitsvorfälle allein keine positiven Änderungen im Schutzverhalten bewirkt – sondern eher Stagnation und Fatalismus bestärkt.

Mit dem Ziel einer Digitalen Aufklärung 2.0 für Unternehmen werden dazu drei Schwerpunkte adressiert, um das Engagement im Mittelstand für IT-Sicherheit zu verbessern – für eine breite und nachhaltige Digitale Sicherheit im Mittelstand.

→ Passgenaue Angebote für den Mittelstand

Um Sicherheitsmaßnahmen wirksam zu verbessern, sind Aufklärungsmaßnahmen besser auf die Bedürfnisse der Unternehmen abzustimmen. Neben der Sensibilisierung sollten praktikable Anleitungen sowie die direkte Ansprache und Motivation zur Umsetzung gerade in kleinen Betrieben eine stärkere Verbreitung finden.

→ Bündelung und Vernetzung von Initiativen

Es bestehen zahlreiche gute Initiativen und Angebote für mittelständische Unternehmen für IT-Sicherheit. Damit sie die Unternehmen wirklich erreichen, sollte eine stärkere Vernetzung stattfinden. Eine Anlaufstelle für kleine Unternehmen, an der sich bereits über 35 Partner beteiligen, bietet der Aktionsbund Digitale Sicherheit.

→ Dialog mit allen Beteiligten

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

Deutschland sicher im Netz (DsiN)

DsiN e.V. 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 am 11. September 2015 die bundesweite Workshopreihe „IT-Sicherheit @ Mittelstand“ in Kooperation mit DIHK und IHKn unter der Schirmherrschaft des BMWi.

www.sicher-im-netz.de

Impressum

DsiN-Sicherheitsmonitor Mittelstand 2015

Eine Studie von Deutschland sicher im Netz gemeinsam mit DATEV eG
Verantwortlich: Dr. Michael Littger

Verfasser: Stefan Brandl (DATEV), Dr. Michael Littger (DsiN)

Redaktion: Veronika Stumpf (DsiN)

Gestaltung: ideengut | Agentur für Kommunikation

Quellennachweise: DsiN, DATEV, © Monkey Business Images / shutterstock, © Yuri_Arcurs / iStock, © AzmanL / iStock, © laflor / iStock

Stand: September 2015

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

Gemeinsam mit:

DATEV