IT-Sicherheitslage im Mittelstand 2013

Update zur Studie von Deutschland sicher im Netz aus dem Jahr 2012

Schirmherrschaft

Bundesministerium des Innern

Ein Handlungsversprechen von

DsiN.de

gemeinsam mit

BITKOM DATEV SAP SOPHOS

Inhaltsverzeichnis

1. Einleitung

Deutschland sicher im Netz e.V. (DsiN) fördert den sicheren Umgang mit dem Medium Internet. Kennzeichnend für den Verein sind Handlungsversprechen der Mitgliedsunternehmen, die einen praktischen Beitrag für mehr Sicherheit im Internet leisten.

Die Broschüre beschreibt die Ergebnisse des „DsiN-Sicherheitschecks", der vom DsiN-Mitglied DATEV mit Unterstützung weiterer Vereinsmitglieder wie BITKOM, SAP und Sophos konzipiert wurde und seit 2010 unter dieser Adresse online verfügbar ist: https://www.sicher-im-netz.de/unternehmen/DsiN-Sicherheitscheck.aspx. Mit dem Sicherheitscheck können sich kleine und mittelständische Unternehmen (KMU) über den Stand ihrer Informationssicherheit informieren. Entsprechend der Ergebnisse erhalten die KMU produktneutrale und herstellerübergreifende Handlungsempfehlungen, um die Einhaltung von Datenschutz-und Datensicherheitsregeln zu verbessern.

Vorangegangene Studien aus den Jahren 2011 und 2012 basierten auf jeweils rund 1.400 durchgeführten IT-Sicherheitschecks. Zwischen April 2012 und März 2013 nutzten mehr als 1.500 weitere Unternehmen den Check, um sich ein Bild vom Stand ihrer Informationssicherheit zu machen. Die Daten wurden den Werten der vorangegangenen Studie von 2011/2012 gegenübergestellt.

Die Ergebnisse zur IT-Sicherheitslage der mittelständischen Unternehmen entwickeln sich im aktuellen Zeitraum insgesamt deutlich positiver. Problematisch bleiben die E-Mail-Sicherheit und die Absicherung mobiler Geräte in KMU. Trotz zunehmender Nutzung von E-Mails und mobilen Geräten stagnieren die Schutzmaßnahmen auf relativ niedrigem Level. Teilweise sinkt das Schutzniveau sogar.

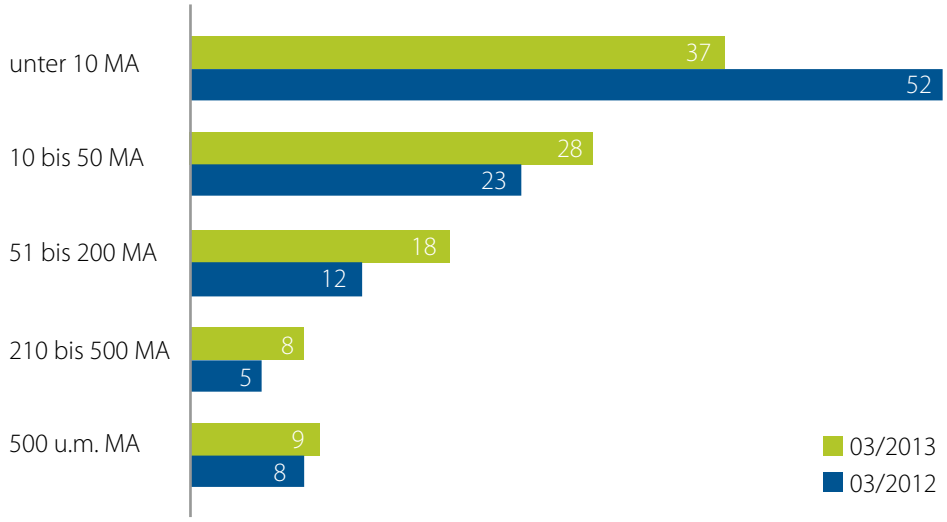
2. Die Befragung

Basis für die Auswertungsergebnisse sind 1.529 Befragungen von Unternehmen im Zeitraum vom 1. April 2012 bis 31. März 2013. Zeitraum, Fragen und Teilnehmerzahl waren nahezu identisch mit der Basis für die DsiN-Sicherheitsstudie 2012, was einen validen Zeitreihenvergleich der Ergebnisse aus beiden Jahren ermöglicht.

3. Generelle Erkenntnisse zur IT-Sicherheitslage 2012

Zusammensetzung nach Unternehmensgrößen

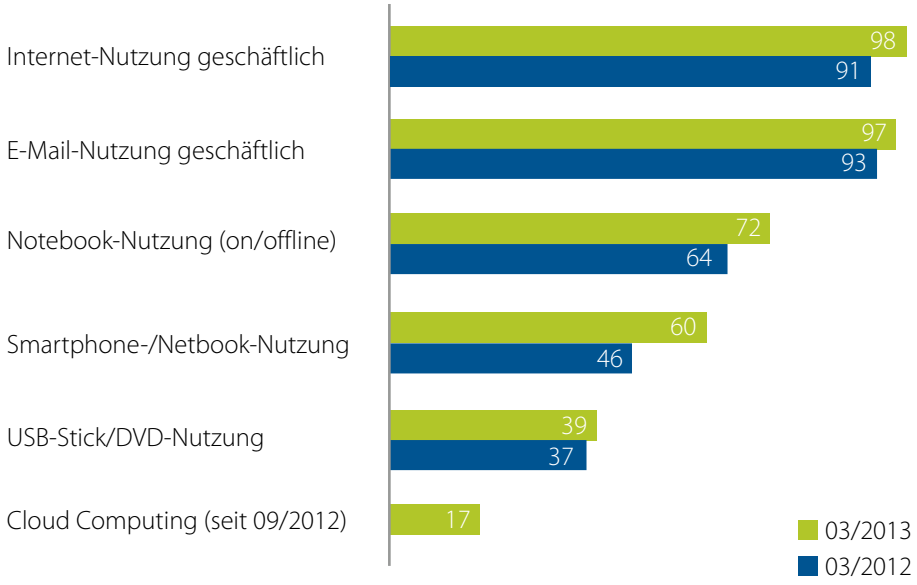
65 % (Vorjahr 75 %) der Unternehmen, die den Sicherheitscheck durchlaufen haben, sind kleine Unternehmen mit bis zu 50 Mitarbeitern. Gegenüber 2012 erhöhte sich die Größenklasse 10–50 Mitarbeiter um 5 Prozentpunkte auf 28 %, während die Größenklasse unter 10 Mitarbeiter von 52 % auf 37% abnahm. Mit 35 % (Vorjahr: 25 %) nutzen auch immer mehr größere KMU mit mehr als 51 Mitarbeitern den Sicherheitscheck. (Grafik 1).



Grafik 1: Wie viele Mitarbeiter arbeiten in Ihrem Unternehmen?

Nahezu alle Unternehmen nutzen E-Mail und Internet geschäftlich

Die Nutzung von E-Mail (97 %, 2012: 93 %) und Internet (98 %, 2012: 91 %) zu Geschäftszwecken ist auf hohem Niveau weiter gestiegen. Für KMU sind diese Medien heute unverzichtbar. Ebenfalls zugenommen hat die Smartphone-/Netbook-Nutzung, und zwar um 14 Prozentpunkte im letzten Betrachtungsjahr. Die Notebooknutzung konnte in den letzten 12 Monaten leichte Zuwächse verzeichnen (+ 8 Prozentpunkte). Stabil blieb im Vergleichszeitraum die Nutzung von USB-Sticks und DVD (Grafik 2)



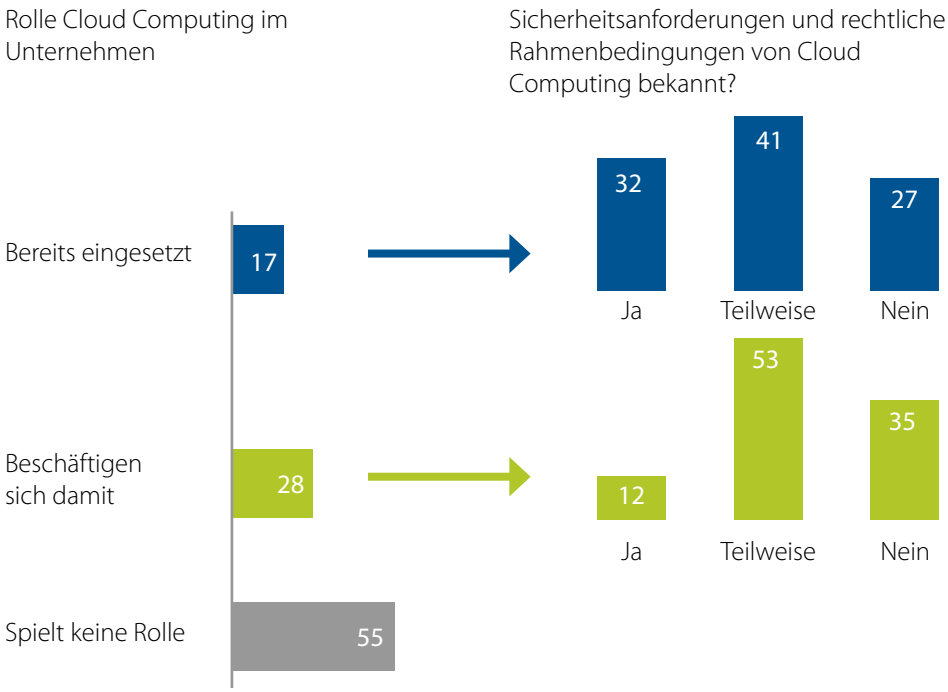
Grafik 2: Digitalisierung im Geschäftsalltag

Jedes sechste Unternehmen nutzt die Cloud

Neu in die Abfrage integriert wurde seit Oktober 2012 der Themenbereich Cloud Computing. Wie in Grafik 2 erkennbar, arbeiten bereits 17 % der befragten Unternehmen mit der Cloud. Allerdings sind 27 % der Cloud-Nutzer die Sicherheitsanforderungen und rechtlichen Rahmenbedingungen der Nutzung überhaupt nicht bekannt, 41 % kennen sie nur teilweise.

Unternehmen, die sich mit der Cloud-Nutzung beschäftigen (28 %), kennen nur zu 12 % die Sicherheitsanforderungen, 53 % sind sie teilweise bekannt, 35 % wissen nichts darüber (Grafik 3).

Für mehr als die Hälfte der befragten KMU (55 %) spielt Cloud Computing zurzeit keine Rolle.

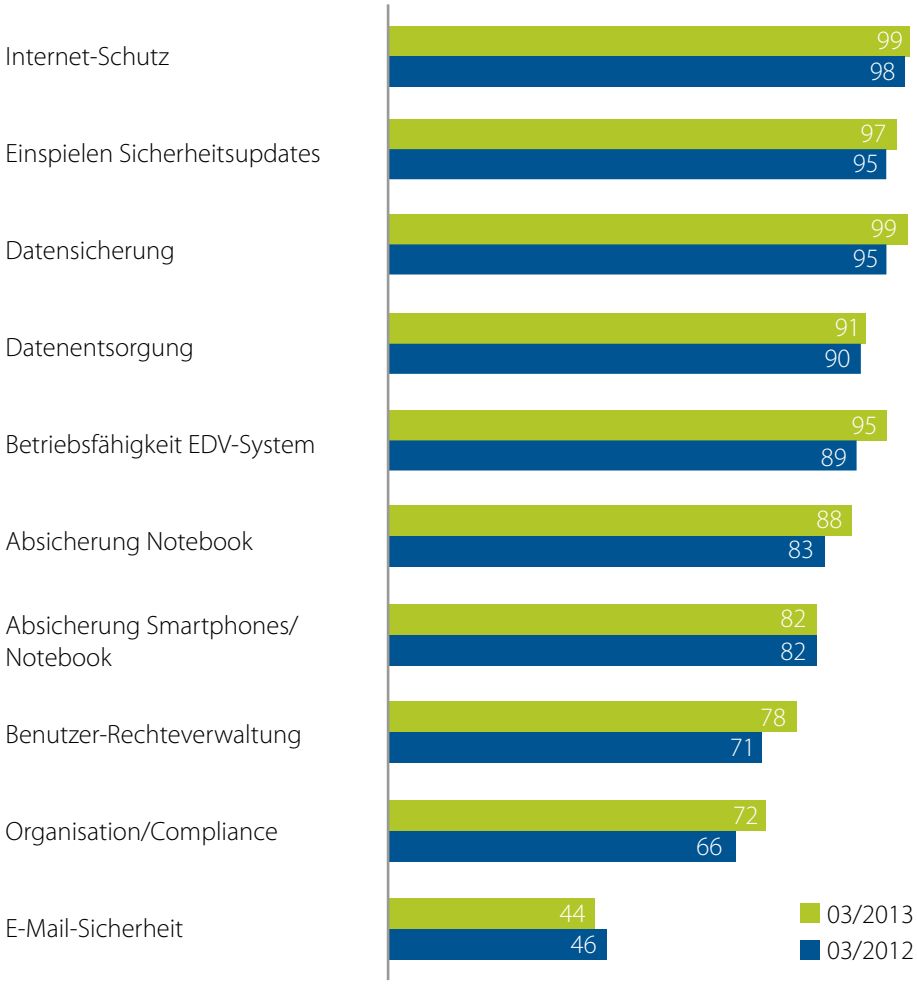


Grafik 3: Rolle der Cloud sowie Bekanntheitsgrad der Sicherheitsanforderungen und rechtlichen Rahmenbedingungen

4. Positive und negative Entwicklungen

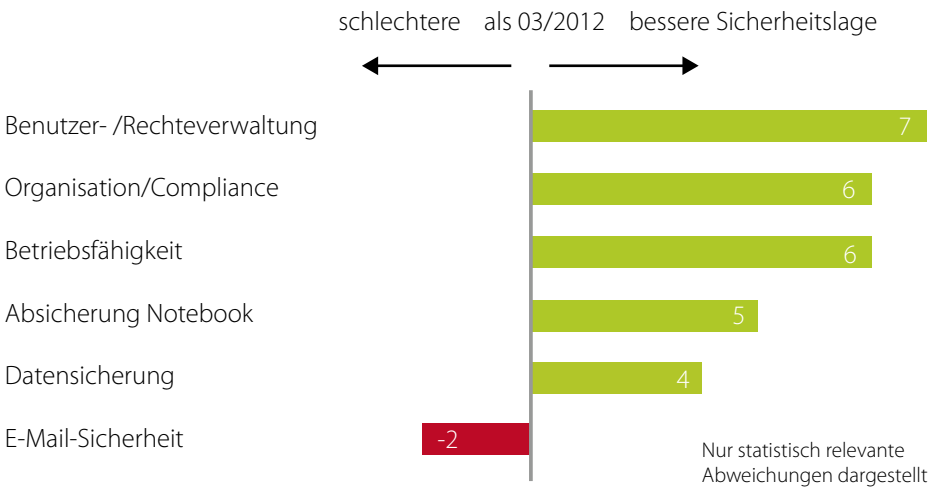
Das Sicherheitsbewusstsein der Unternehmen hat sich in den letzten 12 Monaten teilweise deutlich verbessert, insbesondere hinsichtlich Benutzer- und Rechteverwaltung, Compliance, Sicherung der EDV-Betriebsfähigkeit, Absicherung von Notebooks und Datensicherung.

Internet-Schutz (99 %), Datensicherung (99 %) und Sicherheitsupdates (97 %) sind flächendeckend verbreitet (Grafik 4).



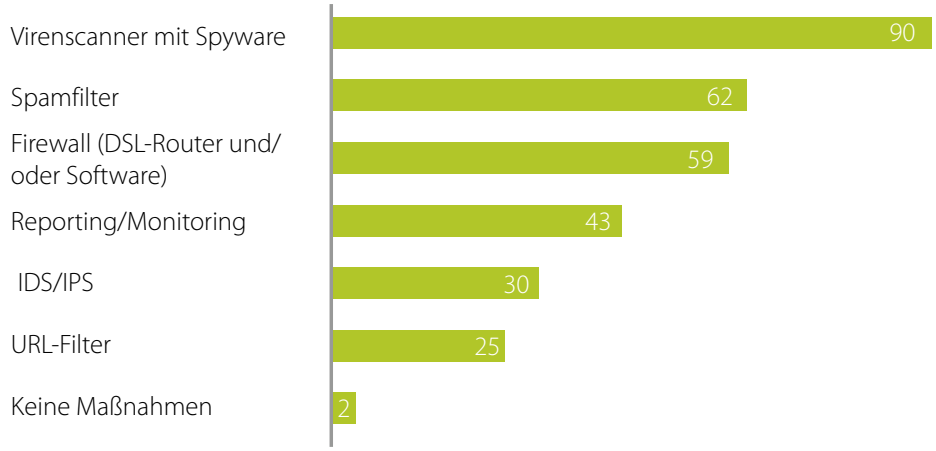
Grafik 4: Vorhandene Schutzmaßnahmen in den befragten Unternehmen

Problematisch bleibt nach wie vor die E-Mail-Sicherheit. Hier ist im Beobachtungszeitraum eine Tendenz hin zu einem weiteren Rückgang der Schutzmaßnahmen feststellbar (Grafik 5) - obwohl hier die geschäftliche Nutzung nochmals gestiegen ist (vgl. Grafik 2 im vorherigen Kapitel).



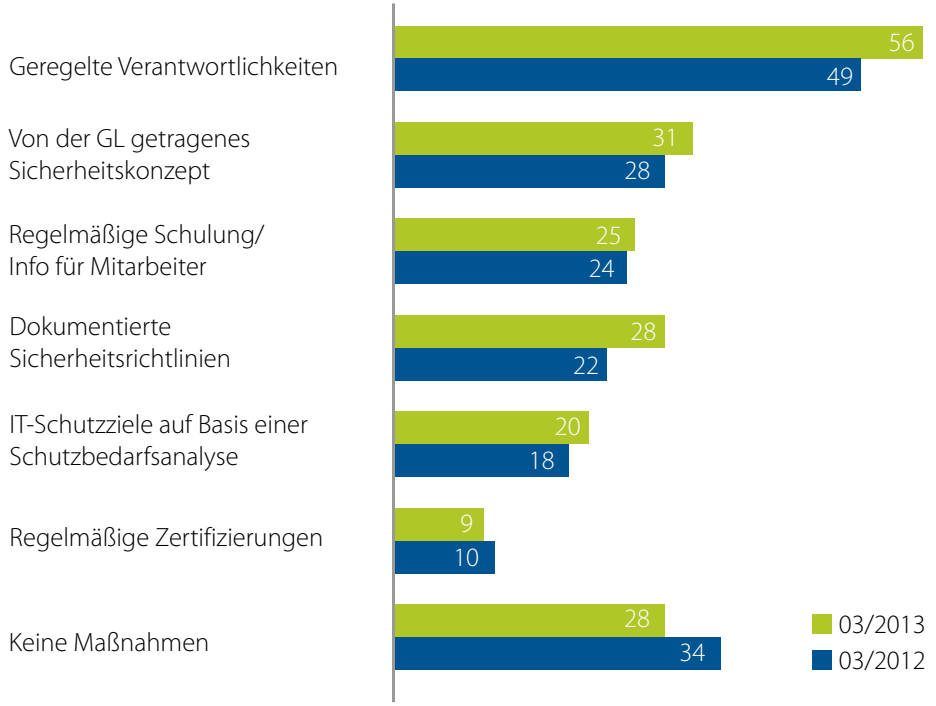
Grafik 5: Schutzmaßnahmen - Abweichungsanalyse

Vermutlich ist das Problembewusstsein bei den Unternehmen nicht sehr ausgeprägt, weil das Versenden von E-Mails so alltäglich ist, dass Gedanken an die Sicherheit nicht aufkommen und deren Schutz als zu aufwändig angesehen wird. Vielleicht fehlen praktische Lösungen für KMU. Oder es herrscht schlicht die irrige Meinung vor, der Schutz des Internet-Zugangs beinhalte die E-Mail-Sicherheit, denn der Zugang zum Internet ist bei fast allen Unternehmen abgesichert, teilweise sogar mehrfach (Grafik 6).



*Grafik 6: Sicherung des Internetzugangs bei Unternehmen, die ihre Mails **nicht** schützen*

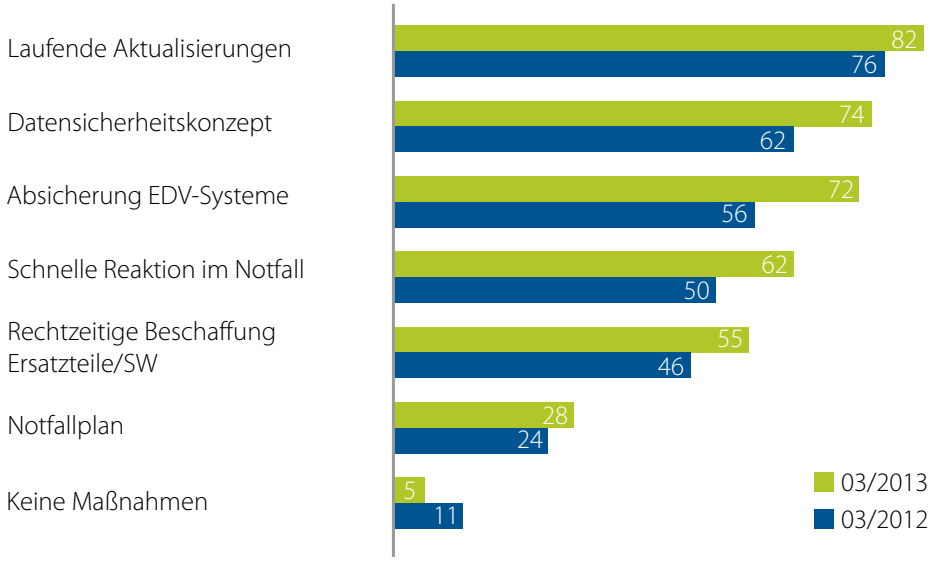
Die allgemeine Erhöhung des Sicherheitsbewusstseins im Bereich Compliance ist vor allem auf Zunahmen in den Bereichen geregelte Verantwortlichkeiten, ein von der Geschäftsleitung getragenes Sicherheitskonzept und dokumentierte Sicherheitsrichtlinien zurückzuführen (Grafik 7)



Grafik 7: Organisatorische Maßnahmen zu Datenschutz und IT-Sicherheit

Schlussfolgerungen

Insgesamt zeigt sich, dass das Bewusstsein für IT-Sicherheit steigt und die unterschiedlichen Sensibilisierungsmaßnahmen verschiedener Akteure und von DsiN bei den Unternehmen offenbar Wirkung zeigen. In diese Richtung deuten auch die erfreulichen Zuwächse bei den verschiedenen Maßnahmen zur Sicherstellung der Betriebsfähigkeit der EDV (Grafik 8).



Grafik 8: Maßnahmen zur Erhaltung der Betriebsfähigkeit der EDV

Die E-Mail-Sicherheit als eigenständiges Handlungsfeld für Unternehmen sollte stärker ins Bewusstsein der Verantwortlichen in Unternehmen gerückt werden. Etwa durch die Kommunikation von Beispielen aus der Praxis, wie entsprechende Maßnahmen aussehen können - nicht zuletzt, um zu zeigen, dass die E-Mail-Sicherheit mit geringen finanziellen Mitteln und geringem Personaleinsatz sichergestellt werden kann.

Verzicht auf Detailauswertungen

Tiefergehende Subgruppenanalysen führen aufgrund der statistisch geringen Veränderungen zu keinen neuen Erkenntnissen. Die weiteren Werte für den untersuchten Zeitraum 2012/2013 entsprechen den Erkenntnissen der IT-Sicherheitsstudie von 2011 und dem Update der Studie aus dem Jahr 2012. Beide Dokumente sind auf der DsiN-Website abrufbar unter der Adresse https://www.sicher-im-netz.de/unternehmen/sicherheitslage_mittelstand.aspx.

5. Handlungsempfehlungen

IT-Sicherheit ist eine fortwährende Aufgabe, an der laufend gearbeitet werden muss. Dafür sind organisatorische Vorkehrungen nötig: Mitarbeiter müssen geschult und sensibilisiert, Sicherheitsvorkehrungen auf ihre Einhaltung kontrolliert werden. Da Unternehmen nicht alle Probleme auf einmal angehen können, empfiehlt sich hierbei ein vierstufiges Verfahren.

In der ersten Phase geht es darum, das Risikoprofil einzuschätzen: „Welche Risiken gibt es und welche Risiken bestehen für mein Unternehmen?". Die zweite Phase umfasst die Identifikation der Risikobereiche („Wo sind die Risiken?"). In der dritten Phase werden entsprechende Kontrollen und IT-Sicherheitsmaßnahmen entwickelt („Welche Maßnahmen brauchen wir?"), die in der vierten Phase umzusetzen und in den Regelbetrieb zu integrieren sind.

Die Ergebnisse der aktuellen Studie legen nahe, dass es insbesondere auf drei Gebieten aktuellen Handlungsbedarf für KMU gibt: (1) E-Mail-Sicherheit, (2) mobile Endgeräte und (3) Cloud Computing.

- Internet-Schutz erfüllt keine E-Mail-Sicherheit
  Dringend zu empfehlen ist die Verwendung einer E-Mail-Verschlüsselung zusätzlich zur Internet-Security. Verschlüsselung und digitale Signatur werden bei den gängigen E-Mail-Programmen standardmäßig angeboten. Auf dem Markt gibt es verschiedene, zentral verwaltete, anwendungsfreundliche Ver- und Entschlüsselungsmethoden. Alle diese Lösungen lassen sich einfach und unkompliziert in vorhandene Geschäftsprozesse einbinden.

- Sichere Nutzung mobiler Endgeräte
  Dringend erforderlich ist die Erstellung eines Sicherheitskonzepts für die Anbindung mobiler Endgeräte. Der sichere Zugriff auf die Unternehmensdaten und der verantwortungsvolle Umgang mit den Geräten sind unabdingbare Voraussetzungen für deren Einsatz. So sollten besipielsweise die Endgeräte unter der Kontrolle des Unternehmens liegen, aber oft wird die Synchronisation mit privaten Geräten explizit gewünscht. Eine Risiko-Nutzen-Analyse für die Synchronisation von mobilen Geräten sollte durchgeführt werden und das spezifische Sicherheitskonzept auf der Basis der individuellen Randbedingungen sich daran orientieren.

- Cloud Computing sicher und rechtskonform nutzen
  Cloud Computing wird für Unternehmen zunehmend wichtiger. Von den Unternehmen, die die Cloud nutzen oder dies planen, ist jeweils einer Mehrheit nur teilweise oder gar nicht bewusst, wie die Cloud rechtskonform und sicher genutzt werden kann. Informationsangebote wie der DsiN-Cloud-Scout unter www.dsin-cloud-scout.de können hier eine wichtige erste Orientierung bieten und den Weg zur einer sicheren Nutzung der Cloud weisen.

Bei der Planung konkreter Maßnahmen bieten die praxisorientierten Hinweise im DsiN-Blog unter www.dsin-blog.de sowie die Leitfäden auf www.sicher-im-netz.de praktische Tipps und Hilfen.

6. Über Deutschland sicher im Netz

Deutschland sicher im Netz e.V. (DsiN) hat das Ziel, bei Verbrauchern und in Unternehmen das Bewusstsein für einen sicheren Umgang mit Internet und IT zu fördern, sowie einen praktischen Beitrag für mehr IT-Sicherheit zu leisten.

Produktneutral und herstellerübergreifend versteht sich DsiN als Partner für die Politik, gesellschaftliche Gruppen und die Wissenschaft im Bereich Sicherheit in der Informationstechnik. So werden Synergien genutzt und Überschneidungen vermieden.

Als Ergebnis des ersten IT-Gipfels der Bundesregierung im Dezember 2006 wurde aus der seit 2005 bestehenden Initiative der Verein Deutschland sicher im Netz e.V. gegründet. Mitglieder von DsiN sind Unternehmen, Branchenverbände und Vereine.

Die Schirmherrschaft des Bundesministeriums des Innern (BMI) hat die Rolle von DsiN weiter bestärkt. In diesem Rahmen wird der Verein auch bei der Umsetzung von Initiativen der Bundesregierung im Bereich Sicherheit in der Informationstechnik unterstützend tätig.

IT-Sicherheitslage im Mittelstand 2013
Eine Studie von Deutschland sicher im Netz

Autoren:
Stefan Brandl, DATEV eG
Sven Scharioth, DsiN

Herausgeber:
Deutschland sicher im Netz e.V.
Albrechtstraße 10a
10117 Berlin

www.sicher-im-netz.de
info@sicher-im-netz.de