IT-Sicherheitslage im Mittelstand 2011

Eine Studie von Deutschland sicher im Netz

Schirmherrschaft

Bundesministerium des Innern

Ein Handlungsversprechen von

DsiN.de

gemeinsam mit

BITKOM DATEV SAP SOPHOS und utimaco

INHALTSVERZEICHNIS

1. DAS WICHTIGSTE IN KÜRZE

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

Die Broschüre beschreibt die Ergebnisse des „DsiN-Sicherheitschecks", welcher von den DsiN-Mitgliedern BITKOM, DATEV, SAP und Sophos als Handlungsversprechen konzipiert und durchgeführt wurde. Ziel des „DsiN-Sicherheitschecks" ist es, den aktuellen Stand der Informationssicherheit in kleinen und mittleren Unternehmen (KMUs) in Deutschland zu ermitteln und daraufhin Handlungsempfehlungen auszusprechen – folglich Anstöße zu geben, wo Unternehmen sinnvoller Weise in Sicherheit investieren sollten.

An der online durchgeführten Studie nahmen fast 1.400 Unternehmen teil, wobei alle Größen – von Ein-Personen-Unternehmen bis Organisationen mit mehr als 500 Mitarbeitern – vertreten waren.

Die Ergebnisse sind grundsätzlich positiv. Sie zeigen eine deutliche Verbesserung der IT-Sicherheit in deutschen Unternehmen im Vergleich zur letzten Studie von 2008. Insbesondere die Verantwortung für IT-Sicherheit im Unternehmen ist inzwischen bei wesentlich mehr Unternehmen klar zugeordnet. Zudem sind Firewall, Anti-Virus- und Anti-Spam-Lösungen inzwischen Standard.

Dennoch gibt es keinen Grund zur Entwarnung. Die Studie zeigt auch, dass Unternehmen im Bereich der Compliance nicht besonders gut aufgestellt sind und insbesondere bei E-Mails und mobilen Geräten, die laut dieser Studie oft viele unternehmenskritische Daten enthalten, im Bezug auf die Sicherheit nachlässig sind.

Wirtschaft und Politik sollten diese Themenbereiche aufgreifen und mit nachhaltigen öffentlichkeitswirksamen Maßnahmen für mehr Sensibilität und Aufmerksamkeit sorgen. Insgesamt profitieren alle Wirtschaftsteilnehmer wie auch die Gesellschaft als Ganzes, wenn durch funktionierende IT-Sicherheit die Wirtschafts- und Innovationskraft gestärkt und damit auch Arbeitsplätze und Zukunftsfähigkeit geschützt werden.

Deutschland sicher im Netz empfiehlt den Unternehmen ganz konkret:

Stärken Sie Ihren Umgang mit Compliance-Vorgaben.

Benennen Sie einen Compliance-Verantwortlichen, erstellen Sie eine Compliance-Richtlinie, sensibilisieren Sie Mitarbeiter für das Thema, etablieren Sie einen Berechtigungs-Vergabe-Prozess und führen Sie eine Schutzbedarfsanalyse durch.

Verwenden Sie sichere E-Mail.

Verschlüsseln und signieren Sie E-Mails mit sensiblem Inhalt, oder schützen Sie zumindest die Anhänge. Eine gute Alternative ist der Einsatz von so genannten Datentresoren zum Austausch mit Kunden und Partnern.

Schützen Sie Ihre mobilen Daten.

Verwenden Sie eine Festplattenverschlüsselung für Notebooks, setzen Sie eine unternehmensweite Synchronisationslösung ein (statt individuelle Angebote), erstellen Sie ein **Sicherheitskonzept**, schützen Sie besonders kritische Dokumente direkt am Dokument, z.B. mit Rights Management Lösungen und ersetzen Sie passwort-basierte Anmeldeverfahren durch stärkere Authentifizierungsmechanismen.

Gewährleisten Sie die Funktionsfähigkeit Ihrer IT-Infrastruktur.

Erstellen Sie Notfallpläne und testen Sie regelmäßig das Einspielen von Backups.

2. ÜBERBLICK ÜBER DIE WICHTIGSTEN ERGEBNISSE

Die Auswertung der Befragungsergebnisse zeigt, dass KMUs beim Thema Compliance noch Nachholbedarf haben. Von den 1.342 kleinen und mittelständischen Unternehmen, die an der anonymen Onlineumfrage teilgenommen haben, besitzen nur 24% eine Compliance-Strategie, in der das Unternehmen Verhaltensmaßregeln und die Berücksichtigung von Gesetzen sowie Richtlinien im IT-Bereich definiert und dokumentiert.

Obwohl vielen Unternehmen nach eigenen Angaben eine Strategie fehlt, haben bereits 69% mit einzelnen Compliance-Maßnahmen begonnen. Jedoch lediglich 21% der Unternehmen leiten die Sicherheitsziele für ihre IT-Infrastruktur von der Analyse ihres eigenen Schutzbedarfs ab.

Compliance ist auch eine Frage der Einhaltung durch die Angestellten. Obwohl praktisch alle Mitarbeiter in ihrer täglichen Arbeit mit Compliance in Berührung kommen, bieten nur 26% der Unternehmen regelmäßig Informationen und Schulungen zu diesen Fragen an.

Während das Sicherheitsdenken zur Absicherung des Internetzugangs bei den Befragten gut ausgeprägt ist, zeigen sich im Bereich E-Mail-Schutz eklatante Versäumnisse: In 50% der Unternehmen werden E-Mails während der Übertragung durch keinerlei Maßnahme vor unberechtigter Einsichtnahme, Missbrauch oder Manipulation geschützt.

Generell kann festgestellt werden, dass das Problembewusstsein bezüglich Datensicherheit mit der Unternehmensgröße zunimmt und entsprechende Maßnahmen häufiger umgesetzt werden.

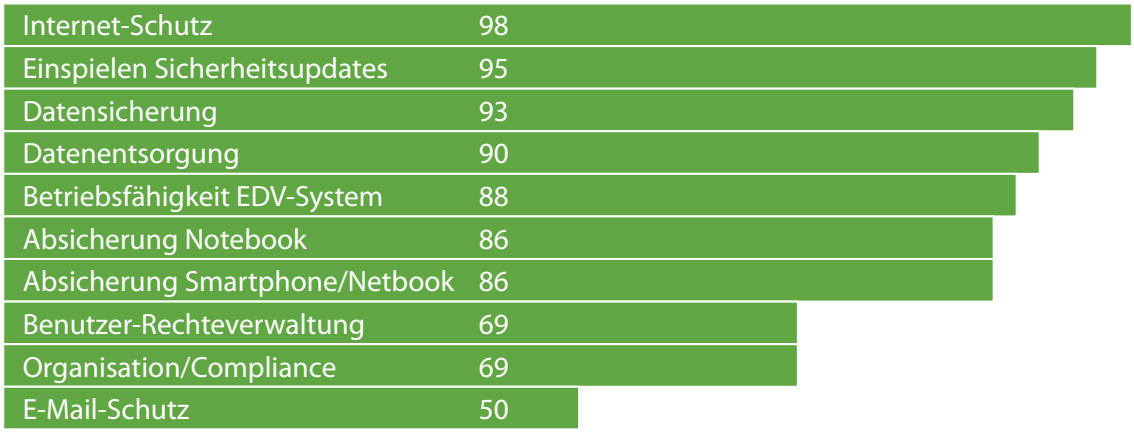
Eine Besonderheit stellt die Unternehmensgrößenklasse von 201-500 Mitarbeitern dar: Im Vergleich zu den ganz großen Unternehmen mit mehr als 500 Mitarbeitern wird in dieser Größenklasse deutlich mehr online gearbeitet als mit mobilen Datenträgern. In dieser Größenklasse bestehen hohe technische Schutzmaßnahmen, organisatorisch ist aber durchaus noch Verbesserungspotenzial vorhanden. Umgekehrt sieht es bei den meisten Kleinunternehmen (< 10 Mitarbeiter) leider insgesamt eher schlecht aus, dort ist erheblicher Nachholbedarf.

Zusammenfassend kann festgestellt werden, dass es in den Unternehmen mittlerweile ein ausgeprägtes Sicherheitsbewusstsein gibt und auch versucht wird, die erforderlichen Schutzmaßnahmen zu ergreifen. Technische Lösungen wie z.B. Firewalls und Spamfilter gehören mittlerweile zur Standardausstattung.

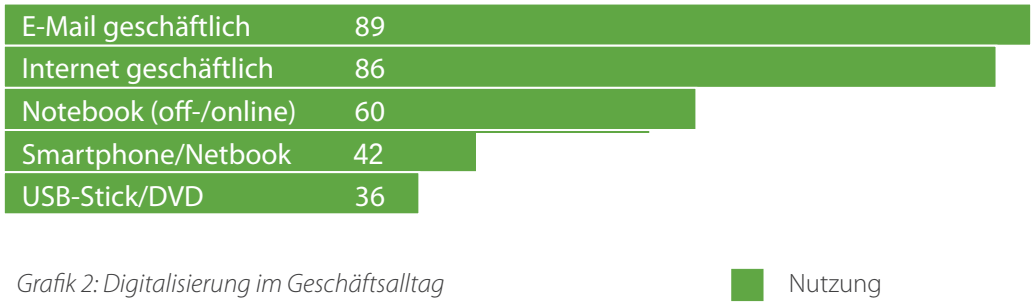
Bei der Umsetzung von IT-Sicherheit in der Unternehmensorganisation besteht noch großes Entwicklungspotenzial, z.B. in den Bereichen Benutzer- und Rechteverwaltung sowie Organisation und Compliance. Dringender Handlungsbedarf ist im Bereich E-Mail-Schutz zu verzeichnen (Grafik 1).

Rund 9 von 10 Unternehmen nutzen E-Mails im Geschäftsalltag, nahezu ebenso viele arbeiten auch mit dem Internet. Notebooks im Off- und Online Modus werden von 60% der Unternehmen verwendet. Externe mobile Endgeräte wie Netbooks und Smartphones gehören in 42% der Unternehmen zur Ausstattung. Unterrepräsentiert ist die Nutzung von USB-Sticks und DVDs, nur gut ein Drittel der Unternehmen arbeitet damit (Grafik 2).

Erwartungskonform nimmt der Digitalisierungsgrad mit der Unternehmensgröße zu.



Grafik 1: Überblick IT-Sicherheitslage



Grafik 2: Digitalisierung im Geschäftsalltag

3. HANDLUNGSEMPFEHLUNGEN

Die Ergebnisse des DsiN-Sicherheitschecks legen eine Reihe von Handlungsempfehlungen nahe. Deutschland sicher im Netz e.V. empfiehlt die folgenden Maßnahmen, um die Sicherheit bei KMUs in Deutschland weiter zu verbessern:

3.1 STÄRKUNG DER COMPLIANCE-AKTIVITÄTEN

Compliance-Aktivitäten sollten mit Bedacht durchgeführt werden. Überzogene Compliance-Maßnahmen können zu Konflikten mit Datenschutzregelungen führen. Dennoch ist für eine gute Sicherheitskultur ein gewisses Maß an Compliance absolut erforderlich. Compliance und Datenschutz widersprechen sich nicht. Richtig gemacht, kann man beides sogar wechselseitig gewinnbringend für das Unternehmen einsetzen.

Die folgenden Maßnahmen sollten ergriffen werden, um die Compliance in Ihrem Unternehmen zu stärken:

Benennen Sie einen Compliance-Verantwortlichen.

Compliance ist vielschichtig und es bestehen große Abhängigkeiten zu anderen Themen, wie Mitarbeitermotivation, Unternehmenskultur und Risikomanagement. Durch die eindeutige Zuordnung der Verantwortung kann überhaupt erst die gesetzeskonforme Verwendung von Informationstechnologie nachhaltig umgesetzt werden.

Erstellen Sie eine Compliance-Policy.

Ergänzend zu einer Richtlinie für IT- Sicherheit sollte es in Ihrem Unternehmen auch Vorgaben für gesetzeskonforme Handlungen von Unternehmensmitarbeitern geben. Lösen Sie Konflikte mit Datenschutz und anderen Vorgaben schon jetzt auf, damit Mitarbeiter keine widersprüchlichen Anweisungen bekommen. Bei der Auswahl von Datenschutz-konformen Compliance-Maßnahmen können Ihnen Experten helfen.

Sensibilisieren Sie Mitarbeiter zum Thema Compliance.

IT- und Informationssicherheit ist kein Selbstzweck, und das Verständnis der Mitarbeiter, dass hinter den Handlungsanweisungen zum sicheren Umgang mit IT oft auch gesetzliche Vorgaben stecken, ist für ein zielgerichtetes Handeln im Sinne des Unternehmens sehr hilfreich.

Etablieren Sie einen Berechtigungsvergabe-Prozess.

Zu den wichtigsten Anforderungen an IT-Compliance gehört es, dass Mitarbeiter nachvollziehbar nur darauf Zugriff haben, was Sie auch für ihre tägliche Arbeit benötigen. Etablieren Sie einen Prozess zur Vergabe und zur regelmäßigen Kontrolle von Berechtigungen – idealer Weise auch mit Untersuchung des damit verbundenen Risikopotenzials. Schon ein Beantragungsprozess per E-Mail, verbunden mit einer guten Protokollierung, ist ein erster, wichtiger Schritt. Es gibt aber auch schon viele gute Werkzeuge zur Automatisierung.

Ermitteln Sie den eigenen Schutzbedarf.

Nicht jede Maßnahme ist für jedes Unternehmen geeignet. Wie der DsiN-Sicherheitscheck gezeigt hat, werden viele IT-Sicherheitsmaßnahmen ungeachtet der Risikosituation eingesetzt. Es besteht damit die Gefahr, über das Ziel hinauszuschießen und zu viel in Maßnahmen zu investieren, die für das eigene Unternehmen gar nicht erforderlich sind. Wenn Sie daher zunächst den eigenen Schutzbedarf ermitteln und dann die Maßnahmen darauf abstimmen, so ist in der Regel eine wirtschaftliche Lösung möglich.

3.2 SICHERER UMGANG MIT VERTRAULICHEN E-MAILS

Offensichtlich hat sich immer noch nicht die Erkenntnis durchgesetzt, dass E-Mails mit Postkarten vergleichbar sind, und dass es für Betrüger und Spione sehr einfach ist, E-Mails im Internet mitzulesen. Gleichzeitig aber nimmt der Druck, einfache und schnelle Kommunikation mit Kunden, Lieferanten und Partnern nutzen zu können, immer mehr zu. Daher sind Schutzmechanismen für vertrauliche E-Mails erforderlich, die dennoch einfach und handhabbar sind.

Die folgenden Maßnahmen sollten ergriffen werden, um den sicheren Umgang mit vertraulichen E-Mails zu ermöglichen:

Verwenden Sie E-Mail-Verschlüsselung.

Alle gängigen E-Mail-Programme unterstützen schon heute standardmäßig die Verschlüsselung und digitale Signatur von E-Mails. Um dies nutzen zu können, ist nur ein persönliches E-Mail-Zertifikat für beide Kommunikationspartner erforderlich. Professionelle Lösungen unterstützen auch Empfänger ohne Zertifikat, sowie die Archivierung von verschlüsselten E-Mails. Hierzu bietet der Markt neben den lokalen Möglichkeiten zur Verschlüsselung auch zentral gemanagte anwendungsfreundlichere Ver- und Entschlüsselungsmöglichkeiten als Alternative an.

Schützen Sie vertrauliche Anhänge von E-Mails.

Stellt der Einsatz von E-Mail-Verschlüsselung keine Alternative für Sie dar, so schützen Sie zumindest die Anhänge von E-Mails, und stellen Sie sicher, dass sich vertrauliche Informationen nur im Anhang befinden. Schützen Sie die Dateien mit Passwörtern (z.B. als PDF-Dokument, ZIP oder Office-Dokument), und wählen Sie dafür ausreichend lange und komplexe Passwörter.

Verwenden Sie sichere, gemeinsame Dateiablagen statt E-Mails.

Kommunizieren Sie häufig innerhalb einer unternehmensübergreifenden Projektgruppe, und sei es nur auf Zeit, so bietet es sich an, eine sichere, gemeinsame Dateiablage („Datentresor“) im Internet zu verwenden. Moderne Systeme dieser Art unterstützen starke Authentifizierung (z.B. MobileTAN), und lassen sich komfortabel in den Dateimanager integrieren.

3.3 SCHUTZ MOBILER DATEN

Durch die immer stärker zunehmende Verwendung von mobilen Endgeräten (Smartphones, Tablet PCs, Notebooks), aber auch die Synchronisation von E-Mail, Kalender und Dateien werden immer mehr möglicherweise vertrauliche Unternehmensinformationen über das Internet zwischen verschiedenen Endgeräten synchronisiert und zum Teil auch im Internet abgespeichert.

Die folgenden Maßnahmen sollten ergriffen werden, um das Risiko des unbemerkten Datenabflusses bei der Verwendung mobiler Endgeräte zu minimieren:

Setzen Sie Festplattenverschlüsselung bei Notebooks ein.

Notebooks stellen den optimalen Kompromiss zwischen Mobilität und maximaler Flexibilität dar. Dies gilt leider auch für Datendiebe, für die es sehr leicht ist, an die Daten einer Festplatte aus einem Notebook heranzukommen. Festplattenverschlüsselung ist inzwischen eine reife Technologie und sollte, zusammen mit einem Recovery-Dienst, unbedingt eingesetzt werden.

Verwenden Sie eine unternehmensweite Synchronisationslösung für mobile Endgeräte.

Die Synchronisation von Unternehmensinformationen auf Tablet PCs und Notebooks kann absolut sinnvoll und produktivitätssteigernd sein, nicht immer ist es das damit verbundene Risiko wert. Auf der anderen Seite ist es besser, einen einheitlichen, vom Unternehmen kontrollierten Synchronisationsdienst einzusetzen, als dass Mitarbeiter eigene, individuelle Cloud-Services dafür verwenden. Cloud-Services für E-Mail- und Kalender-Unternehmenslösungen z.B. unterstützen die sichere Anbindung von mobilen Endgeräten heute schon.

Erstellen Sie ein Sicherheitskonzept für die Anbindung mobiler Endgeräte.

Die mobile Synchronisation ist – richtig betrieben – eine sehr sichere Sache. Allerdings ergeben sich neue Schwachstellen, die Sie im Blick haben sollten. So sollten z.B. die Endgeräte unter der Kontrolle des Unternehmens liegen, aber oft wird die Synchronisation mit privaten Geräten gerade gewünscht. Führen Sie daher eine Risiko-Nutzen-Analyse für die Synchronisation von mobilen Geräten durch, und entwickeln Sie Ihr spezifisches Sicherheitskonzept auf der Basis Ihrer Randbedingungen.

Schützen Sie besonders kritische Informationen direkt am Dokument.

Durch die Synchronisation von Informationen und Verzeichnissen mit mobilen Endgeräten sind gerade kritische Dokumente besonders von unbemerkter Einsichtnahme bedroht. Daher sollten Sie diese Dokumente (wie E-Mail-Anhänge) besonders schützen, idealer Weise mit Information-Rights-Management-Lösungen, die eine sehr detaillierte und dennoch einfache Zugriffskontrolle auf Dokumentenebene ermöglichen. Ist Ihnen dies nicht möglich, schützen Sie diese Dokumente zumindest mit einem Passwort.

Ersetzen Sie sukzessive Passwörter durch stärkere Authentifizierungs-Mechanismen.

Passwörter werden durch die zunehmende Verwendung von mobilen Endgeräten immer unsicherer, da sie leicht abgehört werden können, und bei der Vielzahl der erforderlichen Passwörter entweder schwer zu merken oder oft gleich sind. Fangen Sie jetzt an, passwort-basierte Authentifizierungen bei kritischen Systemen zu ersetzen, etwa durch Einmalpasswort-Verfahren oder Smart-Cards.

Reglementieren Sie die Nutzung von Apps für Smartphones.

Apps können Schwachstellen aufweisen, die den unbefugten Zugriff auf die Daten des Smartphones oder des Firmennetzes ermöglichen.

3.4 GEWÄHRLEISTUNG DER FUNKTIONSFÄHIGKEIT DER IT-INFRASTRUKTUR

Durch die ständige Weiterentwicklung der Informationstechnologie nimmt die Bedeutung von verlässlichen Komponenten für die Informationsinfrastruktur immer mehr ab, dafür aber deren Integration in die Sicherheitsprozesse immer mehr zu. Im Fokus steht nicht mehr die unterbrechungsfreie Stromversorgung und die Existenz eines Backups, um Daten nicht zu verlieren, sondern der tatsächliche Test der Ausfallszenarien, um einen schnellen Wiederanlauf zu gewährleisten.

Die folgenden Maßnahmen sollten ergriffen werden, um das Risiko eines Stillstands der Geschäftstätigkeit durch einen IT-Ausfall zu minimieren:

- **Entwickeln Sie einen Notfallplan.**
  Es ist eine Sache, Maßnahmen zu ergreifen, um im Falle eines IT-Ausfalls nicht alle Daten zu verlieren. Noch besser aber ist es, wenn Sie die Anlaufzeit deutlich verkürzen können. Überlegen Sie bevor etwas passiert, wie Sie in der Situation handeln würden.

- **Sorgen Sie für eine vollständige Sicherung Ihrer Daten.**
  Auch Daten auf mobilen Geräten (z. B. Notebooks, Smartphones, Netbooks, etc.) sind mit zu berücksichtigen. Dokumentieren Sie im Hinblick auf Compliance-Anforderungen die Speicherorte.

- **Testen Sie das Wiedereinspielen von Backups.**
  Ein Backup nützt Ihnen nur wenig, wenn Sie nicht mit den gesicherten Daten möglichst schnell wieder den Geschäftsbetrieb aufnehmen können. Daher sollten Sie sich regelmäßig die Zeit nehmen und ein Backup auf einem Reserve-Rechner einspielen – auch und gerade mit betrieblichen Anwendungssystemen.

4. DIE ERGEBNISSE IM DETAIL

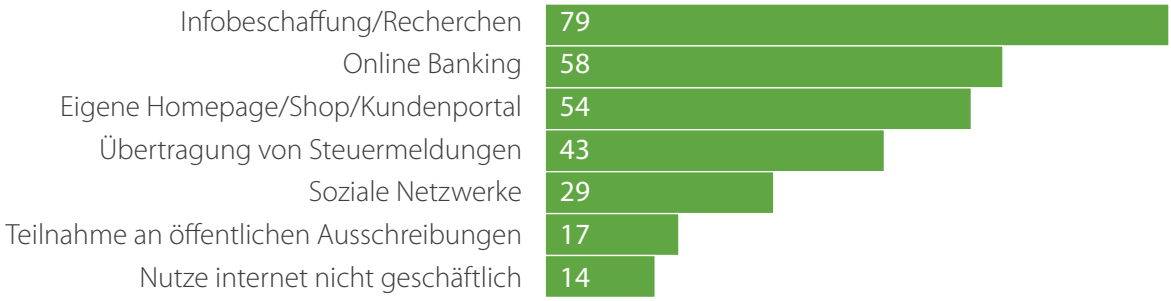
4.1 STRUKTURFRAGEN UND RISIKOEINSCHÄTZUNG DIGITALER ARBEITSABLÄUFE

Mehr als die Hälfte der teilnehmenden Unternehmen gehört zum Segment der Kleinunternehmen mit weniger als 10 Mitarbeitern, die restlichen Teilnehmer verteilen sich zu nahezu gleichen Anteilen auf die weiteren Größenklassen.

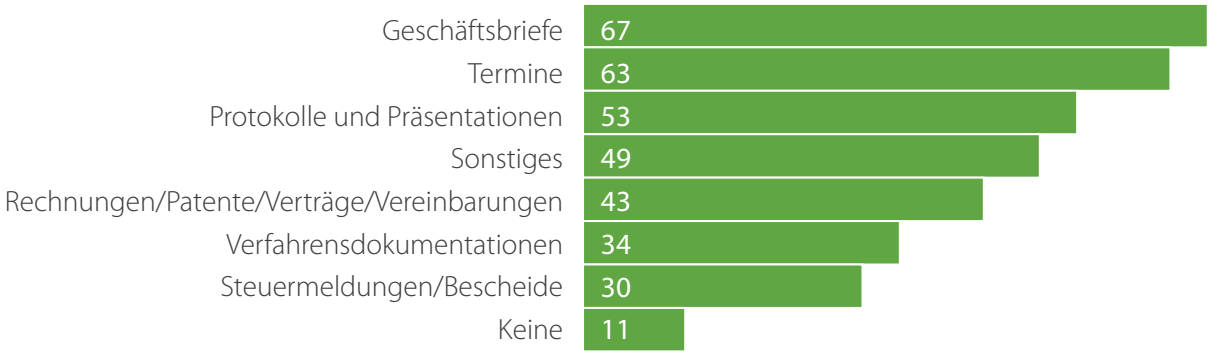
Geschäftlich wird das Internet von mehr als zwei Dritteln der Befragten (79%) zur Informationsbeschaffung und Recherchen verwendet. Mehr als die Hälfte nutzt das Internet zum Zweck des Online Banking (58%). Mit 54% der Nennungen steht die eigene Homepage, ein Online-Shop oder ein Kundenportal an dritter Stelle. 43% übertragen ihre Steuermeldungen an das Finanzamt über das Internet (Grafik 3).

Betrachtet man die wichtigsten Informationen, die geschäftlich per E-Mail verschickt werden, so stehen Geschäftsbriefe mit 67% an der Spitze. Termine vereinbaren 63% über das Internet, 53% versenden Protokolle und Präsentationen an ihre Geschäftspartner (Grafik 4).

Der Datenzugriff und Datenaustausch außerhalb des Unternehmensnetzwerks erfolgt in 47% der Unternehmen direkt, 42% synchronisieren Kalender und Postfächer mit Smartphones und Netbooks. Mittels mobilem Datenträger greifen 36% auf ihre Daten zu, 35% nutzen ihre Daten synchronisiert auf einem Netbook außerhalb des Firmennetzwerks.



Grafik 3: Für welche geschäftlichen Tätigkeiten nutzen Sie das Internet?



Grafik 4: Welche vertraulichen/geschäftskritischen Informationen versenden Sie per E-Mail?

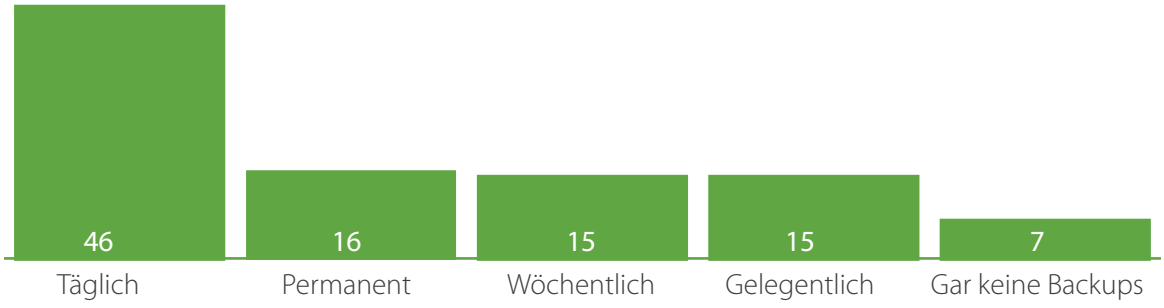
4.2 IT-INFRASTRUKTUR UND IT-MANAGEMENT

Um ihre EDV betriebsfähig zu halten, vertrauen 77% auf laufende Aktualisierungen von Betriebssystemen, Software-Versionen und sicherheitsrelevanten Patches. Ein eigenes Datensicherungskonzept haben 59% der Unternehmen entwickelt, 52% sichern ihre EDV-Systeme mit verschiedenen technischen Tools ab. Auf eine schnelle Reaktion im Notfall durch Wartungsverträge oder die eigene Kompetenz im Unternehmen verlassen sich 45% der Befragten, weitere 44% setzen auf die rechtzeitige Beschaffung von Ersatzteilen und der zugehörigen Software. Nur jedes vierte Unternehmen hat einen Notfallplan, sollten deren Computersysteme ausfallen.

Knapp die Hälfte der Unternehmen (46%) sichert täglich ihre wichtigsten Geschäftsdaten, insgesamt ebenfalls 46% der Befragten sichern die Daten permanent/wöchentlich oder gelegentlich. In 7% der Unternehmen findet überhaupt keine Datensicherung statt (Grafik 5).

Die Funktionsfähigkeit der Datensicherung im Unternehmen wird von 40% der Unternehmen regelmäßig geprüft, 46% geben an, Prüfungen teilweise vorzunehmen. In 14% der Unternehmen findet keine Überprüfung der Datensicherung statt.

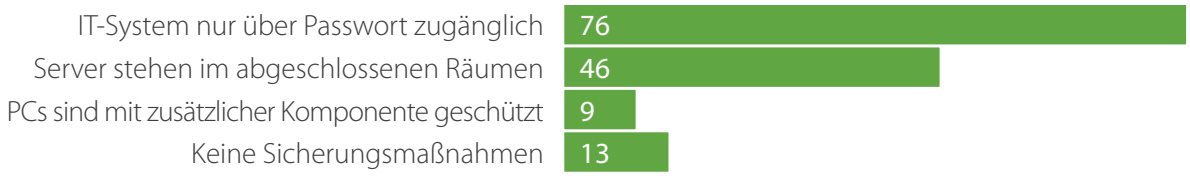
Von den 59%, die angeben, ein eigenes Datensicherungskonzept zu haben, sichern 80% der Unternehmen die Daten täglich oder permanent. Die Funktionsfähigkeit der Datensicherung erfolgt zu 45% regelmäßig, knapp die Hälfte (47%) prüft die Funktionsfähigkeit nur teilweise, 8% verzichten völlig darauf.



Grafik 5: Wie häufig werden Ihre wichtigsten Geschäftsdaten gesichert?

Eine Aktualisierung der IT-Systeme mit Sicherheitsupdates nehmen drei Viertel (74%) der Unternehmen sofort nach Herstellerfreigabe vor, ein Fünftel (21%) aktualisieren diese zwar, führen dies aber nicht zeitnah durch. Jedes zwanzigste Unternehmen (5%) aktualisiert die Sicherheitsupdates überhaupt nicht.

Die deutliche Mehrheit (76%) der Unternehmen sichert ihre IT-Systeme mit Passwörtern ab, knapp die Hälfte (46%) hat die Server in abgeschlossenen Räumen stehen, zu denen ausschließlich autorisierte Personen Zugang haben. Der Schutz der PCs mit zusätzlichen Komponenten ist von eher untergeordneter Bedeutung (9%). Keinerlei Sicherungsmaßnahmen zur Nutzung der IT-Systeme werden in 13% der Unternehmen getroffen (Grafik 6).

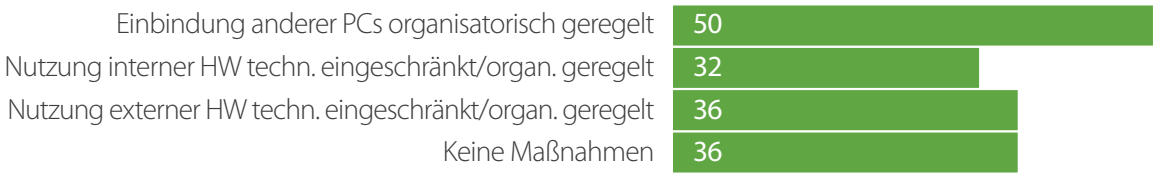


Grafik 6: Welche Sicherungsmaßnahmen zur Nutzung Ihrer IT-Systeme setzen Sie ein?

In 72% der Unternehmen haben die Mitarbeiter nur die Datenzugriffsberechtigungen, die sie für ihre Arbeit auch benötigen. Bei den restlichen 28% der Unternehmen können alle Mitarbeiter auf alle Daten zugreifen. Bei den 28% wiederum haben über ein Drittel keinerlei Sicherungsmaßnahmen zur Nutzung der IT-Systeme.

Um den unerlaubten Datentransfer mit Hilfe externer Hardwarekomponenten zu unterbinden, hat die Hälfte der Unternehmen die Einbindung anderer PCs ins Firmennetzwerk technisch und organisatorisch geregelt. 36% bzw. 34% haben die Nutzung externer bzw. interner Hardware technisch und organisatorisch geregelt. Ein Drittel der Befragten ergreift keine diesbezüglichen Maßnahmen (Grafik 7).

Durch Prüfung mit einem Virenscanner beim Einspielen von Daten stellen 84% den Virenschutz bei der Nutzung mobiler Datenträger sicher, 16% prüfen die Daten nicht, die sie z.B. von einem USB-Stick übernehmen. Mobile Datenträger werden von insgesamt 45% der Unternehmen gegen unberechtigte Verwendung geschützt, 26% schützen die Dateien mit einem Passwort, 19% verschlüsseln die Daten. Die restlichen 55% schützen ihre Daten nicht.



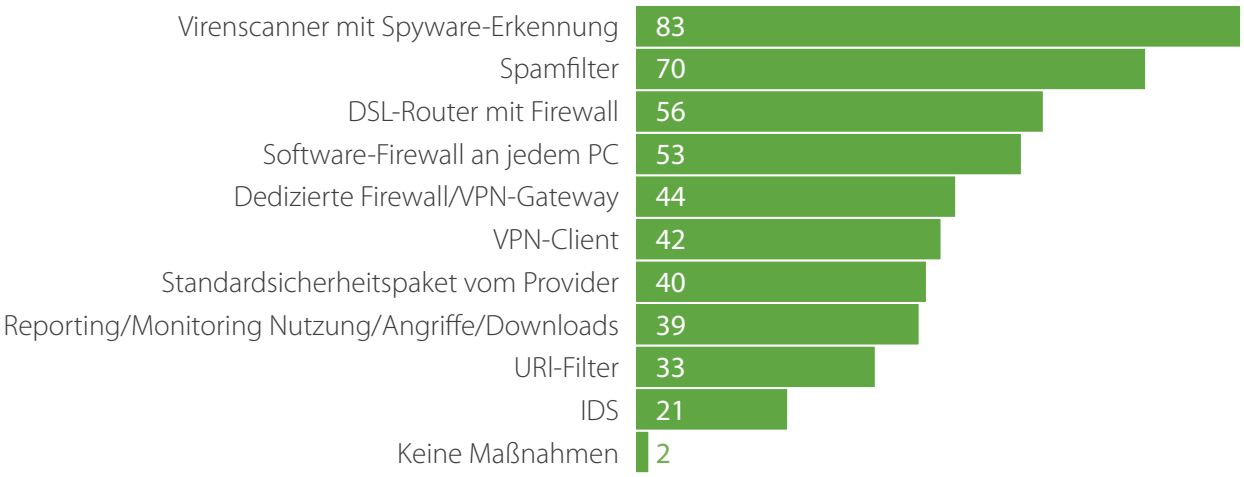
Grafik 7: Wie stellen Sie sicher, dass nicht unerlaubt Daten von Ihrem IT-System transferiert werden?

4.3 INTERNET- UND E-MAIL-NUTZUNG

Insgesamt 88% der Unternehmen haben sich mit den Risiken und rechtlichen Anforderungen bei der geschäftlichen Nutzung von Internet und E-Mails bereits intensiv oder teilweise auseinandergesetzt, 12% geben an, sich diesbezüglich noch keine weiteren Gedanken gemacht zu haben (Grafik 8).

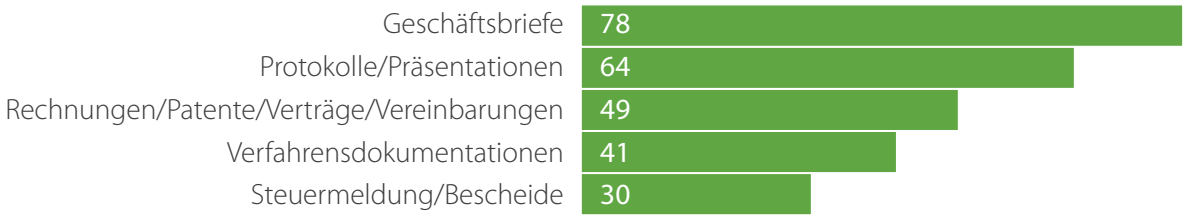
Grafik 8: Haben Sie sich mit den Risiken und rechtlichen Anforderungen bei der geschäftlichen Nutzung von Internet und E-Mails bereits auseinandergesetzt?

An der Spitze der Maßnahmen zur Absicherung des Internetzugangs steht mit 83% der Einsatz eines Virenscanners mit Spyware-Erkennung für die Endgeräte. Einen Spamfilter nutzen 70% der Unternehmen, 56% verlassen sich auf einen DSL-Router mit Firewall, weitere 53% haben an jedem PC eine Software-Firewall installiert (Grafik 9).



Grafik 9: Mit welchen Maßnahmen sichern Sie Ihren Internetzugang ab?

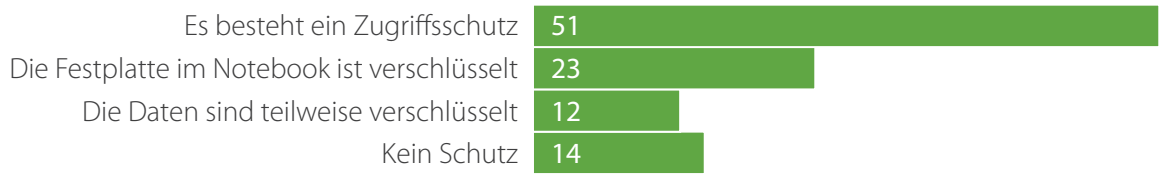
Hinsichtlich des E-Mail-Schutzes gegen unberechtigte Einsichtnahme, Missbrauch oder Manipulation besteht noch großer Handlungsbedarf, die Hälfte der befragten Unternehmen hat derzeit keinerlei Sicherungsvorkehrungen getroffen. Und das, obwohl sie per E-Mail auch schützenswerte Daten (z.B. Geschäftsbriefe 78%, Protokolle und Präsentationen 64%, Rechnungen, Patente, Verträge 49%) versendet. Zu etwa gleichen Teilen werden die Dokumente mit Passwörtern, elektronischen Signaturen und Verschlüsselungen der Anhänge geschützt (Grafik 10).



Grafik 10: Welche Informationen werden per E-Mail ungeschützt versendet?

4.4 MOBILE BUSINESS

Notebooks werden hauptsächlich (51%) mittels Zugriffschutz vor unberechtigter Nutzung oder Einsichtnahme geschützt, knapp ein Viertel (23%) verschlüsselt die Festplatte des Notebooks. Ungeschützt verwenden 14% ihre Notebooks (Grafik 11).

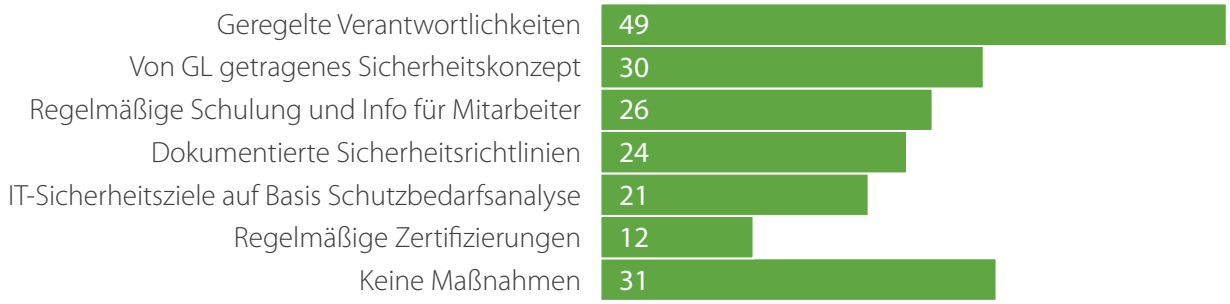


Grafik 11: Wie schützen Sie Ihr Notebook vor unberechtigter Nutzung bzw. Einsichtnahme durch Dritte?

51% der Unternehmen sind sich zwar der Gefahren bei der Nutzung von mobilen Endgeräten wie Smartphones und Netbooks inkl. WLAN bewusst, sind sich aber nicht sicher, ob ihre getroffenen Maßnahmen ausreichend sind. Ein Drittel (36%) ist der Ansicht, ihre Maßnahmen decken die Risiken ab, 14% sind sich der Gefahren nicht bewusst und haben auch deswegen noch keine geeigneten Maßnahmen in die Wege geleitet.

4.5 DATENSCHUTZ / IT-SICHERHEITSMANAGMENT

Geregelte Verantwortlichkeiten sollen in 49% der Unternehmen Datenschutz und IT-Sicherheit sicherstellen, knapp ein Drittel wendet ein von der Geschäftsleitung getragenes Sicherheitskonzept im Unternehmen an. Rund ein Viertel der Unternehmen setzt auf regelmäßige Schulungen und Informationen für ihre Mitarbeiter, fast ebenso viele dokumentieren die Sicherheitsrichtlinien im Unternehmen. Ein Fünftel der Befragten hat IT-Sicherheitsziele auf Basis der Schutzbedarfsanalyse formuliert, weitere 12% setzen auf regelmäßige Zertifizierungen. Mit knapp einem Drittel (31%) ist der Anteil der Unternehmen, die keinerlei organisatorische Maßnahmen im Unternehmen festgelegt haben, als relativ hoch zu bezeichnen (Grafik 12).



Grafik 12: Welche organisatorischen Maßnahmen zu Datenschutz und IT-Sicherheit sind bei Ihnen vorhanden?

Die Entsorgung vertraulicher Daten wird in jeweils rund einem Drittel der Unternehmen durch eine vom BSI empfohlene Software gelöscht bzw. physikalisch zerstört oder aber durch Löschung oder Formatierung der entsprechenden Datenträger sichergestellt. Über ein beauftragtes Unternehmen erledigen 24% die vertrauliche Entsorgung der Daten. 10% entsorgen ihre sensiblen Datenträger ohne weitere Maßnahmen.

5. DIE BEFRAGUNG

Der Verein Deutschland sicher im Netz e.V. (DsiN) hat zusammen mit BITKOM, DATEV, SAP und Sophos einen IT-Sicherheitscheck entwickelt, mit dem sich kleine und mittelständische Unternehmen (KMUs) über den Stand ihrer Informationssicherheit informieren können. Entsprechend der Ergebnisse erhalten die KMUs produktneutrale und herstellerübergreifende Handlungsempfehlungen, um die Einhaltung von Datenschutz- und Datensicherheitsregeln verbessern zu können.

Die Befragung wurde online mittels standardisiertem Fragebogen in anonymisierter Form durchgeführt. Der Erhebungszeitraum war vom 1. Oktober 2010 bis zum 31. März 2011. Es haben 1.342 Unternehmen an der Befragung teilgenommen. Die Auswertung erfolgte durch DATEV, unterstützt durch das Kompetenzzentrum für Sicherheit der Fachhochschule Brandenburg

HINTERGRUNDINFORMATIONEN

Deutschland sicher im Netz e.V.

Deutschland sicher im Netz e.V. hat das Ziel, bei Verbrauchern und in Unternehmen ein 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.

Die Partner des Handlungsversprechens

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., **BITKOM**, vertritt mehr als 1.350 Unternehmen, davon über 1.000 Direktmitglieder. Neben der Förderung von Innovationen, E-Government, Mittelstandspolitik und digitaler Konvergenz stehen Sicherheit und Vertrauen in IT und Internet als Kernthemen auf der Agenda des BITKOM. BITKOM verknüpft die Aktivitäten seiner Kompetenzbereiche wie z. B. IT-Sicherheit oder Mittelstand mit den Projekten des Vereins Deutschland sicher im Netz e.V.

Die **DATEV eG** ist das Softwarehaus und der IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten. Das Leistungsspektrum umfasst vor allem die Bereiche Rechnungswesen, Personalwirtschaft, betriebswirtschaftliche Beratung, Steuern, Enterprise Resource Planning (ERP), IT-Lösungen und Security sowie Organisation und Planung. DATEV unterstützt DsiN insbesondere durch Handlungsversprechen in den Bereichen Leitfäden, Kommunikation und Befragungen.

Als drittgrößter Softwarelieferant der Welt unterstützt **SAP** Firmen aller Größen und Industriezweige bei einer effizienteren Zusammenarbeit und einer besseren Nutzung von Informationen. Der Beitrag von SAP zu Deutschland sicher im Netz e.V. konzentriert sich auf die Unterstützung kleiner und mittelständischer Unternehmen bei der Absicherung ihrer Geschäftsanwendungen und die Stärkung des Vertrauens in das Internet. Aus diesem Grunde beteiligt sich SAP insbesondere an Projekten zum Thema IT -Sicherheit für den Mittelstand, zuletzt durch die Veröffentlichung des Pocketseminars „IT-Sicherheit für kleine und mittlere Unternehmen".

Durch die Übernahme des weltweit führenden Datensicherheitsspezialisten **Utimaco Safeware** erweiterte **Sophos** im Jahr 2009 sein Leistungsspektrum um Datensicherheitslösungen, mit denen sich mittelständische Firmen und Großunternehmen vor vorsätzlichem Datendiebstahl sowie unbeabsichtigtem Datenverlust schützen und die Einhaltung geltender Datenschutzbestimmungen sicherstellen können. Im Mittelpunkt der Sophos-Beteiligung stehen die Aufklärung und Unterstützung kleiner und mittelständischer Unternehmen bei der Absicherung ihrer elektronischen Werte - egal an welchem Aufbewahrungsort.

IT-Sicherheitslage im Mittelstand 2011

Eine Studie von Deutschland sicher im Netz

Autoren:
Prof. Dr. Sachar Paulus, Fachhochschule Brandenburg
Stefan Brandl, DATEV eG

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