KfW Research
Fokus Volkswirtschaft

»» Chancen der Digitalisierung nutzen: Datenschutz und IT-Sicherheit gehören dazu

Nr. 117, 8. Februar 2016

Autoren: Dr. Michael Schwartz, Telefon 069 7431-8695
Aurelia Muhle, research@kfw.de

Die Digitalisierung birgt Potenzial für die zukünftige Wettbewerbsfähigkeit des Mittelstands. Damit sich dieses Potenzial entfalten kann, müssen Schadensrisiken abgewendet werden. Den kleinen und mittleren Unternehmen (KMU) scheint das bewusst zu sein: Zwischen 2013 und 2015 haben fast alle Mittelständler zumindest grundlegende Vorkehrungen für mehr IT-Sicherheit und Datenschutz getroffen.

Das KfW-Mittelstandspanel zeigt außerdem: Die Maßnahmen sind geboten. Jedes dritte KMU war von 2013 bis 2015 von konkreten Sicherheitsvorfällen betroffen – kleine Mittelständler sogar leicht häufiger als größere KMU.

Es ist viel passiert. Jedes zweite Unternehmen sieht bei seinem Sicherheitsniveau allerdings noch Nachbesserungsbedarf. Vielen KMU fehlen jedoch die Zeit und das Personal. Zuweilen werden die Gefahren unterschätzt.

Die Abwendung von Schadensrisiken ist aufgrund des rasch voranschreitenden Digitalisierungsgrades als Daueraufgabe zu verstehen.

Die Chancen der Digitalisierung gilt es zu schützen

Moderne digitale Technologien und digitale Vernetzung nehmen rasant an Bedeutung zu (Industrie 4.0, Social Media, Online-Banking, Cloud Computing, etc.). In Zeiten stetiger Intensivierung digitaler Geschäftsabläufe gilt es für viele Unternehmen Schritt zu halten, um ihre künftige Wettbewerbsfähigkeit zu erhalten.

Die Digitalisierung bietet Chancen, parallel steigen die Herausforderungen für die Unternehmen, die eigenen Ressourcen zu schützen. Die Sicherheit der eigenen IT-Infrastruktur und der Schutz vorhandener Daten sind daher gebotener denn je.

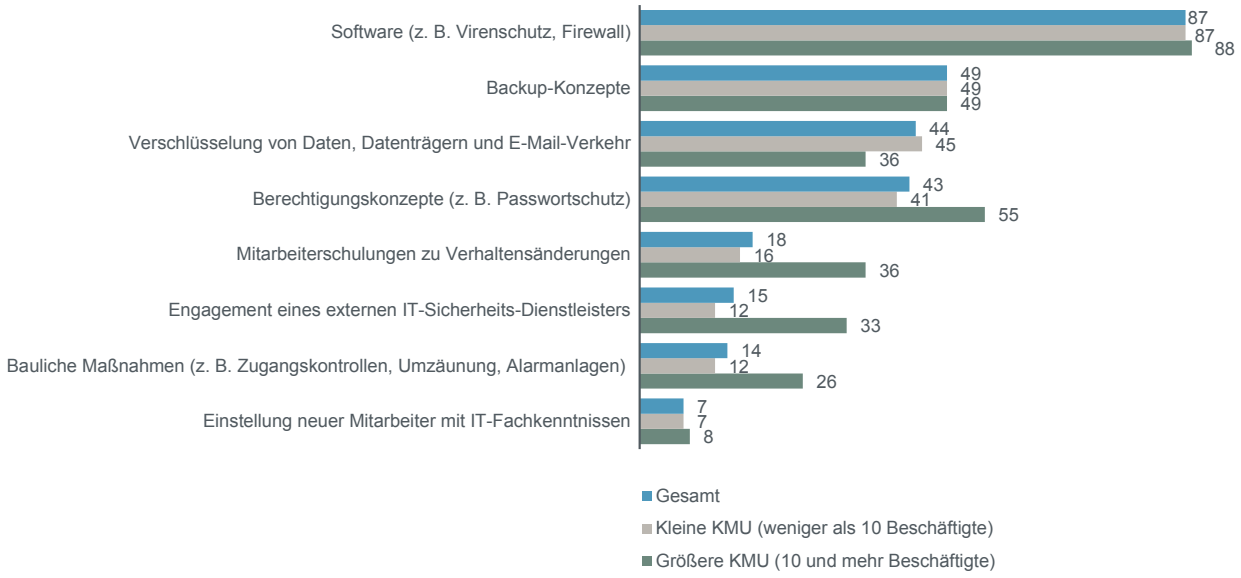
Die mittelständischen Unternehmen in Deutschland wissen das und reagieren: Eine Sondererhebung des KfW-Mittelstandspanels 2015 zeigt, dass die Bedeutung von IT-Sicherheit und Datenschutz in der Unternehmenspraxis des Mittelstands groß ist.[1]

Der Mittelstand investiert in digitalen Schutz

Zwischen 2013 und 2015 haben 85 % der kleinen und mittleren Unternehmen (KMU) Maßnahmen zur Verbesserung des Datenschutzes und ihrer IT-Sicherheit ergriffen. Bei den größeren KMU (zehn und mehr Beschäftigte) haben 95 % der Unternehmen spezifische Maßnahmen umgesetzt. Hier spielen der mit der Unternehmensgröße wachsende Einsatz von IT-Anwendungen sowie die oftmals stärkere Vernetzung eine Rolle.

Grafik 1: Maßnahmen zur Verbesserung der IT-Sicherheit und des Datenschutzes (2013–2015)

Unternehmensanteile jeweils in Prozent, nur Unternehmen mit Maßnahmen, Mehrfachnennung möglich.



Quelle: KfW-Mittelstandspanel 2015 (Zusatzbefragung im September 2015)

Hinweis: Dieses Papier gibt die Meinung der Autoren wieder und repräsentiert nicht notwendigerweise die Position der KfW.

ISSN 2194-9433

Was tun die Unternehmen konkret?

Im genannten Zeitraum haben fast neun von zehn KMU entsprechende (Standard-) Softwarekonzepte implementiert (87 %). Mit großem Abstand ist diese – relativ kostengünstige und rasch umzusetzende – Maßnahme der häufigste Schritt hin zu mehr IT-Sicherheit (beispielsweise Virenschutz, Firewalls, Spamfilter, Patch-Management).

Backup-Konzepte (49 %), der Einsatz von Verschlüsselungstechniken (44 % – bspw. für Email-Verkehr, USB-Sticks, Festplatten) und die Einrichtung von Berechtigungskonzepten (43 % – bspw. Passwörter, Protokollierung von Zugriffen) spielen dagegen bereits eine deutlich geringe Rolle.

Eher umfangreiche und teilweise Maßnahmen mit höheren Kosten, wie Mitarbeiterschulungen (bspw. zur Schaffung eines Bewusstseins für Datenschutzprobleme, Aufklärung über gesetzliche Regelungen), Beauftragung eines externen IT-Sicherheits-Dienstleisters und bauliche Maßnahmen werden erheblich häufiger von größeren KMU mit zehn oder mehr Beschäftigten in Angriff genommen.

Gesetzliche Vorgaben ergänzen die eigene Initiative

Die Mittelständler werden dabei sowohl von sich aus präventiv aktiv, als auch durch umfassende gesetzliche Vorgaben dazu aufgefordert (siehe Erläuterungskasten). Dabei ist das gesteigerte Auftreten der personalbezogenen Maßnahmen bei den größeren Unternehmen womöglich zum Großteil der Notwendigkeit eines betrieblichen Datenschutzbeauftragten (bDSB) ab einer Unternehmensgröße von zehn Beschäftigten zuzuschreiben. Dieser bDSB kann dabei aus der Belegschaft heraus rekrutiert oder extern beauftragt werden. Beide Varianten spiegeln sich in Grafik 1 wider.

Aktuell ausreichender Schutz? Über die Hälfte der KMU sagen ja …

Bereits jetzt sieht sich mehr als die Hälfte der Unternehmen beim Datenschutz gut aufgestellt: Fünfundfünfzig Prozent der KMU attestieren sich einen aktuell ausreichenden Schutz. Vergleichbare Studien kommen zu ähnlichen Ergebnissen.[2] Die Einschätzung findet sich in der gesamten Breite des Mittelstands, über sämtliche Segmente hinweg. Im Dienstleistungssektor gilt dies sogar für 58 %.

Das heißt jedoch zugleich: Fünfundvierzig Prozent der KMU sieht sich aktuell noch nicht ausreichend geschützt. Hier besteht Skepsis bei den Unternehmen hinsichtlich eines angemessenen Sicherheitsniveaus. Bedenklich stimmt außerdem, dass am aktuellen Rand der Aufwand im Mittelstand für mehr Schutzmaßnahmen eher zu stagnieren scheint.[3]

Datenschutz in der Unternehmenspraxis: Die aktuelle Gesetzeslage

Unternehmen mit einem Sitz in Deutschland sind dem Bundesdatenschutzgesetz (BDSG) unterworfen. Die Regelungen des BDSG behandeln dabei den Schutz der Daten natürlicher Personen: Alle personenbezogenen Daten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener), müssen von Unternehmen vertraulich und sicher behandelt werden. Geschützt werden müssen dabei nicht nur Daten von Kunden, Mitarbeitern und Geschäftspartnern sondern sämtliche Daten, die Rückschlüsse auf diese Personen zulassen würden.

Laut BDSG müssen Unternehmen – unabhängig von Größe oder Wirtschaftszweig – geeignete Maßnahmen ergreifen, um die Vertraulichkeit und Sicherheit personenbezogener Daten zu gewährleisten. Hierzu zählt eine Reihe von technischen und organisatorischen Maßnahmen, deren Anwendung verhältnismäßig sein muss und daher für Unternehmen auf unterschiedlichem Niveau Anwendung findet (bspw. Zutrittskontrolle, Zugangs- und Zugriffskontrolle, Weitergabekontrolle).

Sind mindestens zehn Personen (gleich ob Vollzeit, Teilzeit, Auszubildende, etc.) mit der automatisierten Verarbeitung von personenbezogenen Daten, d. h. unter EDV-Einsatz beschäftigt, besteht die Pflicht, einen betrieblichen Datenschutzbeauftragten (bDSB) zu stellen. Der bDSB muss die erforderliche Fachkunde vorweisen können (Zertifikat, Studium, Berufserfahrung). Verzichtet ein Unternehmen auf die Bestellung eines Datenschutzbeauftragten steht der Inhaber bzw. Geschäftsführer selbst in Haftung und muss für die Einhaltung der Datenschutzbestimmungen Sorge tragen.

Neben dem BDSG existieren für jedes Bundesland spezielle Datenschutzgesetze sowie branchen- bzw. tätigkeitsspezifische gesetzliche Regelungen, die in ihrer Anwendung gegenüber dem BDSG immer Vorrang haben (z. B. Verschwiegenheitspflichten von Ärzten und Anwälten).

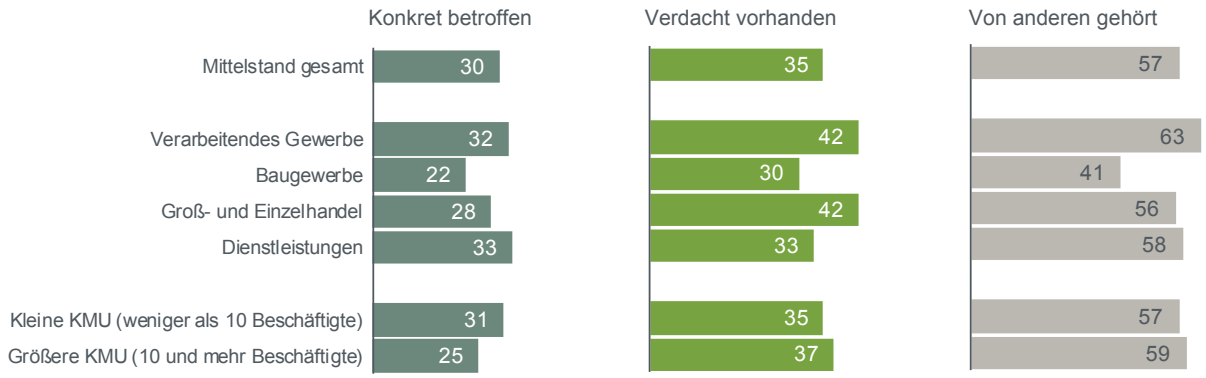
… aber Sicherheitsprobleme im Mittelstand keine Ausnahmeerscheinung

Die von den Mittelständlern getroffenen Maßnahmen sind nötig. Denn der wachsende Digitalisierungsgrad geht Hand in Hand mit sich verbreiternden Angriffsflächen: Von 2013 bis 2015 waren mehr als eine Million kleiner und mittlerer Unternehmen (KMU) in Deutschland von den Folgen eines Angriffs auf ihre IT-Sicherheit und Datenbestände betroffen – und damit fast jeder dritte Mittelständler (30 % – Grafik 2).

Cyberkriminalität[4] ist folglich keine Ausnahmeerscheinung im Mittelstand. Wird berücksichtigt, dass „lediglich“ ein Dreijahreszeitraum abgebildet wird, kann angenommen werden, dass die überwiegende Mehrheit der KMU bereits konkrete Erfahrungen hat.

Grafik 2: Häufigkeit von IT-sicherheitsrelevanten Vorfällen – nach Branchen und Größenklassen (2013–2015)

Unternehmensanteile jeweils in Prozent



Quelle: KfW-Mittelstandspanel 2015 (Zusatzbefragung im September 2015)

Kleine Mittelständler sogar häufiger im Visier

Die Gefährdungslage für kleine KMU ist nicht zu unterschätzen. Mit 31 % konkreter Betroffenheit übersteigt die Häufigkeit von Cyberkriminalität die von größeren KMU (25 %). Die öffentliche Diskussion wird zwar von (bekannt gewordenen) Fällen bei Großunternehmen beherrscht: Apple, Sony, T-Mobile oder Microsoft:[5] Allesamt waren sie in jüngster Vergangenheit betroffen von elektronischer Kriminalität. Auch öffentliche Institutionen bleiben nicht verschont. Im Sommer 2015 gelang es Hackern in das IT-Netzwerk des Deutschen Bundestages einzudringen.[6] Das KfW-Mittelstandspanel zeigt dennoch: Auch kleine Unternehmen sind nicht vor Bedrohungen sicher.

Sichtbar ist ebenso die unterschiedliche Bedrohungslage nach Branchen. Unternehmen des Verarbeitenden Gewerbes haben vergleichsweise häufig mit Folgen von Angriffen auf ihre IT-Sicherheit zu kämpfen bzw. hegen zumindest einen Verdacht. Hingegen sind Mittelständler aus dem Baugewerbe weniger anfällig – in der gesamten Branche äußern lediglich 41 % der KMU etwas von anderen Unternehmen gehört zu haben.

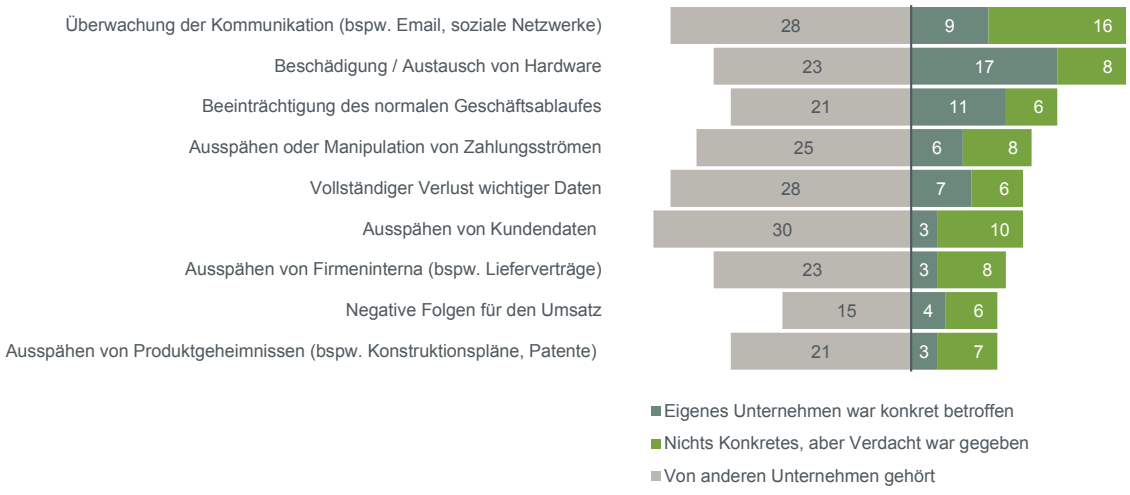
Hardware und Kommunikationsüberwachung am meisten im Fokus

Die Beschädigung bzw. der notwendige Austausch von Hardwarekomponenten rangiert an erster Stelle der konkret im eigenen Unternehmen erfahrenen Folgen (17 %). Elf Prozent der KMU berichten von einer Beeinträchtigung des Geschäftsablaufes. Die Überwachung der Unternehmenskommunikation (bspw. durch Emails) hat im Zeitraum 9 % der Mittelständler getroffen – weitere 16 % haben aber zumindest einen entsprechenden Schadensverdacht. Den vollständigen Verlust wichtiger Daten vermelden 7 % der KMU.

Dabei ist Folgendes zu berücksichtigen: In der öffentlichen Wahrnehmung spielen Angriffe Externer oft eine übergeordnete Rolle. Nicht zuletzt durch die öffentlichkeitswirksame Diskussion prominenter Fälle. Vorhandene Erkenntnisse deuten allerdings darauf hin, dass in der breiten Masse die Schäden aber eher von eigenen oder ehemaligen Mitarbei-

Grafik 3: IT-sicherheitsrelevante Vorfällen im Einzelnen (2013–2015)

Unternehmensanteile jeweils in Prozent



Quelle: KfW-Mittelstandspanel 2015 (Zusatzbefragung im September 2015)

tern verursacht werden – sei es durch irrtümliches Fehlverhalten (bspw. Verlust von Datenträgern, unbeabsichtigtes Einbringen von Schadsoftware in das Unternehmensnetzwerk) oder – deutlich weniger häufig – vorsätzlich (bspw. Verkauf von Kundendaten).[7]

Vermutlich hohe Dunkelziffer

Nicht in jedem Fall haben betroffene Unternehmen stichhaltige Nachweise für Sicherheitsvorfälle. Über alle genannten Schadensfolgen sind es 35 % der Mittelständler, die einen Verdacht hegen, aber keine konkreten Hinweise vorliegen haben (Grafik 2). Hinzu kommen diejenigen Fälle, in denen ein Angriff vom Unternehmen unentdeckt bleibt. Über deren Häufigkeit lässt sich lediglich spekulieren. Die „Dunkelziffer" tatsächlich stattgefundener Angriffe könnte demnach entsprechend höher sein.

Zumindest einen Anhaltspunkt liefert folgende Erkenntnis: Unternehmen haben häufiger von konkreten Fällen in anderen Unternehmen Kenntnis erhalten, als dass sie selbst Betroffenheit bekanntgeben (Grafik 2).

Dazu passt, dass gemäß Bundeskriminalamt (BKA) das Anzeigeverhalten betroffener Unternehmen sehr verhalten ist:[8] Rund 87 % der von Cyber-Angriffen betroffenen Unternehmen erstatten demnach keine Anzeige. Die Gründe können vielfältig sein, so u. a.:

- Anzeigeverzicht, da eigener Mitarbeiter und firmeninterne Regulierung.
- Angriffe werden abgewehrt. Schäden sind nicht erkennbar.
- Angriffe auf das Unternehmen bleiben unentdeckt oder werden nicht als solche wahrgenommen.
- Fehlende Sensibilisierung bei den verantwortlichen Personen.
- Sorge vor Reputationseinbußen und Wettbewerbsnachteilen.

Nur Kosten – kein messbarer Ertrag: Das bremst die Unternehmen

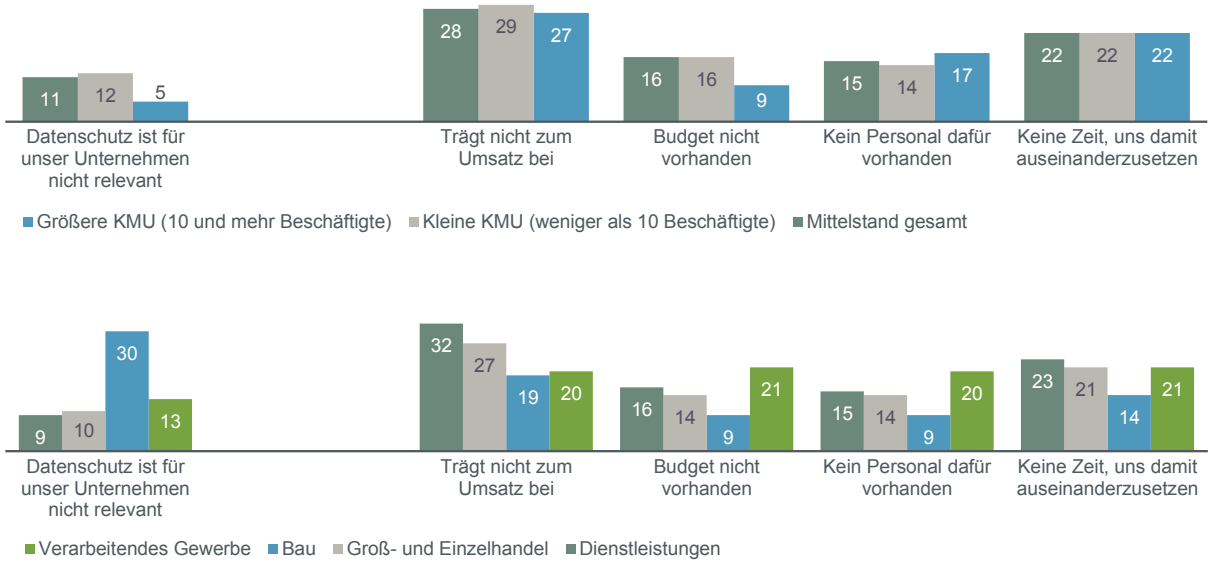
Datenschutz verursacht Aufwand und Kosten, schlägt sich parallel aber nicht in den Einnahmen der Unternehmen nieder. Ein unmittelbarer Umsatzbeitrag ist nicht erkennbar – Eine Ansicht, die viele Mittelständler teilen: Fast ein Drittel der KMU (28 %) hält dies ab, weitere Verbesserungen des Datenschutzes vorzunehmen. Vor allem KMU aus Dienstleistungsbranchen sehen hier eine Hürde.

Diese Sicht ist nachvollziehbar, birgt allerdings die Gefahr, dass der Handlungsdruck verkannt wird. Datenschutz wird vielfach nicht als drängendes Problem wahrgenommen. Das Dilemma: Bei Angriffen auf die IT-Sicherheit könnten dennoch Umsatzfolgen spürbar werden und zwar im negativen Sinn. Immerhin hat bereits jeder zehnte Mittelständler zumindest den Verdacht zwischen 2013–2015 mit negativen Umsatzfolgen aufgrund eines Cyberangriffes konfrontiert gewesen zu sein (Grafik 3). Mit anderen Worten: 150.000 KMU waren allein in diesen drei Jahren konkret betroffen – weitere 220.000 hatten den Verdacht. Es gilt, das Gefahrenbewusstsein weiter zu schärfen.

Unzureichendes Budget für (weitere) Sicherheitsmaßnahmen spielt bei 16 % der Unternehmen eine Rolle. Größere Mittelständler sind ressourcenstärker – in diesem Segment ist das nur bei 9 % der KMU ein Hindernis. Unternehmen des Verarbeitenden Gewerbes sehen Budgetrestriktionen deutlich häufiger als Schwierigkeit (21 %). Das lässt sich darauf zurückführen, dass Produktionsanlagen mitunter aufwendigere

Grafik 4: Gründe gegen eine weitere Verbesserung des Datenschutzes nach Größenklassen und Branchen

Unternehmensanteile jeweils in Prozent, Mehrfachnennung möglich



Quelle: KfW-Mittelstandspanel 2015 (Zusatzbefragung im September 2015)

– und damit teurere – Maßnahmen erfordern, um dem BDSG gerecht zu werden (siehe Kasten) wie bspw. Fenstersicherungen, Umzäunung, Alarmanlagen oder Sicherheitsverglasung. Nötige Investitionen stehen dann in Konkurrenz zu anderen investiven Maßnahmen.

Den Unternehmen fehlt die Zeit

Kein ausreichendes Personal zu haben scheint im Vergleich wenig ausschlaggebend (15 %). Hingegen findet jedes fünfte Unternehmen (22 %) nicht die Zeit, sich gezielt mit Datenschutz auseinander zu setzen. Gesetzliche Neuerungen oder geänderte Gefahrenlagen könnten damit allerdings übersehen werden.

So ist deutschen Unternehmen möglicherweise nicht bewusst, dass sie derzeit ohne gesonderte Verträge keine personenbezogenen Daten in die USA übermitteln dürfen – der Europäische Gerichtshof (EuGH) hat das Safe-Harbor-Abkommen im Oktober 2015 gekippt (siehe Kasten).

Nicht zuletzt bleibt abzuwarten, welche konkreten Änderungen die Ende 2015 von der EU beschlossene Datenschutzgrundverordnung (DSGVO) in der Unternehmenspraxis mit sich bringt. Die Verordnung ersetzt die seit 1995 geltende EU-Datenschutzrichtlinie und zielt auf die Vereinheitlichung von rechtlichen Standards im Datenschutz in Europa. Die DSGVO wird mit Inkrafttreten ab dem 1. Januar 2018 das aktuelle BDSG weit gehend ablösen. Die Übergangszeit sollten KMU daher nutzen, sich mit den neuen Regelungen vertraut zu machen. Aktuell ist beispielweise noch nicht final geregelt, inwieweit die Pflicht zu einem bDSB auch für KMU unter der neuen Verordnung gilt. Auch die Strafen für die Missachtung der dann geltenden Regelungen steigen stark.

Baugewerbe sieht die geringste Relevanz

Für einen weiteren Teil der Unternehmen ist Datenschutz und IT-Sicherheit kein relevantes Thema für ihr Unternehmen (11 %). Speziell KMU aus dem Baugewerbe stechen hervor: Eines von drei KMU sieht für das eigene Unternehmen keine Relevanz (30 %). Für diese KMU lässt sich allerdings auch die geringste Häufigkeit von Angriffen im Zeitraum 2013–2015 feststellen.

EuGH erklärt Safe-Harbor für unzulässig

Europäische Unternehmen, die personenbezogene Daten in die USA übertragen möchten, konnten sich bislang auf das Safe-Harbor-Abkommen beziehen. US-Amerikanische Unternehmen unterwarfen sich darin den EU-Datenschutzvorgaben. Am 6. Oktober 2015 erklärte der EuGH das Abkommen für unwirksam, da die Daten von Europäern nicht ausreichend geschützt seien.

Unternehmen müssen nun prüfen, ob sie Daten in die USA übermitteln (bspw. im Rahmen von Cloud Computing). Dabei müssen sie gesondert anhand von vertraglichen Regeln mit ihren amerikanischen Geschäftspartnern agieren, wenn Daten transferiert werden sollen. Zudem muss es bindende, unternehmensinterne Vorschriften zur Datenübermittlung innerhalb eines Konzerns geben, welchen den EU-Standards entsprechen. Hierfür legte die EU-Kommission Leitlinien vor.

Fazit

Die Digitalisierung birgt Potenzial für die zukünftige Wettbewerbsposition von Unternehmen. Damit sich dieses Potenzial entfalten kann, müssen Schadensrisiken abgewendet werden. Vorkehrungen in den Bereichen IT-Sicherheit und Datenschutz sind ratsam und unabdingbar. Das zeigen unsere Ergebnisse deutlich.

Aktuell fühlt sich über die Hälfte der KMU ausreichend geschützt. Dennoch besteht Handlungsbedarf. Vor allem personelle Maßnahmen werden noch vergleichsweise (zu) selten in Angriff genommen. Das könnte sich künftig rächen. Die Digitalisierung von Geschäftsprozessen wird weiter rasch zunehmen – neue Technologien kommen dazu. Derzeit eventuell ausreichender Schutz kann schnell überholt sein. Auch wurde unlängst mehrfach die Zunahme elektronischer Kriminalität festgestellt.[9] Umso wichtiger ist es für Unternehmen daher, kontinuierlich ihre Schutzvorkehrungen auf den Prüfstand zu stellen.

Das aber erfordert mehr als einmalige Anpassungen, sondern dauerhafte Anstrengungen: Monitoring der rechtlichen Vorgaben sowie Umsetzung neuer Gesetze, Übernahme neuer Standards oder schlicht das Erkennen und Beheben von Sicherheitslücken in Anwendersoftware. Der Bedarf an Fachkenntnissen auf der Ebene der Mitarbeiter ist dabei entscheidend. Genau hier lässt sich aber Nachholbedarf feststellen, vor allem bei den kleineren Mittelständlern.

IT-Sicherheit und Datenschutz dürfen aus Unternehmenssicht nicht als „lästige“ Aufgabe, sondern sollten verstärkt als Absicherung der Wettbewerbsfähigkeit wahrgenommen werden. ■

Die Datenbasis: Das KfW-Mittelstandspanel

Das KfW-Mittelstandspanel wird seit dem Jahr 2003 als Wiederholungsbefragung der kleinen und mittleren Unternehmen in Deutschland durchgeführt. Zur Grundgesamtheit des KfW-Mittelstandspanels gehören alle privaten Unternehmen sämtlicher Wirtschaftszweige, deren Umsatz die Grenze von 500 Mio. EUR pro Jahr nicht übersteigt.

Mit einer Datenbasis von bis zu 15.000 Unternehmen pro Jahr stellt das KfW-Mittelstandspanel die einzige repräsentative Erhebung im deutschen Mittelstand und damit die wichtigste Datenquelle für mittelstandsrelevante Fragestellungen dar. Der Befragungszeitraum der Hauptbefragung der 13. Welle lief vom 23.02.2015 bis 26.06.2015.

Die hier vorgelegten Ergebnisse basieren auf einer ergänzenden Befragung zum KfW-Mittelstandspanel 2015. Diese Erhebung wurde im Zeitraum 08.09.–18.09.2015 durchgeführt. Befragt wurden sämtliche Unternehmen, die bereits zur Hauptuntersuchung teilnahmen und zu denen eine valide E-Mail Adresse bekannt war. Insgesamt konnten Antworten von etwa 2.200 Unternehmen berücksichtigt werden. Aufgrund der Anbindung an das KfW-Mittelstandspanel geben auch die hier vorgelegten Sonderauswertungen zum Themenkomplex Datenschutz und IT-Sicherheit im Mittelstand ein repräsentatives Abbild.

Weiterführende Informationen sowie den aktuellen Jahresbericht finden Sie im Internet unter: www.kfw-mittelstandspanel.de

[1] Siehe KfW-Mittelstandspanel 2015, https://www.kfw.de/KfW-Konzern/KfW-Research/KfW-Mittelstandspanel.html

[2] Vgl. WIK-Consult GmbH (2012), IT-Sicherheitsniveau in kleinen und mittleren Unternehmen, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie, S. 34.

[3] Deutschland sicher im Netz (DsiN) (2015), DsiN-Sicherheitsmonitor 2015, Berlin.

[4] Cybercrime oder Cyberkriminalität ist laut Bundeslagebild Cybercrime (2014) des BKA definiert als alle Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten oder mittels dieser Informationstechnik begangen werden. Darunter fallen folgende Delikte: Computerbetrug (PKS 517500), Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS 517900), Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (PKS 543000), Datenveränderung / Computersabotage (PKS 674200) sowie Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen (PKS 67800).

[5] Siehe unter anderem: ZEIT Online (2015), Hacker schmuggeln Malware in den App Store, http://www.zeit.de/digital/datenschutz/2015-09/apple-app-store-malware-xcodeghost. – DIE WELT (2014), Hacker knipsen Playstation- und Xbox-Netzwerke aus, http://www.welt.de/wirtschaft/webwelt/article135743908/Hacker-knipsen-Playstation-und-Xbox-Netzwerke-aus.html. – Spiegel Online (2015), Hacker erbeuten Daten von Millionen T-Mobile-Kunden, http://www.spiegel.de/netzwelt/web/hacker-erbeuten-daten-von-millionen-t-mobile-us-kunden-a-1055828.html.

[6] Siehe unter anderem: Spiegel ONLINE (2015), Cyberattacke auf Bundestag-Es droht ein Millionenschaden, http://www.spiegel.de/netzwelt/web/cyberattacke-auf-bundestag-es-droht-ein-millionenschaden-a-1038178.html. – Süddeutsche Zeitung (2015): Bundestag bekommt Hackerangriff nicht unter Kontrolle, http://www.sueddeutsche.de/politik/berlin-bundestag-bekommt-hackerangriff-nicht-unter-kontrolle-1.2515345. – FAZ (2015), Hackerangriff auf Bundestag-Anfällige Systeme, http://www.faz.net/aktuell/politik/inland/hackerangriff-auf-bundestag-anfaellige-systeme-13642190.html#.

[7] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2015): Cyber-Sicherheits-Umfrage 2015; S.16.

[8] Vgl. dazu KPMG (2015), e-crime. Computerkriminalität in der deutschen Wirtschaft, Berlin, - Bundeskriminalamt (2013), Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime, http://www.bka.de/nn_238144/SharedDocs/Downloads/DE/ThemenABisZ/InternetKriminalitaet/handlungsempfehlungenWirtschaft.html. – Landeskriminalamt Niedersachsen (2013), Befragung zu Sicherheit und Kriminalität in Niedersachsen.

[9] Mittlerweile versucht eine Reihe von Studien das Bedrohungs- sowie Betroffenheitspotenzial elektronische Kriminalität für Unternehmen zu erfassen und zu quantifizieren. Meist handelt es sich dabei aber um vergleichsweise kleine Samples oder Erhebungen ohne den Anspruch der Repräsentativität. Dennoch sind die Ergebnisse eindeutig: Elektronische Kriminalität nimmt zu. Siehe hierzu beispielsweise WIK-Consult GmbH (2012), IT-Sicherheitsniveau in kleinen und mittleren Unternehmen, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie. – KPMG (2015), e-crime. Computerkriminalität in der deutschen Wirtschaft, Berlin. – Deutschland sicher im Netz (DsiN) (2015), DsiN-Sicherheitsmonitor 2015, Berlin. – Allianz für Cyber-Sicherheit (2015), Cyber-Sicherheits-Umfrage 2015, im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik.