2015
Informationssicherheit
in deutschen Unternehmen

Mit Sicherheit sicher!

Inhalt

Überblick

2015 hat Shred-it seine Security Tracker Studie zur Informationssicherheit in Unternehmen erstmals auch in Deutschland durchgeführt. Das Meinungsforschungsinstitut Ipsos Reid befragte im Auftrag von Shred-it 1.000 Inhaber von Betrieben mit weniger als 100 Mitarbeitern und 100 Führungskräfte aus Unternehmen mit mehr als 250 Mitarbeitern zum Thema Datenschutz – mit teils überraschenden Ergebnissen.

Denn: Obwohl Datenschutz und Informationssicherheit unter anderem aufgrund der NSA-Affäre weiterhin großer Bestandteil des gesellschaftlichen Diskurses sind, haben insbesondere kleine und mittelständische Betriebe beim Verständnis und der Umsetzung von Datenschutzrichtlinien großen Nachholbedarf. Unsere Infografik (Seite 5) zeigt die Resultate auf einen Blick.

Informationssicherheit in Unternehmen muss sich gleichzeitig aktuellen Trends des deutschen Arbeitsmarktes anpassen: Flexible Arbeitsmodelle werden beliebter, mobile Endgeräte gehören zum betrieblichen Standard. Das hat Konsequenzen für den betrieblichen Datenschutz. Shred-it hilft Führungskräften, Datenschutzbeauftragten und Mitarbeitern mit einfachen Tipps, durchgängige Informationssicherheit auch bei flexibler Arbeitsplatzgestaltung zu gewährleisten.

Eine der größten potentiellen Sicherheitslücken im Unternehmen sind leider nach wie vor die Mitarbeiter: Viele Datenverluste entstehen, weil schlicht die Richtlinien für die Aufbewahrung und Vernichtung vertraulicher Informationen nicht beachtet werden oder gar unbekannt sind. Shred-it stellt Maßnahmen vor, mit denen Betriebe weltweit bereits erfolgreich mehr Informationssicherheit gewährleisten.

Beim Verständnis und der Umsetzung von Datenschutz-richtlinien können beispielsweise externe Datenschutzbeauftragte helfen. Sie unterstützen Geschäftsinhaber und Führungskräfte in diesem hochsensiblen Themenbereich. Shred-it sprach mit dem Datenschutzbeauftragten Jürgen Hartz darüber, woran die Informationssicherheit in vielen Unternehmen derzeit noch scheitert. Seine Einblicke aus der Praxis lesen Sie in Kapitel 6.

Grundlegend für die Informationssicherheit und die Vermeidung geschäftsschädigender Datenverluste ist die Kenntnis der Gesetzeslage. Beim Thema Datenschutz gibt es in Deutschland rechtlich verschiedene Perspektiven – Shred-it gibt einen Überblick.

Der Shred-it State of the Industry Report fasst die neuesten Entwicklungen und die größten Herausforderungen deutscher Unternehmen im Bereich Informationssicherheit zusammen und gibt Tipps, wie diese Herausforderungen gemeistert werden können. So trägt Shred-it dazu bei, die Informationssicherheit in Deutschland Schritt für Schritt zu verbessern.

Stand der Informationssicherheit in deutschen Unternehmen: Nach wie vor viele Wissenslücken

2015 führte Shred-it erstmals gemeinsam mit dem Ipsos Reid Institut die Security Tracker Studie zur Informationssicherheit in Unternehmen auch in Deutschland durch. Befragt wurden 1.000 Inhaber von Betrieben mit weniger als 100 Mitarbeitern, sowie 100 Führungskräfte aus Unternehmen mit mehr als 250 Mitarbeitern. Fazit: Beim Thema Informationssicherheit haben viele deutsche Unternehmen Nachholbedarf – insbesondere kleine und mittelständische Betriebe.

Was sind vertrauliche Daten?

Die Probleme beginnen schon ganz am Anfang: Auch im Jahr 2015 besteht in kleineren Betrieben weiterhin Unsicherheit bei der Frage, welche Daten tatsächlich sicher aufzubewahren und zu vernichten sind. 35% der Befragten aus Betrieben mit weniger als 100 Mitarbeitern gaben an, dass ihre Betriebe keinerlei Dokumente besitzen, deren Verlust sich geschäftsschädigend auswirken würde.

„Von Betrieben bei denen wir uns vorstellen hören wir sehr häufig, man habe gar keine schützenswerten Daten“, bestätigt Peter Husseck, Vizepräsident von Shred-it Deutschland und Österreich, die Ergebnisse der Studie aus eigener Erfahrung. „In vielen Fällen ist das ein Trugschluss. Fast jedes Unternehmen besitzt und verarbeitet personenbezogene Daten von Mitarbeitern und Kunden.“ Diese fallen per Datenschutzgesetz in den Bereich vertraulicher Informationen und müssen entsprechend behandelt werden.

Besser sieht die Lage bei den Verantwortlichen größerer Unternehmen aus. Sie nannten vor allem Kundendaten (51%), Finanzaufzeichnungen (15%), Personalakten (11%), sowie interne Korrespondenzen (15%) als besonders geschäftsschädigend, sollten diese in falsche Hände gelangen.

Kenntnis der rechtlichen Vorschriften

Aber auch bei größeren Unternehmen besteht noch Aufklärungsbedarf: Nur 67% der Befragten aus Unternehmen mit mehr als 250 Mitarbeitern gaben an, sich sehr gut mit den rechtlichen Bestimmungen des Bundesdatenschutzgesetzes zur Aufbewahrung und Vernichtung vertraulicher Informationen auszukennen. Unter den Befragten aus kleinen Betrieben kannten sich gar nur 35% mit der aktuellen Gesetzeslage aus.

Wie sieht es in der Praxis aus?

Mehr als die Hälfte der Verantwortlichen aus größeren Unternehmen bestätigten, dass in ihrem Betrieb ein festes Protokoll für die Aufbewahrung und Vernichtung vertraulicher Informationen gibt, das von den Mitarbeitern auch streng befolgt wird. 42% wiederum sagten, dass ein solches Protokoll existiere, aber nicht alle Mitarbeiter davon Kenntnis hätten. Da 80% der Unternehmen Ihre Mitarbeiter mindestens einmal jährlich im Bereich Informationssicherheit schulen, scheinen hier andere Faktoren einer ordnungsmäßen Umsetzung der Vorschriften im Wege zu stehen.

Ganz anders das Bild in den Betrieben mit weniger als 100 Mitarbeitern: In 70% dieser Betriebe existieren keinerlei feste Vorschriften für den Umgang mit vertraulichen Informationen. Das zeigt sich natürlich in der konkreten Umsetzung: Während in 35% der größeren Unternehmen vertrauliche Daten in verschließbare Konsolen geworfen werden und ein professioneller Aktenvernichtungs-Dienstleister das Schreddern übernimmt, schreddern 70% der kleineren Betriebe selbstständig.

Einschätzung der Konsequenzen eines Datenverlustes

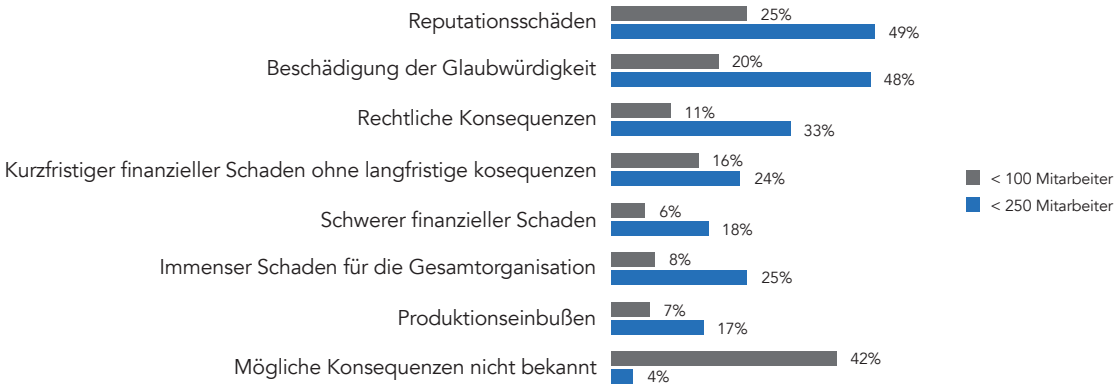


Abb. 1: Welche Folgen hätte es für Ihr Unternehmen, sollten vertrauliche Informationen Ihres Unternehmens verloren gehen oder gestohlen werden?

Die mangelnde Umsetzung von Datenschutzrichtlinien im Betrieb rührt sicher auch daher, dass sich die Risikowahrnehmung zwischen kleineren und größeren Betrieben deutlich unterscheidet. Die Security Tracker Studie ergab, dass die Befragten kleinerer Betriebe die Konsequenzen des Verlustes vertraulicher Daten für ihr Unternehmen deutlich geringer einschätzen, als die Verantwortlichen der Unternehmen mit mehr als 250 Mitarbeitern. Immerhin 42% der Inhaber kleiner Unternehmen konnten keine möglichen Konsequenzen für ihr Geschäft abschätzen (siehe Abb. 1).
Ein möglicher Faktor für das geringe Risikoempfinden der kleineren Betriebe: 77% von ihnen haben (wissentlich) noch keinen Datenverlust erlitten, während 63% der befragten größeren Unternehmen bereits mit einer solchen Situation konfrontiert waren und dabei vor allem Reputationsschäden erlitten haben.

Einbindung von Experten

Bei der Optimierung der Datensicherheit helfen kann beispielsweise ein interner oder externer Datenschutzbeauftragter, wie im Bundesdatenschutzgesetz für Betriebe mit mehr als 20 Mitarbeitern vorgesehen. Entsprechend haben 92% aller Unternehmen mit mehr als 250 Mitarbeitern einen solchen Experten an der Hand – allerdings nur rund ein Fünftel der kleineren Betriebe.

Vorteile der Beratung durch einen Datenschutzbeauftragten: Dieser kennt sich mit der komplexen rechtlichen Situation in Deutschland aus, begleitet nach Wunsch die Einführung eines festgelegten Protokolls für Informationssicherheit nach DIN-Standard (DIN 66399) und unterstützt bei regelmäßigen Audits der bestehenden Datenschutzprozesse. Dies passiert in 47% aller befragten Unternehmen selten oder gar nicht.

INFORMATIONSSICHERHEIT AUF DER SPUR

UMGANG MIT DATEN IN KLEINEN UND MITTLEREN UNTERNEHMEN

DEFIZITE

SCHULUNG

53% schulen ihre Mitarbeiter nicht im **Bereich Datensicherheit**

PROTOKOLL

70% haben keine Bestimmungen für die **Aufbewahrung und Vernichtung vertraulicher Daten**

75% haben keine **Bestimmungen für Internetsicherheit**

22% haben keine Möglichkeit, vertrauliche Dokumente **sicher aufzubewahren und zu vernichten**

WISSEN

35% sagten aus, dass ihre Betriebe **keinerlei Dokumente besitzen, deren Verlust sich geschäftsschädigend auswirken würde**

13% kennen nicht die **rechtlichen Bestimmungen**

EXPERTE

81% haben keinen **Datenschutzbeauftragten**

92% arbeiten nicht mit einem **professionellen Dienstleister** für Aktenvernichtung zusammen

KONSEQUENZEN

23%
hatten bereits eine DATENPANNE.

Diese zogen **finanzielle Schäden, den Verlust von Kunden und Reputation und / oder rechtliche Konsequenzen nach sich.**

Die Zahl der Datensätze, die bei DATENPANNEN in 2014 verloren gingen, rangierte zwischen

5.100 UND 81.600

IM DURCHSCHNITT WAREN ES: **24.103**

DIREKTE KOSTEN:

€69 PRO DATENSATZ

DATENPANNEN kosten Unternehmen im Schnitt €152 pro verlorenen Datensatz.

IN 2014 betrugen die Gesamtkosten für DATENPANNEN in deutschen Unternehmen

€3.52 MIO

Alle dargestellten Ergebnisse stammen aus einer Studie, die 2015 von Ipsos im Auftrag von Shred-it durchgeführt wurde. Befragt wurden 1.000 Inhaber von Betrieben mit weniger als 100 Mitarbeitern.

Weitere Quellen: 2015 Cost of Data Breach Study: Germany; durchgeführt vom Ponemon Institut LLC, finanziert durch IBM

Shred-it Mit Sicherheit sicher.™

Wenn Sie erfahren möchten, wie Sie potentielle Risiken in Ihrem Unternehmen aufdecken und Ihre vertraulichen Informationen schützen können, kontaktieren Sie Shred-it und buchen Sie einen kostenlosen Sicherheitscheck unter 0800 0281160 oder besuchen Sie shredit.de.

Trendthemen in der Informationssicherheit: Flexible Arbeitsmodelle, mobile Enderäte und mangelnder Datenschutz

Aktuellen Trends im deutschen Arbeitsmarkt zeigen, dass flexible Arbeitsmodelle für Arbeitgeber und Mitarbeiter an Bedeutung gewinnen. Die rasante Weiterentwicklung von mobilen Geräten bietet nicht nur viele Chancen für Unternehmen verschiedener Geschäftsbereiche - Mobilität wird mit anziehender Konjunktur und zunehmendem Fachkräftemangel auch zu einem entscheidenden Wettbewerbsvorteil. Doch diese Entwicklung hat auch Konsequenzen für den betrieblichen Datenschutz.

Nachfrage an flexiblen Arbeitsmodellen steigt

Laut einer aktuellen Studie des Stellenportals Monster legen Arbeitnehmer großen Wert auf flexible Arbeitszeitmodelle: Mehr als acht von zehn der befragten Stellen- und Karriereinteressierten würden am liebsten bei einem Unternehmen arbeiten, das eben diese Form der Arbeit ermöglicht. Knapp jeder Zweite stellt bei der Arbeitsplatzwahl als nötige Bedingung, von zu Hause aus arbeiten zu können.[1] Auch mobile Endgeräte sind mehrheitlich in den Berufsalltag integriert. So nutzen laut der Smart Worker Umfrage 2015 inzwischen 59% der befragten Berufstätigen geschäftlich ein Smartphone, ebenso viele ein Notebook, 30% sogar ein Tablet.[1]

Die Zukunft des mobilen Arbeitsplatzes

Viele Arbeitgeber sind aber in der Realität noch längst nicht so weit, allen Arbeitnehmern die Arbeit von zu Hause aus zu ermöglichen. Laut Monster-Studie bieten nur knapp die Hälfte der Unternehmen derzeit Heimarbeit an.[1] Insbesondere mittelständische Unternehmen sind Home Office-Regelungen gegenüber konservativ

eingestellt: Aktuell geben nur rund 19% der Befragten ihren Mitarbeitern die Möglichkeit, von zu Hause aus zu arbeiten. Immerhin: Mehr als 20% der deutschen Mittelständler möchten dieses Angebot aber zukünftig ausweiten.[1]

Sicherheitsbedrohung wird unterschätzt

Für viele Betriebe entsteht durch eine zunehmend mobile Belegschaft eine Gefahrenquelle für die Informationssicherheit, wenn Mitarbeiter vertrauliche bzw. geschäftsrelevante Daten mit ins Home Office nehmen. Dies gilt nicht nur bei dem Gebrauch von elektronischen Geräten wie Laptops und Tablets, sondern auch für Papierunterlagen. Denn auch das zeigen Studien: Das papierlose Büro ist auch 2015 noch längst nicht Alltag. Gedruckt wird weiterhin und auf hohem Niveau: 45% der in der Smart Worker Studie Befragten gaben an, dass sie in etwa gleich viel drucken wie noch vor zwei Jahren.[2]

Verständnis bei Mitarbeitern schulen

Deshalb sind spezielle Datenschutzrichtlinien für flexibles Arbeiten essentiell, um vertrauliche Informationen auf mobilen Endgeräten sowie Papier zu schützen. Dazu gehören angemessene Datenverschlüsselung und Firewalls ebenso wie Standards für die Aufbewahrung und Vernichtung von Papierunterlagen außerhalb des Büros. Wenn ein solches Datenschutzprotokoll erstellt wurde, gilt es insbesondere Mitarbeiter für das Thema zu sensibilisieren und regelmäßig in der ordnungsgemäßen Umsetzung der Richtlinien zu schulen.

Mangelhafte Umsetzung in kleinen Betrieben

In diesem Zusammenhang zeigten sich große Unterschiede in der Umsetzung von Datenschutzrichtlinien zwischen kleinen und großen Unternehmen, wie eine Umfrage von Shred-it 2015 ergeben hat: 63% der kleineren Unternehmen (bis 100 Mitarbeiter) haben keine internen Vorgaben für die Datenaufbewahrung und -vernichtung von vertraulichen Daten außerhalb des Arbeitsplatzes oder im Home Office. Im Vergleich dazu stehen größere Unternehmen wesentlich besser dar: 89% haben ein Sicherheitsprotokoll, das auch Arbeit außerhalb des Büros abdeckt.[3]

Regelungen von Dienstleistern prüfen

Der gleiche Standard sollte übrigens auch für Dienstleister und Zulieferer gelten. Bisher überprüfen allerdings nur 45% der größeren Unternehmen vor Einkauf oder Vertragsabschluss, ob der potentielle Geschäftspartner Datenschutzrichtlinien für die Heimarbeit festgelegt hat, und sogar nur 16% der kleinen Betriebe.[3]

Fazit: Es gibt noch viel Luft nach oben beim betrieblichen Datenschutz im Hinblick auf die zunehmende Mobilität der Belegschaft.

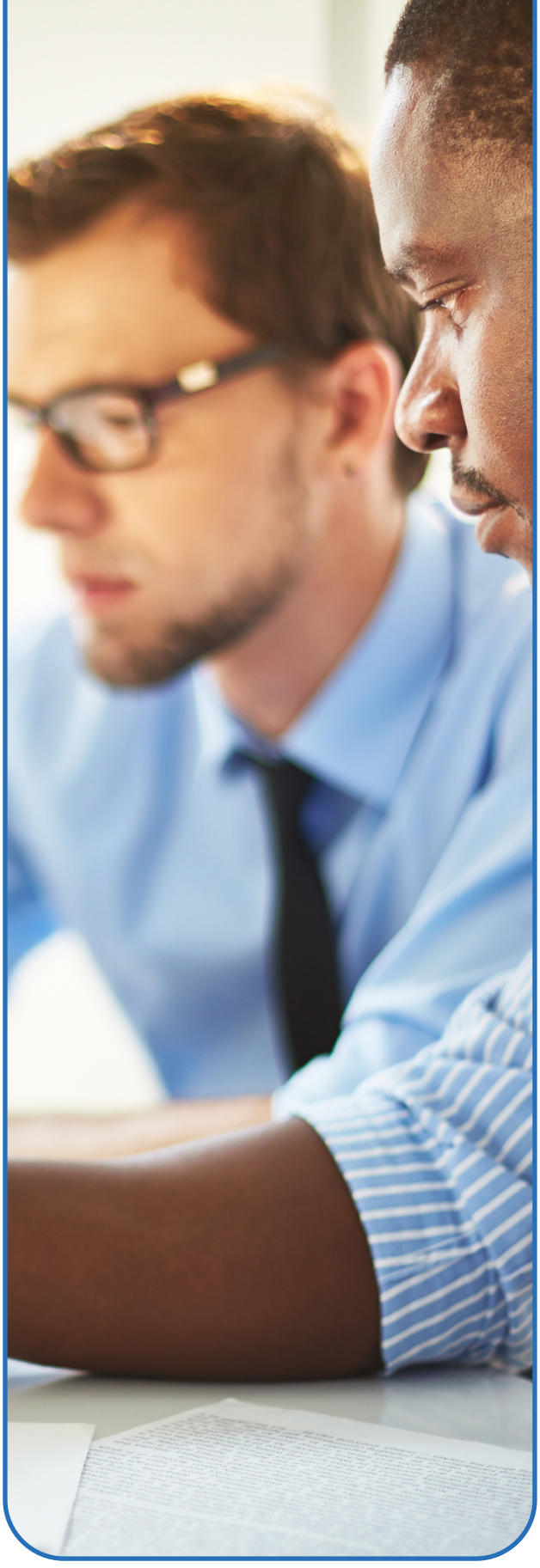
Diese Tipps helfen Führungskräften, Datenschutzbeauftragten und Mitarbeitern, Informationssicherheit auch bei flexibler Arbeitsplatzgestaltung zu gewährleisten:

- Gehen Sie grundsätzlich davon aus, dass alle Dokumente vertraulich sind und nur aus dem Büro entfernt werden sollten, wenn dies absolut notwendig ist.
- Stellen Sie sicher, dass Sie alle vertraulichen Dokumente zur sicheren Entsorgung durch einen professionellen Dienstleister zurück ins Büro bringen.
- Führen Sie auch zu Hause eine „clean-desk-policy" ein: Schließen sie vertrauliche Dokumente und mobile Geräte weg, wenn sie nicht genutzt werden.
- Vermeiden Sie das Drucken vertraulicher Informationen von Laptops oder anderen Computern aus.
- Installieren Sie Verschlüsselungstechnologien auf allen Speichergeräten.
- Stellen Sie sicher, dass Geräte mit Internet-Verbindungen durch die Sicherheitseinstellungen sowie mit Passwörtern und Firewalls geschützt sind.
- Schützen Sie bei der Arbeit an einem öffentlichen Ort Ihre Geräte und Informationen gewissenhaft. Seien Sie besonders vorsichtig, wenn Sie in öffentlichen Räumen wie Cafés oder im Park arbeiten – entsorgen Sie nichts in öffentlichen Müllcontainern.

Quellen:
1 Monster, (2015): Monster Studienreihe: Unterschrift bei flexiblen Arbeitszeitmodellen.
2 Dokulife Consulting & Brother, (2015): Smart Worker Umfrage 15.
3 Shred-it Security Tracker 2015

Mit mehr Wissen zum Ziel: Informationssicherheit leicht gemacht

Eine der größten potentiellen Sicherheitslücken im Unternehmen sind die Mitarbeiter: Viele Datenverluste resultieren aus Unkenntnis oder Nichtbeachten der Richtlinien für die Aufbewahrung und Vernichtung vertraulicher Informationen. Die aktuelle Security Tracker Studie zeigt, dass lediglich rund 20% der Befragten dieses Risiko auch als solches wahrnimmt. Doch insbesondere kleine Unternehmen ergreifen zu selten die Chance, dieses Risiko zum Schutz der eigenen Organisation zu mindern: Immerhin 70% aller kleinen Betriebe haben keine Vorgaben für die Aufbewahrung und Vernichtung vertraulicher Daten implementiert. Um die Hürden für Unternehmen kleiner zu machen, stellt Shred-it Maßnahmen vor, mit denen Betriebe weltweit bereits erfolgreich mehr Informationssicherheit gewährleisten.



Klare Richtlinien festsetzen

Die Erfahrung zeigt: Es genügt nicht Mitarbeitern vorzugeben, „sensible Daten schützen zu müssen". Sie müssen auch verstehen, was diese Vorgabe bedeutet. Dabei bietet es sich an, auf Führungsebene leicht verständliche Kategorien zu definieren, je nachdem, welche Art von Daten im Unternehmen anfallen. Die Mitarbeiter sollten diese Kategorien kennen und verstehen, wie sie mit jeweils darunter fallenden Daten umgehen müssen.

Das bedeutet:

- Implementieren Sie formelle Datenschutzrichtlinien, schulen Sie Ihre Mitarbeiter diese zu kennen und zu befolgen.
- Führen Sie periodisch Informationssicherheits-Audits durch.

- Überprüfen Sie regelmäßig die Datenschutzrichtlinien Ihres Unternehmens und stellen Sie sicher, dass diese auch neue Formen der (elektronischen) Kommunikation abdecken.

Mitarbeiter vor sich selbst schützen

Vertrauen ist die Grundvoraussetzung jeder Geschäftsbeziehung. Wir vertrauen auf Kollegen, Vorgesetzte und Führungskräfte, dass sie uns bei der Erreichung unserer Ziele unterstützen. Die schlichte Wahrheit ist allerdings, dass Menschen Fehler machen - vor allem in Bereichen, die ihnen fremd sind. Deshalb ist es notwendig, Mitarbeiter dabei zu unterstützen das Thema Informationssicherheit für sich zu priorisieren und im Arbeitsalltag einfach umzusetzen.

Das bedeutet:

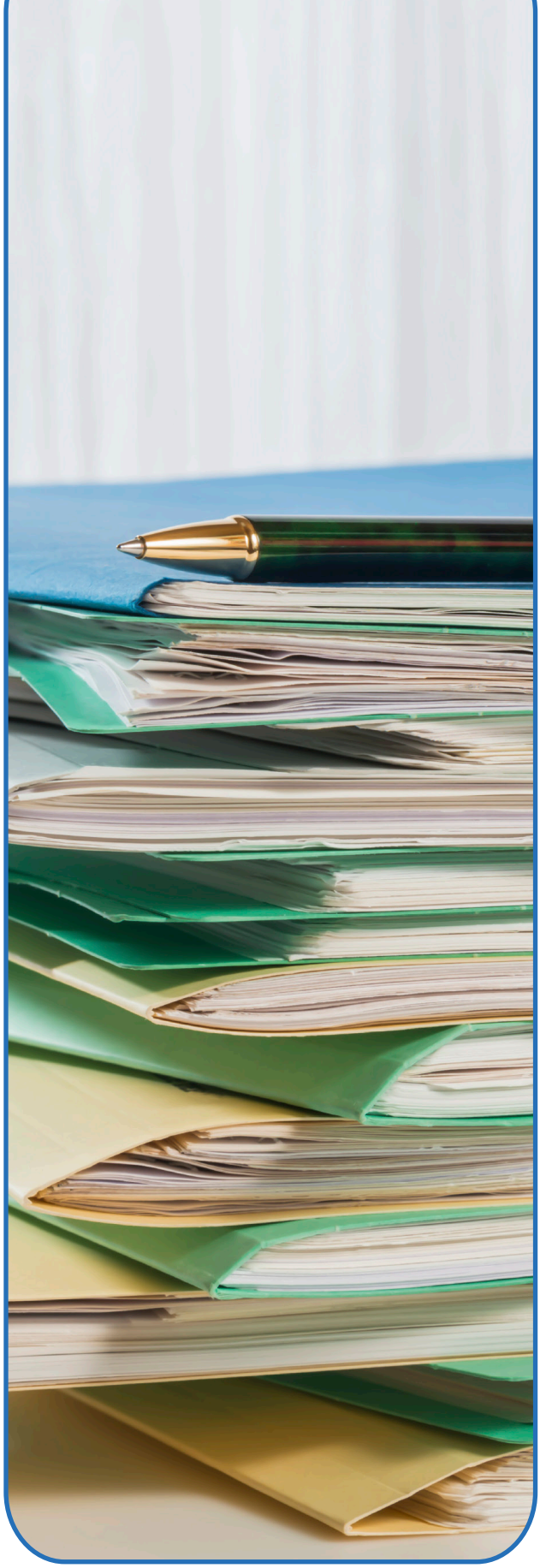
- Mit gutem Beispiel vorangehen: Wenn die Führungsebene nach außen demonstriert, dass Informationssicherheit wichtig ist, werden die Mitarbeiter dem Vorbild folgen. Wenn sich aber Führungskräfte selbst über Richtlinien hinwegsetzen, werden auch Mitarbeiter geneigt sein, diese nicht ernst zu nehmen.
- Vertrauliche Informationen im Papierkorb zu entsorgen ist genauso riskant, wie sie im Drucker oder auf dem Schreibtisch zu lassen. Die Vorgabe, einfach jedes Dokument sicher aufzubewahren und zu vernichten eliminiert die Entscheidung zwischen Datenmülltonne und Papierkorb. Ein professioneller Aktenvernichtungsdienstleister sorgt dafür, dass auch der sensible Papier-müll recycelt wird.
- Vernichten oder sichern: Implementieren Sie eine Clean-Desk-Policy, so dass Mitarbeiter am Ende des Tages ihre Papierunterlagen entweder wegschließen oder vernichten müssen.
- Ausdrucke sollten einen Sicherheitscode erfordern, so dass vertrauliche Informatio-nen nicht für jeden einsehbar im Drucker vorzufinden sind.
- Präsentationsmaterialien sollten nicht in Konferenzräumen verbleiben. Es empfiehlt sich, Whiteboards und FlipCharts abzufotografieren und das Bildmaterial auf einem sicheren Server zu speichern.
- Halten Sie Mitarbeiter, die im Home Office arbeiten, dazu an, auf Dokumente über sicheren VPN Zugang zuzugreifen, anstatt sie auszudrucken.
- Stellen Sie sicher, dass alle Diensthandys für den Fall des Verlustes oder Diebstahls Passwortgeschützt und die Daten verschlüsselt sind.
- Begrenzen Sie die Anzahl gemeinsamer Online-Accounts mehrerer Mitarbeiter. Ein bekanntes, einheitliches Passwort erhöht das Risiko für das Unternehmen, vor allem, wenn Mitarbeiter den Betrieb verlassen.

Mehr Sicherheit durch Vernichtung

Abschließbare Lagerräume und Aktenschränke können zwar für einen gewissen Zeitraum die Sicherheit vertraulicher Unterlagen oder ungenutzter Festplatten gewährleisten. Die einzige Möglichkeit Informationssicherheit hundertprozentig sicherzustellen ist jedoch, nicht mehr genutzte Papierunterlagen und elektronische Datenträger zu vernichten.

Das bedeutet:

- Führen Sie spezielle, abschließbare Container an Stelle von Papierkörben ein, um vertrauliche Dokumente zu entsorgen.
- Denken Sie an Festplatten auf Computern und Kopierern. Festplatten zu löschen bedeutet nicht, dass die Daten endgültig vernichtet wurden – das kann nur die physische Zerstörung von Festplatten sicherstellen.
- Führen Sie regelmäßige Aufräumaktionen in Ihren Lagerräumen durch und vermeiden Sie das Ansammeln ungenutzter Festplatten.
- Begrenzen Sie die Anzahl der Dokumente, die Mitarbeiter aus dem Büro entfernen können. Außerhalb der Büroräumlichkeiten lässt sich die Informationssicherheit nicht sicherstellen.



„Datenschutz wird als hinderlich empfunden“

Datenschutzbeauftragte helfen Unternehmen dabei, die für das Geschäft relevanten Datenschutzrichtlinien zu verstehen und umzusetzen. Geschäftsinhaber und Führungskräfte, die für die Sicherheit vertraulicher Daten zuständig sind, bekommen dadurch Unterstützung in einem sensiblen Bereich, in dem vor allem mittelständische Unternehmen noch große Defizite aufweisen. Shred-it sprach mit dem Datenschutzbeauftragten Jürgen Hartz darüber, woran die Informationssicherheit in vielen Unternehmen derzeit noch scheitert.

Welche Schwachstellen bei der Informationssicherheit sehen Sie am häufigsten, wenn Sie als externer Datenschutzbeauftragter in ein Unternehmen kommen?

Jürgen Hartz: Zunächst werden Datenschutz und IT-Sicherheit insbesondere in kleinen und mittelständischen Betrieben vielfach vermengt. Die Unternehmen sind bei der IT-Sicherheit oft schon gut aufgestellt oder bedienen sich qualifizierter Dienstleister. Das Thema Datenschutz, im Sinne des Schutzes der Persönlichkeitsrechte von Mitarbeitern, Kunden, Interessenten etc. wird dagegen so gar nicht wahrgenommen. Oft werden personenbezogene Daten gespeichert und weitergegeben, ohne dass man sich über derartige Vorgänge besondere Gedanken macht.

Eine weitere Schwachstelle ist immer noch die vertragliche Beziehung mit Dienstleistern. Egal ob Unternehmen als Auftraggeber oder Auftragnehmer auftreten, sehr oft fehlen die datenschutzrechtlichen Vereinbarungen zur Auftragsdatenverarbeitung im Sinne §11 BDSG[1]. Dazu zählen im Übrigen auch Dienstleister, die für die Aktenvernichtung zuständig sind – auch bei der Entsorgung handelt es sich um die Verarbeitung von Daten.

Was ist das Problem, wenn mit Dienstleistern nichts vertraglich vereinbart wurde?

Die Folge ist, dass weder Auflagen zur Datenverarbeitung noch technisch organisatorische Maßnahmen beim Dienstleister abgestimmt und festgelegt wurden. Dabei ist es die Aufgabe des Auftraggebers, seinen unternehmensinternen Schutzstandard zum Mindeststandard für die Auftragnehmer zu erheben. Denn was viele nicht wissen: Wer personenbezogene Daten erhebt ist auch noch für ihren Schutz verantwortlich, wenn er diese an Dritte weitergibt – bis zur endgültigen Vernichtung.

Welche sind die größten Irrtümer, denen Unternehmen und ihre Mitarbeiter bei der Aufbewahrung und Vernichtung vertraulicher Daten unterliegen?

Jürgen Hartz: Unternehmen, die keine externen Dienstleister beauftragen, entsorgen immer noch sehr oft Fehldrucke und überflüssiges Schriftgut im normalen Abfall. Platt ausgedrückt: Wenn ich ein Unternehmen ausspionieren wollte, würde ich nach Geschäftsschluss einfach mal in die Papiertonne draußen im Hof schauen. Da würde ich sicher schon einiges finden – und zwar säuberlich getrennt vom restlichen Müll, was mir die Entwendung noch einmal deutlich erleichtert.

Ein weiterer Klassiker: Es gibt zwar eine verschließbare Datenschutztonne für sensiblen Papiermüll, aber jeder im Unternehmen weiß, wo die Schlüssel liegen. In diesem Fall sind Datenschutz und Datensicherheit trotz entsprechender Vorkehrungen natürlich nicht gewährleistet.

Dann gibt es die Unternehmen, die zwar einen professionellen Dienstleister bestellen, aber diesen vorrangig nach wirtschaftlichen Gesichtspunkten auswählen. Wichtiger wäre allerdings darauf zu achten, dass der Dienstleister zertifiziert ist sensible Daten zu vernichten (zum Beispiel nach den Auflagen der DIN 66399) und die technischen Voraussetzungen erfüllt, vertrauliche Papiere und elektronische Datenträger ordnungsgemäß zu schreddern. Im Zweifel muss der Auftraggeber das persönlich kontrollieren, sonst verletzt er seine Sorgfaltspflicht. Die Beauftragung zur Vernichtung allein entlässt ihn nicht aus der Haftung. Das ist ein Vorteil der Vor-Ort-Vernichtung: Die Unterlagen werden vor der Haustür geschreddert, man kann also bei der Vernichtung zusehen.

Woran liegt es, dass insbesondere kleine und mittelständische Unternehmen beim Thema Datenschutz so schlecht aufgestellt sind?

Jürgen Hartz: Zum einen liegt das am intensiven Wettbewerb, in dem sich vor allem kleine Betriebe befinden. Das Thema Datenschutz wird dabei eher als hinderlich empfunden, da es selten direkten wirtschaftlichen Nutzen bringt. In vielen Fällen ist der interne Datenschutzbeauftragte eher alibimäßig bestellt und so intensiv in sein eigentliches Tagesgeschäft eingebunden, dass für Datenschutzthemen kaum Zeit bleibt. Oft bleiben dabei auch eine qualifizierte Grundausbildung und Fortbildung auf der Strecke.

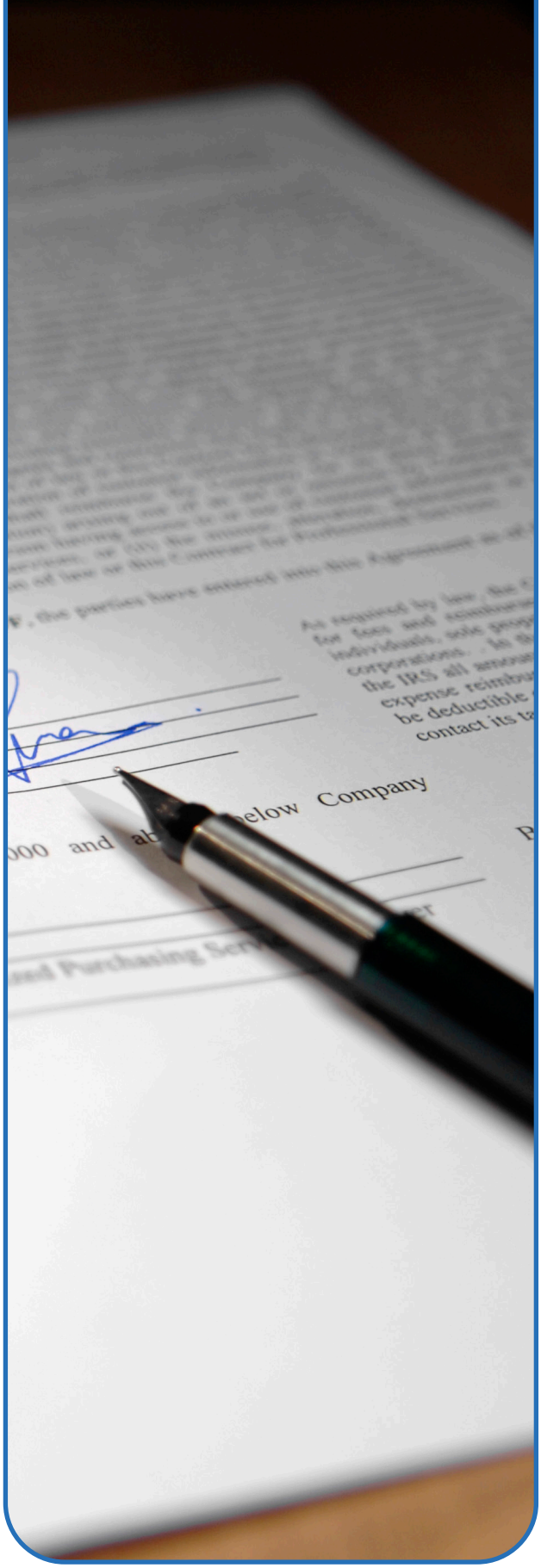
Zum anderen muss man feststellen: Es passiert vergleichsweise selten etwas. Entweder die Fahrlässigkeit im Umgang mit vertraulichen Daten hat keinen Verlust oder Diebstahl zur Folge – oder das Unternehmen erfährt nie, dass Daten abhandengekommen sind. Dass Defizite bei der Informationssicherheit ernsthafte Konsequenzen haben, ist relativ selten. Das scheint viele Unternehmen in Sicherheit zu wiegen, nichts ändern zu müssen.

Jürgen Hartz berät seit vielen Jahren Unternehmen in Fragen des Datenschutzes und ist bei verschiedenen mittelständischen Unternehmen als externer Datenschutzbeauftragter bestellt. Als stellvertretender Vorstandsvorsitzender im Berufsverband der Datenschutzbeauftragten e.V. (BvD e.V.) ist er in verschiedenen Verbandsgremien engagiert.

1 §11, BDSG: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.
(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. […]

Überblick über die Gesetzeslage in Deutschland

Informationssicherheit wird in Deutschland rechtlich aus verschiedenen Perspektiven betrachtet. Neben dem Bundesdatenschutzgesetz greifen unter anderem Abgabenordnung, Sozialgesetzbuch und Telemediengesetz das Thema Datenschutz auf. Es obliegt dem betrieblichen Datenschutzbeauftragten, sich mit der spezifischen Gesetzeslage für die jeweilige Branche und Geschäftstätigkeit auseinanderzusetzen. Allerdings haben 81% aller kleineren Betriebe keinen Datenschutzbeauftragten und auch die relevanten, rechtlichen Vorgaben sind weitestgehend unbekannt – so das Ergebnis der Security Tracker Umfrage 2015. Shred-it hilft durch den Paragraphen-Dschungel.



Das Bundesdatenschutzgesetz

In kaum einem anderen Land der Welt herrschen so strikte Datenschutzbestimmungen wie in Deutschland. Bereits 1970 wurde im Hessischen Landtag das weltweit erste Datenschutzgesetz verabschiedet. 1977 trat das Bundesdatenschutzgesetz (BDSG) in Kraft. Es gilt als das strengste Datenschutzgesetz in der Europäischen Union. Datenschutzbeauftragte im Unternehmen sollten vor allem diese Paragraphen kennen.

§4f BDSG: Beauftragter für den Datenschutz

„(1) Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. […]“

§9 BDSG: Angemessener Aufwand für Datensicherheit

Der Gesetzgeber verpflichtet datenverarbeitende Unternehmen, angemessene Schutzmaßnahmen für vertrauliche Informationen zu ergreifen – von der Aufbewahrung bis zur Vernichtung:

„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. […]"

§11 BDSG: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Es ist Aufgabe des Auftraggebers, die Sicherheit erhobener Daten auch bei Übertrag an einen Auftragnehmer zu gewährleisten. Wer personenbezogene Daten erhebt, ist auch noch für ihren Schutz verantwortlich, wenn er diese an Dritte weitergibt bzw. bis zur endgültigen Vernichtung.

„(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. […]"

§43 BDSG: Bußgeldvorschriften

Bei Verstoß gegen das Bundesdatenschutzgesetz werden Bußgelder in Höhe von bis zu 300.000 Euro fällig.

Abgabenordnung und Handelsgesetzbuch

Die Abgabenordnung und das Handelsgesetzbuch reglementieren in Deutschland die Aufbewahrung von Daten. Je nach Art der Unterlagen beträgt die Aufbewahrungsfrist zwi-schen drei und zehn Jahre:

§257 HGB: Aufbewahrung von Unterlagen

„Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:

1. *Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,*
2. *die empfangenen Handelsbriefe,*
3. *Wiedergaben der abgesandten Handelsbriefe,*
4. *Belege für Buchungen in den von ihm nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege)."*

§147 AO: Ordnungsvorschriften für die Aufbewahrung von Unterlagen

„(1) Die folgenden Unterlagen sind geordnet aufzubewahren:

1. Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
2. die empfangenen Handels- oder Geschäftsbriefe,

3. Wiedergaben der abgesandten Handels- oder Geschäftsbriefe,
4. Buchungsbelege,
4a. Unterlagen, die einer mit Mitteln der Datenverarbeitung abgegebenen Zollanmeldung nach Artikel 77 Abs. 1 in Verbindung mit Artikel 62 Abs. 2 Zollkodex beizufügen sind, sofern die Zollbehörden nach Artikel 77 Abs. 2 Satz 1 Zollkodex auf ihre Vorlage verzichtet oder sie nach erfolgter Vorlage zurückgegeben haben,
5. sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind.[…]"

Sozialgesetzbuch

Für gesetzliche Krankenkassen und Sozialdienstleister greifen darüber hinaus weitere gesetzliche Bestimmungen für den Datenschutz im Umgang mit Sozial- und Gesundheitsdaten, die im Sozialgesetzbuch festgelegt sind.

§§284-285 SGB 5: Sozialdaten bei den Krankenkassen und Personenbezogene Daten bei den Kassenärztlichen Vereinigungen

SGB 10: Sozialverwaltungsverfahren und Sozialdatenschutz

Telemediengesetz

Der Umgang mit elektronisch erhobenen Daten, beispielsweise über eine Unternehmenswebsite, ist zusätzlich im Telemediengesetz festgehalten.

§§11-15a TMG

Fazit

Der Shred-it State of the Industry Report fasst jährlich die neuesten Entwicklungen und die größten Herausforderungen deutscher Unternehmen im Bereich Informationssicherheit zusammen und soll diese dabei unterstützen, die betriebliche Informationssicherheit weiter zu verbessern.

Die Ergebnisse der Security Tracker Studie 2015 haben zwei Dinge gezeigt: Zum einen hat die Informationssicherheit in größeren Betrieben in Deutschland bereits einen hohen Stellenwert, sie haben mehrheitlich bereits Vorgaben für die Aufbewahrung und Vernichtung vertraulicher Informationen implementiert. In der Regel werden die Unternehmen dabei unterstützt von einem internen oder externen Datenschutzbeauftragten, der sie durch die komplexen rechtlichen Bestimmungen in Deutschland führt. Verbesserungspotential ist trotzdem noch gegeben: Im Idealfall sollte zukünftig jedes Unternehmen über Konsequenzen eines Datenverlustes Bescheid wissen und die notwendigen Maßnahmen ergreifen Datenverlust zu vermeiden - darunter auch eine sichere Datenvernichtung.

Zum anderen vernachlässigen viele kleine und mittlere Unternehmen immer noch das Thema Informationssicherheit. Der Mangel an Wissen und die fehlende Umsetzung von Maßnahmen zur Verbesserung der Informationssicherheit ist alarmierend, insbesondere angesichts des beträchtlichen Reputationsverlustes sowie der substantiellen finanziellen Schäden, die kleinen und mittleren Unternehmen durch einen Datenverlust entstehen können.

Mit Blick in die Zukunft können Experten für sichere Datenvernichtung sowie Datenschutzbeauftragte helfen, die allgemeine Aufmerksamkeit für das Thema Informationssicherheit weiter zu steigern und Unternehmen individuell dabei zu beraten, welche Maßnahmen ergriffen werden müssen, um die Informationssicherheit zu steigern. Wie in diesem Bericht aufgezeigt, können schon simple, kleine Schritte den Unterschied machen.