Informationssicherheit in deutschen Unternehmen 2016

2016 DEUTSCHLAND

Shred-it®

Inhalt

Überblick

Im März 2016 führte Shred-it zum zweiten Mal gemeinsam mit Ipsos MORI die Security Tracker Studie zur Informationssicherheit in deutschen Unternehmen durch. Befragt wurden rund 1.000 Inhaber von Betrieben mit weniger als 100 Mitarbeitern, sowie ungefähr 100 Führungskräfte aus Unternehmen mit mehr als 250 Mitarbeitern.

Überblick

Weiterhin erweisen sich Wissenslücken als größte Hürde für Informationssicherheit in kleinen und mittleren Betrieben. Große Unternehmen sind zwar deutlich besser informiert, aber auch hier wird das Thema Datenschutz nicht immer mit aller Konsequenz verfolgt. Kapitel zwei dieses Reports fasst diese und weitere Ergebnisse der diesjährigen Security Tracker Studie zusammen.

Die Ergebnisse auf einen Blick zeigt die Infografik in Kapitel drei.

Insbesondere kleine Betriebe geben häufig an, gar keine schützenswerten Daten zu besitzen. Mit dieser Fehleinschätzung räumt Kapitel vier auf. Während personenbezogene Daten per Bundesdatenschutzgesetz besonders geschützt werden müssen, gibt es noch viele weitere Dokumente, deren Verlust sich auch ohne rechtliche Konsequenzen geschäftsschädigend auswirken kann. Führungskräfte und Mitarbeiter sollten sich dessen bewusst sein – in Kapitel vier werden auch einige Best Practice Tipps vorgestellt, wie Informationssicherheit in der Praxis funktioniert.

In der Praxis nutzen bisher noch verhältnismäßig wenige Unternehmen einen externen Dienstleister für die Vernichtung vertraulicher Informationen. Viele vernichten und recyceln – ganz gleich ob Papier oder elektronische Datenträger – ihre Daten selbst. Kapitel fünf erläutert die Vor- und Nachteile der beiden Methoden.

Auch rechtlich ergaben sich im Jahr 2016 Neuigkeiten: Im April hat das Europäische Parlament die neue EU-Datenschutz-Grundverordnung (DSGVO) beschlossen, die ab 2018 für alle EU-Staaten bindend sein wird und den Datenschutz in Europa grundlegend neu regelt. Was sich dadurch ändert, lesen Sie in Kapitel sechs.

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: Aufklärungsbedarf und neue Herausforderungen

2016 führte Shred-it die Security Tracker Studie zur Informationssicherheit in Deutschland durch. Befragt wurden einerseits Inhaber von Betrieben mit weniger als 100 Mitarbeitern, andererseits Führungskräfte aus Unternehmen mit mehr als 250 Mitarbeitern. Auch 2016 zeigte sich: In kleinen und mittleren Betrieben sind Wissenslücken die größte Hürde auf dem Weg zu mehr Informationssicherheit. Große Unternehmen dagegen sind deutlich besser informiert, aber auch dort wird das Thema Datenschutz noch immer nicht mit letzter Konsequenz verfolgt.

Große Verunsicherung in kleinen und mittleren Betrieben

Datenschutz ist ohne Frage ein komplexes Feld. Insbesondere Unternehmen mit weniger als 100 Mitarbeitern sind damit häufig nicht nur bei der Umsetzung überfordert. Lediglich 38% der Befragten gaben an, die rechtlichen Rahmenbedingungen für die Aufbewahrung und Vernichtung vertraulicher Informationen genau zu kennen. Gleichzeitig bemängelten 64% der Unternehmen das fehlende Engagement der Regierung beim Schutz physischer und elektronischer Daten. Das liegt sicher an der NSA-Affäre 2015, die den Datenschutz in Deutschland in den Fokus rückte. Zugleich zeigt dieses Ergebnis aber auch einen Mangel an Aufklärung: Das Bundesdatenschutzgesetz gilt bereits seit seiner Einführung 1970 als eines der weitreichendsten und striktesten der Welt.

Neben rechtlichen Konsequenzen kann ein Datenleck gravierende Reputationsschäden und hohe finanzielle Verluste nach sich ziehen. 21% der Betriebe haben diese Folgen eines Datenverlustes bereits erlebt. Dass 50% der Befragten angeben, nicht im Besitz von Dokumenten zu sein, deren Verlust sich geschäftsschädigend auswirken könnte, offenbart einen weiteren, häufig fatalen Trugschluss. Denn neben personenbezogenen Daten wie Kundenadressen und Personalakten gehören zu solchen Dokumenten beispielsweise auch persönliche Korrespondenzen oder Aufzeichnungen geistigen Eigentums, die, falls sie in die falschen Hände geraten, zu großen Einbußen führen können.

Konkrete Richtlinien für die Aufbewahrung und Vernichtung vertraulicher Daten, sowohl auf Papier wie auf elektronischen Trägermedien, haben nur etwa die Hälfte der befragten Unternehmen. Hier zeigt sich immerhin eine erfreuliche Entwicklung: 2015 gaben sogar nur 26% der Betriebe an, über derlei Richtlinien zu verfügen.

Stand der Informationssicherheit in deutschen Unternehmen: Aufklärungsbedarf und neue Herausforderungen

Dabei lassen sich viele Maßnahmen zur Verbesserung der Informationssicherheit sehr einfach umsetzen, wie beispielsweise eine Clean-Desk-Policy (gibt es bisher formell nur in einem Fünftel der befragten Betriebe) oder die Beauftragung eines professionellen Dienstleisters für Aktenvernichtung (nutzen bisher nur 9% der Betriebe).

Mitarbeitern den Schutz sensibler Daten so leicht wie möglich zu machen, bleibt auch weiterhin der beste Weg, um Informationssicherheit zu gewährleisten. Denn mehr als die Hälfte der Betriebe mit weniger als 100 Mitarbeitern gaben an, dass ein Datenleck mit größter Wahrscheinlichkeit durch den Fehler eines Mitarbeiters entstehe. Trotzdem schulen nur knapp 30% der Betriebe ihre Mitarbeiter jährlich oder häufiger im Bereich Datenschutz.

Selten ziehen kleine und mittlere Betriebe den Rat eines Experten hinzu: Nur 24% der Befragten gaben an, 2016 einen Datenschutzbeauftragten in ihrem Unternehmen zu haben. Immerhin sind dies 5% mehr im Vergleich zur Vorjahresumfrage.

Neue Herausforderungen für große Unternehmen

Unternehmen mit mehr als 250 Mitarbeitern sind kleinen und mittleren Betrieben in vielen Belangen voraus. 95% haben einen internen oder externen Datenschutzbeauftragten nach BDSG §4f. Immerhin geben 64% an, sich selbst sehr gut mit den rechtlichen Bestimmungen für die Aufbewahrung und Vernichtung vertraulicher Daten auszukennen. In 96% der Unternehmen schlagen sich die rechtlichen Vorgaben in konkreten Richtlinien nieder. Inzwischen haben 71% der Unternehmen die Vorgabe eingeführt, dass alle Papierdokumente vor der Entsorgung geschreddert werden müssen. Damit nehmen sie ihren Mitarbeitern die Entscheidung ab, welche Daten sensibel sind und welche nicht - eine effektive Art und Weise, um Fehlentscheidungen vorzubeugen. Diese *„Shred-it All"* Regel empfiehlt auch Shred-it seinen Kunden.

Darüber hinaus stellen graduelle Veränderungen der Arbeitswelt Unternehmen allgemein vor weitere Herausforderungen im Bereich Datenschutz:

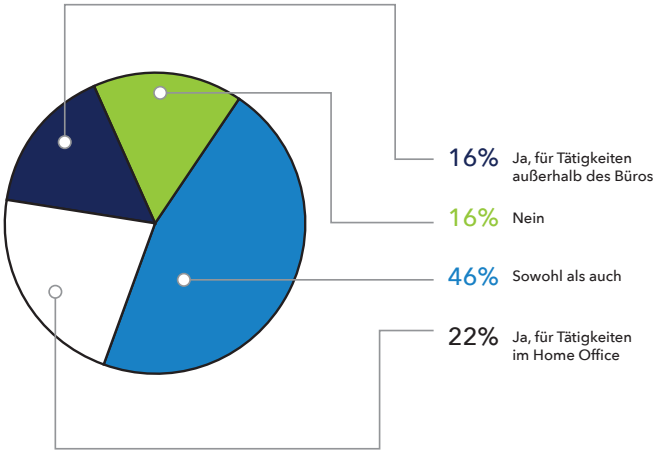
1. Neue Mobilität

Ein Drittel der Befragten gab an, dass bis zu 50% ihrer Belegschaft inzwischen die Möglichkeit nutzen, außerhalb des Büros oder im Home Office zu arbeiten.

Diese Veränderungen sollten auch in den Richtlinien für die Aufbewahrung und Vernichtung sensibler Daten berücksichtigt werden.

Die Security Tracker Studie zeigt, dass Unternehmen mit mehr als 250 Mitarbeitern bereits auf einem guten Weg sind:

Hat Ihre Organisation spezielle Richtlinien für die Aufbewahrung und Vernichtung vertraulicher Informationen für Tätigkeiten außerhalb des Büros beziehungsweise im Home Office?



2. Vom Papier zum Pixel:

Unter der Maxime der Papierreduzierung befinden sich viele Daten heute auf elektronischen Datenträgern wie Festplatten oder USB-Sticks. Auch bei diesen Speichermedien muss die sichere Aufbewahrung und Vernichtung gewährleistet werden. Das Löschen der Daten von den Trägern bedeutet in diesem Fall nicht, dass diese tatsächlich vollständig vom Speichermedium entfernt wurden. Deswegen ist es essentiell, dass elektronische Datenträger nicht nur professionell bereinigt, sondern auch physisch zerstört werden, wenn sie nicht mehr benötigt werden. Bisher nutzen nur 20% der Unternehmen mit mehr als 250 Mitarbeitern einen professionellen Dienstleister für die Vernichtung elektronischer Datenträger.

Stand der Informationssicherheit in deutschen Unternehmen: Aufklärungsbedarf und neue Herausforderungen

In 36% der Betriebe übernehmen die Datenbereinigung und Entsorgung Mitarbeiter des Unternehmens. Immerhin 6% der Befragten bestätigten, dass sie nicht mehr gebrauchte elektronische Datenträger auf unbestimmte Zeit einlagern – ein Vorgehen, das sich auf Dauer raum- und kostentechnisch schwierig gestalten dürfte.

Ob Papier oder elektronische Datenträger: 35% der befragten Unternehmen nutzen bereits einen externen Dienstleister für die Vernichtung sensibler Daten. 53% davon gaben an, dass diese Lösung am bequemsten sei und Zeit spare. 26% nannten Compliance-Gründe als ausschlaggebend für die Wahl eines externen Dienstleisters.

„Die Ergebnisse der Studie bestätigen, dass wir unseren Kunden weiterhin nicht nur mit unserem Vernichtungsservice helfen können, sondern ihnen auch durch ganzheitliche Beratung in Sachen Informationssicherheit zur Seite stehen", resümiert Peter Husseck, Vizepräsident von Shred-it für Deutschland und Österreich, die Ergebnisse der diesjährigen Security Tracker Studie.

Shred-it führt auf Anfrage unter anderem eine kostenlose Risikoanalyse im Unternehmen durch und berät bei der Einführung und Umsetzung von Datenschutzrichtlinien.

Über die Security Tracker Studie

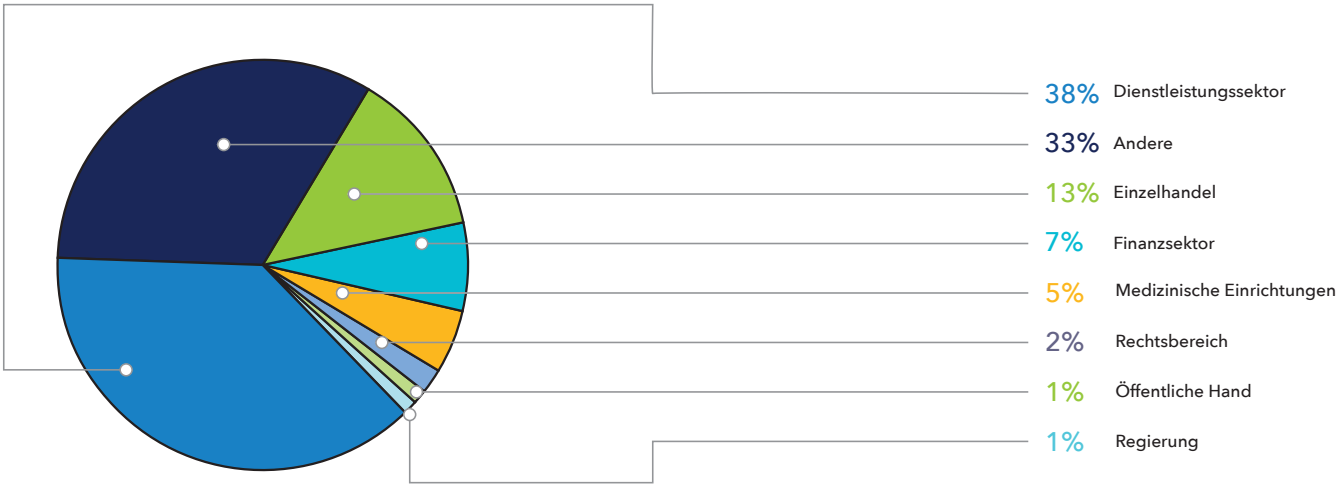
Im März 2016 führte das Markt- und Meinungsforschungsinstitut Ipsos MORI im Auftrag von Shred-it zum zweiten Mal seit 2015 die Security Tracker Studie auch in Deutschland durch. In einer quantitativen Online-Umfrage wurden 1.002 Inhaber von Betrieben mit weniger als 100 Mitarbeitern und 101 Führungskräfte aus Unternehmen mit mehr als 250 Mitarbeitern zu allen Belangen der Informationssicherheit in ihren Betrieben befragt.

Die Ergebnisse lassen nicht nur Rückschlüsse auf die Informationssicherheit in deutschen Unternehmen zu, sondern geben auch größen- und branchenspezifische Einblicke.

In Nordamerika und dem Vereinigten Königreich wurde die Studie 2016 bereits zum sechsten Mal durchgeführt und hat sich mittlerweile zu einem wichtigen Stimmungsbarometer in Sachen Informationssicherheit entwickelt.

Ipsos MORI ist das drittgrößte Unternehmen im Bereich Markt- und Meinungsforschung, mit 87 Länder-Vertretungen und 16.000 Mitarbeitern weltweit.

Befragte nach Branchen (n=1.103)



Security Tracker: Infografik

Was sind eigentlich schützenswerte Daten?

Auch 2016 bestritten noch 38% aller Betriebe mit weniger als 100 Mitarbeitern, dass sie im Besitz von Dokumenten seien, deren Verlust geschäftsschädigend wirken würde. In den meisten Fällen dürfte es sich hierbei um eine Fehleinschätzung handeln – mit potenziell teuren Folgen. Die untenstehende Aufstellung zeigt, dass eine ganze Reihe von Informationen besonderen Schutz genießen sollten – von der Aufbewahrung bis zur Vernichtung.

Was sind eigentlich schützenswerte Daten?

Personenbezogene Daten

Vom kleinen Handwerksbetrieb bis zum multinationalen Konzern: Personenbezogene Daten gemäß § 3 Abs. 9 BDSG fallen in jedem Betrieb an. Bei Datenverlust drohen gemäß § 42 BDSG Bußgelder in Höhe von bis zu 300.000 Euro, sowie immense Reputationsschäden und der Verlust von Kunden. 57% aller Unternehmen mit mehr als 250 Mitarbeitern hatten bereits mit Folgen eines Datenlecks zu kämpfen, so das Ergebnis der Security Tracker Studie 2016.

Grundsätzlich gilt: Alle Informationen, über die irgendwie ein Personenbezug hergestellt werden kann, fallen auch unter den Begriff der personenbezogenen Daten. Klar zuzuordnen sind der Name, die Telefonnummer sowie Kreditkarten- oder Personalnummern. Aber auch Kontodaten, Kfz-Kennzeichen, das Aussehen, die Kundennummer oder die Anschrift zählen zu den personenbezogenen Daten.

Geistiges Eigentum

Informationssicherheit bedeutet auch Schutz von Produktinformationen vor Wettbewerbsspionage. So können Konstruktionspläne für neue Produkte, die Planung des nächsten Messeauftritts, aktuelle Forschungsergebnisse oder die Resultate der internen Testabteilung für Mitbewerber von hohem Interesse sein und sollten nicht in falsche Hände gelangen. Ihr Verlust ist nicht strafbar, aber dennoch unmittelbar geschäftsschädigend.

Geschäftsbezogene Daten

Auch andere Informationen sind für den Wettbewerb interessant: Geschäftsabschlüsse, Verträge oder Aufzeichnungen über Einkaufskonditionen bei Zulieferern können, wenn sie an die Öffentlichkeit geraten, nicht nur für Nachteile in Verhandlungen sorgen, sondern im schlimmsten Fall zu Unruhen in einer ganzen Branche führen.

Vertraglich festgelegter Schutzbedarf

Andere Informationen ohne direkten Personenbezug können einen erhöhten Schutzbedarf haben, wenn sie Gegenstand eines Vertrages mit Kunden sind. Werden zum Beispiel Beratungsleistungen für einen Kunden erbracht, muss die Strategiepräsentation des Kunden ebenfalls besonders geschützt werden. Gelangen diese Informationen an die Öffentlichkeit oder in die falschen Hände, hat das möglicherweise für beide Vertragspartner verheerende Folgen. Informationssicherheit bedeutet an dieser Stelle auch, das Vertrauen des Kunden und damit den Auftrag zu behalten und somit eine langfristig gute Zusammenarbeit sicherzustellen.

Fehleinschätzungen vorbeugen

Wie geht man im Unternehmen nun am besten mit der Vielzahl an schützenswerten Informationen um? Hier ein paar Best-Practice-Tipps:

- Es genügt nicht, Mitarbeitern vorzugeben, „sensible Daten schützen zu müssen". Mitarbeiter müssen auch genau verstehen, was diese Vorgabe bedeutet und wie sie im Alltag auszuüben ist.
- Implementieren Sie formelle Datenschutzrichtlinien und schulen Sie Ihre Mitarbeiter, damit sie diese kennen und befolgen.
- Die Vorgabe, einfach jedes Dokument sicher aufzubewahren und zu vernichten, eliminiert die Entscheidung zwischen Datenmülltonne und Papierkorb und beugt teuren Fehleinschätzungen der Mitarbeiter vor.
- Alternativ sollten auf Führungsebene leicht verständliche Kategorien definiert werden, 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.
- Überprüfen Sie regelmäßig die Datenschutzrichtlinien Ihres Unternehmens und stellen Sie sicher, dass diese auch neue Formen der (elektronischen) Kommunikation abdecken.

Expertenhilfe in Anspruch nehmen

Insbesondere kleinere Betriebe, die sich mit dem komplexen Thema Datenschutz schwer tun und unsicher sind, wie sie Informationssicherheit gewährleisten können, sollten auf den Rat von Experten wie Datenschutzbeauftragten, Rechtsbeiständen oder anderen Fachdienstleistern setzen.

Interne oder externe Datenvernichtung – eine Pro- und Kontra-Liste

Die Security Tracker Studie 2016 hat gezeigt, dass nur rund die Hälfte (56%) der großen Unternehmen auf externe Datenvernichtungs-Dienstleistungen zurückgreift. Ganze 86% der kleineren Unternehmen geben an, dass sie nicht mit einem professionellen Dienstleister für Aktenvernichtung arbeiten. Shred-it präsentiert im Folgenden die Vor- und Nachteile der internen und professionellen Datenvernichtung und deckt dabei einige Missverständnisse auf.

Interne oder externe Datenvernichtung – eine Pro- und Kontra-Liste

Interne Datenvernichtung

Vorteile

- Keine laufenden Kosten durch einmalige Anschaffung eines Schredders.
- Dokumente können direkt im Unternehmen vernichtet werden, ohne das Gelände zu verlassen.
- Hauseigene Mitarbeiter können die Datenvernichtung direkt vornehmen, ohne externe Dienstleister zu beauftragen.

Nachteile

- Übliche Streifen-Schredder sind nicht zwangsläufig sicher, da Dokumente rekonstruiert werden können.
- Beim Thema Datenschutz sollte man sich nicht auf seine Mitarbeiter verlassen: Die Security Tracker Studie 2016 hat gezeigt, dass 40 Prozent der großen und 52 Prozent der kleineren Unternehmen ein Datenleck bestätigen, das auf Mitarbeiter-Fehlverhalten oder unbeabsichtigten Datenverlust zurückzuführen ist.
- Die interne Datenvernichtung überlässt die finale Entscheidung, ob und wann ein Dokument schützenswert ist, dem Mitarbeiter. 46 Prozent der Unternehmen attestieren jedoch, ihre Mitarbeiter überhaupt nicht in Datenschutz-Maßnahmen zu schulen.
- Interne Datenvernichtung ist zeitintensiv für die hauseigenen Mitarbeiter und somit ineffizient. Ferner sind unerwartete Instandhaltungsmaßnahmen und Reparaturkosten der Schred der keine Seltenheit.

Fazit

Die Nutzung eines externen Dienstleisters kann folglich dabei helfen, Risiken zu minimieren und den Verlust von schützenswerten Daten zu verhindern.

Professionelle Datenvernichtung

Vorteile

- Professionell geschreddertes Material lässt sich aufgrund von Beschaffenheit und Größe nicht rekonstruieren.
- Durch Vor-Ort-Datenvernichtung verlässt kein Dokument oder Datenträger das Unternehmen, ohne vorher fachgerecht geschreddert worden zu sein. Ein potenzieller Verlust oder Diebstahl der Daten während des Transports oder der Entsorgung ist somit ausgeschlossen. Der Dienstleister gewährleistet, dass alle schützenswerten Informationen sicher vernichtet werden.
- Externe Dienstleister prüfen und zertifizieren all ihre Mitarbeiter. Um für mehr Kontinuität im Kundenkontakt zu sorgen, teilen externe Dienstleister jedem Kunden einen eigenen Mitarbeiter zu.
- Durch eine *„Shred-it All"* Richtlinie müssen Mitarbeiter nicht mehr entscheiden, wann und ob ein Dokument schützenswert ist oder nicht. Ein externer Dienstleister gewährleistet und dokumentiert die professionelle Vernichtung aller Informationen und schont gleichermaßen die Mitarbeiter-Ressourcen.
- Dienstleistungsunternehmen wie Shred-it bieten umfassende Beratungsangebote und unterstützen Unternehmen bei der Konzeption und Anwendung von Informationssicherheits-Richtlinien.
- Unternehmen können ihren Kunden die professionelle und sichere Verarbeitung ihrer Daten garantieren, indem sie externe Datenvernichtungs-Dienstleister beauftragen.

Wahrgenommene Nachteile

- Auf den ersten Blick schafft die Nutzung eines externen Dienstleisters höhere Betriebskosten gegenüber einer internen Datenvernichtung. Zugleich schont sie aber Mitarbeiter-Ressourcen und wertvolle Zeit. Die Betriebskosten einer professionellen Datenvernichtung wirken verschwindend gering, wenn im Falle eines Datenverlusts gesetzlich vereinbarte Strafgebühren von bis zu 300.000 Euro drohen und gravierende Reputations- und finanzielle Schäden sehr wahrscheinlich sind.

Fazit

Vor dem Hintergrund der strengen Datenschutzauflagen, denen Unternehmen im Umgang mit ihren Mitarbeitern und Kunden verpflichtet sind, bieten externe Dienstleister überzeugende Vorteile für eine Zusammenarbeit. Interne Datenvernichtung wird durch menschliches Fehlverhalten und resultierende Datenlecks zum permanenten internen Sicherheitsrisiko des Unternehmens. Dieses Risiko lässt sich durch die Nutzung eines professionellen Dienstleisters minimieren.

Experteninterview

„Über Datenschutzrecht machen sich Unternehmen viel zu wenig Gedanken“

Das Datenschutzrecht macht Unternehmen klare Vorgaben, wie sie mit sensiblen Daten ihrer Mitarbeiter und Kunden umzugehen haben. Mangelndes Bewusstsein und Wissen kann gravierende Folgen für die Reputation eines Unternehmens haben und hohe Bußgelder nach sich ziehen. Shred-it sprach mit Dr. Philip Kempermann, Partner bei der Wirtschaftskanzlei Heuking Kühn Lüer Wojtek, über die rechtlichen Spitzfindigkeiten im Datenschutz und darüber, warum Unternehmen durch externe Beratung und Dienstleistung nicht nur im rechtlichen Sinne profitieren.

Welche sind die größten Irrtümer, denen Unternehmen und ihre Mitarbeiter beim Thema Datenschutz unterliegen?

Kempermann: Der größte Irrtum liegt meines Erachtens im mangelnden Bewusstsein der Unternehmen. Besonders kleine Unternehmen wissen gar nicht, welche Daten schutzbedürftig sind – das sind nicht immer nur personenbezogene Daten.

Um ein veranschaulichendes Beispiel zu geben: Wenn ich als Dienstleister für meinen Kunden im Entwicklungsbereich tätig bin, muss ich doch sehr darauf achten, wie ich meine Daten – sei es in IT- oder Papierform – zu sichern habe, um die Forschungs- und Entwicklungsergebnisse meines Kunden zu schützen. Dies gilt selbstverständlich für alle Unternehmen. Gerade in kleineren und noch nicht ganz so spezialisierten Unternehmen fehlen oftmals klare interne Richtlinien, wie mit Daten umzugehen ist.

Demensprechend müsste wesentlich mehr Augenmerk auf die Mitarbeiterschulung gelegt werden, damit Sicherheitsmaßnahmen eingehalten werden. Ein weiteres klassisches Beispiel aus der Praxis ist die Bewerbungsmappe, die ohne böse Absicht nach Feierabend auf dem Schreibtisch liegen gelassen wird. In diesem Zusammenhang ist eine Clean-Desk-Policy, wie sie in vielen Unternehmen schon gelebt wird, sehr empfehlenswert, um sicherzustellen, dass vertrauliche Informationen weggeschlossen werden.

Wann ist ein betrieblicher Datenschutzbeauftragter zu bestellen und welche Unternehmen sind betroffen?

Kempermann: Sobald in einem Unternehmen mehr als neun Mitarbeiter regelmäßig personenbezogene Daten mit IT-Systemen verarbeiten, ist ein Datenschutzbeauftragter zu bestellen. Daher betrifft diese Regel selbst kleine Unternehmen, die dies allerdings oft gar nicht realisieren. Denn kaum ein Unternehmen arbeitet heute noch ohne ein Mailprogramm oder ein Personaltool, das personenbezogene Daten verarbeitet.

Daher müssen sich selbst kleine Unternehmen über die Notwendigkeit eines externen oder internen Datenschutzbeauftragten informieren und sich der Konsequenzen und Tragweite des Datenschutzrechts bewusst sein.

Welche Konsequenzen drohen Unternehmen beim Verlust von sensiblen Daten?

Kempermann: Neben dem finanziellen Schaden, der durch einen Datenverlust entsteht, ist in erster Linie der Reputationsschaden und Vertrauensverlust für ein Unternehmen gravierend. Laut § 42a des Bundesdatenschutzgesetzes[1] besteht in bestimmten Fällen die Notwendigkeit, einen Verlust von personenbezogenen Daten der Aufsichtsbehörde sowie den Betroffenen zu melden. Der Gang an die Öffentlichkeit und der resultierende Reputationsschaden sind daher eine nicht zu unterschätzende Konsequenz.

Neben dem Reputationsschaden drohen aber auch erhebliche finanzielle Strafen. Im Datenschutzrecht gibt es zwei Bußgeldrahmen. Mit bis zu 50.000 Euro pro Einzelfall werden Verstöße geahndet, wenn zum Beispiel Unternehmen im Fall einer Auftragsdatenverarbeitung keine schriftliche Vereinbarung treffen, die auch technische und organisatorische Maßnahmen enthalten muss.

Schwerwiegende Verletzungen von Datenschutzvorschriften werden aktuell mit bis zu 300.000 Euro Bußgeld pro Einzelfall belegt. Ein Transfer von personenbezogenen Daten ins Ausland, ohne Gewährleistung eines adäquaten lokalen Sicherheitsniveaus, ist ein exemplarischer Fall. Die unzulässige Verarbeitung von Daten zur Überwachung der Mitarbeiter wäre ein weiterer Aspekt, der eine schwerwiegende Verletzung der Datenschutzvorschriften darstellt.

Experteninterview

„Über Datenschutzrecht machen sich Unternehmen viel zu wenig Gedanken“

Die Bußgelder werden allerdings mit der neuen Datenschutzgrundverordnung, die am 24.05.2018 EU-weit verbindlich wird, potenziell weiter steigen. Der Bußgeldrahmen umfasst dann bis zu 20 Millionen Euro oder vier Prozent des Unternehmensumsatzes. Das zeigt, dass das Datenschutzrecht und eine Sensibilisierung für das Thema auch in den kommenden Jahren eine steigende Brisanz aufweisen werden.

Ist die Beauftragung eines externen Dienstleisters zur Akten- und Datenvernichtung ratsam?

Kempermann: Ja, die Beauftragung eines externen Dienstleisters bietet mehrere Vorteile. Als Unternehmen werde ich selbst gar nicht datenschutzkonform Datenträger und große Datenmengen vernichten können. Dies wird nur ein externer technischer Dienstleister in einem vernünftigen, effizienten Maß gewährleisten können. Da wir noch weit vom papierlosen Büro entfernt sind, stellt sich auch die Frage, inwieweit ich mich als Unternehmen damit befassen möchte, da ich diese Tätigkeit an einen externen Dienstleister viel sicherer und ressourcenschonender, also effizienter, auslagern kann.

Ein weiterer wichtiger Punkt ist die professionelle Betreuung. Durch einen externen Dienstleister habe ich jemanden an meiner Seite, der rechtliche Beratung in den komplexen Themen des Datenschutzrechts gewährleistet und zugleich die Vermeidung potenzieller Reputationsschäden sicherstellt.

Dr. Philip Kempermann ist Experte für Datenschutz- und IT-Recht und Partner bei der Kanzlei Heuking Kühn Lüer Wojtek. Er begleitet internationale Unternehmen bei IT-Projektverträgen, IT-Outsourcing und Einführungen von IT-Projekten mit direkter mitarbeiterrelevanter Bedeutung.

1 §42a, BDSG: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle […] fest, dass bei ihr gespeicherte

1 besondere Arten personenbezogener Daten (§3 Absatz 9),[…] unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. […]

Aktuelle Gesetzesänderungen

Nach der Rechtsprechung des Bundesverfassungsgerichts ist Datenschutz ein Grundrecht. In Deutschland wird auf Bundesebene der Datenschutz für die Bundesbehörden und den privaten Bereich durch das Bundesdatenschutzgesetz (BDSG) geregelt. Europaweit ist die Rechtsgrundlage die EU-Datenschutz-Grundverordnung (DSGVO). Diese wurde am 14. April 2016 vom EU-Parlament beschlossen und bildet die Grundlage für die Vereinheitlichung der Regeln für die Verarbeitung von personenbezogenen Daten.

Aktuelle Gesetzesänderungen

Die automatisierte Datenverarbeitung ist ein unverzichtbarer Bestandteil des wirtschaftlichen und gesellschaftlichen Lebens geworden. Sie bietet fast unbegrenzte Möglichkeiten, Informationen zu speichern und zu kombinieren und erleichtert dadurch in vielerlei Hinsicht unseren Alltag. Zugleich birgt sie aber auch Gefahren für die Privatsphäre des Einzelnen, weil Staat und Wirtschaft – teilweise ohne Wissen des Betroffenen – auf immer mehr persönliche Daten zurückgreifen können.

Datenschutzgesetze sollen das Recht jedes Menschen bewahren, selbst entscheiden zu können, wem wann welche seiner persönlichen Daten zugänglich sind. Während das deutsche Bundesdatenschutzgesetz dieses Recht bereits seit 1970 streng schützt, soll es nun auch europaweit institutionalisiert werden.

Vereinheitlichung auf europäischer Ebene

Nach fast vierjähriger Debatte zwischen dem Europäischen Rat, dem Europäischen Parlament und der Europäischen Kommission wurde am 14. April 2016 die neue EU-Datenschutz-Grundverordnung vom Europäischen Parlament verabschiedet. 2018 wird sie in Kraft treten. „Bürger und Unternehmen werden sich auf klare Vorschriften berufen können, die für das digitale Zeitalter taugen, einen starken Schutz garantieren und gleichzeitig im europäischen digitalen Binnenmarkt neue Möglichkeiten eröffnen und Innovationen fördern", erklärt Věra Jourová, EU-Kommissarin für Justiz, Verbraucher und Gleichstellung. „Gleichzeitig werden harmonisierte Datenschutzvorschriften für Polizei- und Strafverfolgungsbehörden die Zusammenarbeit unter den Mitgliedstaaten auf der Grundlage gegenseitigen Vertrauens erleichtern und so einen Beitrag zur europäischen Sicherheitsagenda leisten."

Neue Vorschriften

Die neuen Vorschriften sind weitreichend, wie etwa die Stärkung der Betroffenenrechte, das Recht auf Vergessenwerden, das Recht auf Datenübertragbarkeit, ein einfacheres Informationsrecht, die Stärkung des Datenschutzrechts, sowie eine neueingeführte Meldepflicht für Datenlecks. Des Weiteren sind künftig bei Verletzungen des Datenschutzrechts empfindliche Geldstrafen von bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes des Unternehmens vorgesehen (Art. 79 f. EU-DSGVO). Auch die Datenschutzbehörden werden durch die neuen Vorschriften gestärkt (Kapitel VI, Art. 46 ff. EU-DSGVO).

Die Vorschriften werden auch Einfluss auf die deutsche Gesetzgebung haben. Im für den Datenschutz zuständigen Bundesministerium des Innern arbeitet man bereits an der Implementierung. „Ziel ist die volle Umsetzung der Grundverordnung zum Zeitpunkt ihrer Anwendbarkeit ab Mitte 2018 im öffentlichen und privaten Bereich", so Bundesinnenminister Thomas de Maizière.

Fazit

Die Ergebnisse des State of the Industry Reports 2016 haben gezeigt, dass deutsche Unternehmen sich komplexen Datenschutz-Bestimmungen und einem wandelnden Umfeld stellen müssen.

Elektronische Datenverarbeitung und -sicherung sowie flexible Arbeitsmodelle sind in modernen Unternehmen nicht mehr wegzudenken – also müssen Firmen auch sicherstellen, dass ihre Datenschutzrichtlinien neben klassischen Papierformaten auch elektronische Datenträger berücksichtigen. Dabei dürfen Unternehmen die aktuelle Gesetzeslage nicht aus den Augen verlieren und müssen sicherstellen, dass sie ihre Mitarbeiter dementsprechend schulen.

Trotz dieser Entwicklungen und der Notwendigkeit hoher Informationssicherheits-Standards hat die Studie gezeigt, dass große Wissenslücken bei deutschen Unternehmen bestehen. Besonders kleine Betriebe müssen sich der Bedeutung der Informationssicherheit in ihrem Unternehmen bewusst werden. Obwohl größere Unternehmen allgemein besser über Informationssicherheit informiert sind, mangelt es auch bei ihnen oftmals an einer konsequenten Umsetzung von notwendigen Datenschutzmaßnahmen.

Unternehmen müssen daher Informationssicherheit als Priorität behandeln, um die Sicherheit ihrer Informationen und Kundendaten gewährleisten zu können.

- Welche Daten sind überhaupt schützenswert?
- Was passiert, wenn Daten verloren gehen?
- Wo liegen die Hauptrisiken für einen Datenverlust im Unternehmen?
- Welche Maßnahmen kann man ergreifen, um das Risiko eines Datenverlustes zu verringern?
- Wie sind die rechtlichen Rahmenbedingungen für Datenschutz in Unternehmen?

Betriebsinhaber und Datenschutzverantwortliche sollten die Antworten auf diese Fragen kennen – oder sich Rat von Experten wie Datenschutzbeauftragten oder Fachdienstleistern holen, die sich im komplexen Feld der Informationssicherheit auskennen. Sie können sowohl Risiken identifizieren als auch konkrete Maßnahmen für mehr Informationssicherheit im Unternehmen empfehlen und bei der Umsetzung unterstützen.

Mit ihrem Expertenwissen können externe Dienstleister Unternehmen dabei unterstützen, die komplexen Datenschutzstandards und die Gesetzeslage zu verstehen und angemessene Lösungen für bestehende Risikostellen zu entwickeln. Denn Verstöße können in diesem Zusammenhang zu substantiellen finanziellen Schäden und beträchtlichem Reputationsverlust führen.

Der Shred-it State of the Industry Report hat die neuesten Entwicklungen und Herausforderungen für deutsche Unternehmen im Bereich Informationssicherheit zusammengefasst. Damit möchte Shred-it Unternehmen helfen, auf dem neuesten Stand der Informationssicherheitsbestimmungen und Gesetzgebungen zu bleiben und schlussendlich finanzielle Strafen und Reputationsschäden zu minimieren.

Wenn Sie mehr erfahren möchten, wie Sie die Informationssicherheit in Ihrem Unternehmen verbessern können, besuchen Sie: **shredit.de/mediencenter**.

facebook.com/shredit

linkedin.com/company/shred-it

@Shredit