techconsult
The IT Market Analysts

Hewlett Packard Enterprise

Studie

„Spurlose Datensicherheit noch nicht erreicht“

Eine Studie zur Datensicherheit und sicheren Datenvernichtung in deutschen Unternehmen ab 250 Mitarbeitern

Inhalt

Copyright

Disclaimer

Vorwort

Ab 2018 wird die neue EU-Datenschutzverordnung in Kraft treten. Diese ist für alle Unternehmen innerhalb der EU verpflichtend und kann bei Nichtbeachtung zu drastischen Strafen führen.

Jedes Unternehmen, welches personenbezogene und sensible Daten in irgendeiner Form speichert oder weiterverarbeitet muss dafür Sorge tragen, dass die datenschutzrechtlichen Bestimmungen genau eingehalten werden. Gleichzeitig sind Unternehmen auch dafür verantwortlich, dass geistiges Eigentum, wie Forschungs- und Entwicklungsergebnisse, nicht in die Hände Dritter gelangt.

Wesentliche Treiber für die Verschärfung der Datenschutzmaßnahmen sind die zunehmende Digitalisierung und Vernetzung sowie die stärkere Nutzung von Cloud Lösungen.

Nicht nur die Datenaufbewahrung, auch die professionelle Löschung und sichere Außerbetriebnahme von Datenträgern sind für jedes Unternehmen und jede Behörde gesetzlich vorgeschrieben. Dadurch ist zu gewährleisten, dass Daten nicht in falsche Hände geraten. Für all diejenigen, die es auf personenbezogene oder geschäftliche Daten abgesehen haben, sind elektronische Geräte eine perfekte Zielscheibe. Unternehmen müssen Maßnahmen zur sicheren Datenlöschung ergreifen und ausgediente elektronische Datenträger vor unberechtigten Zugriffen schützen.

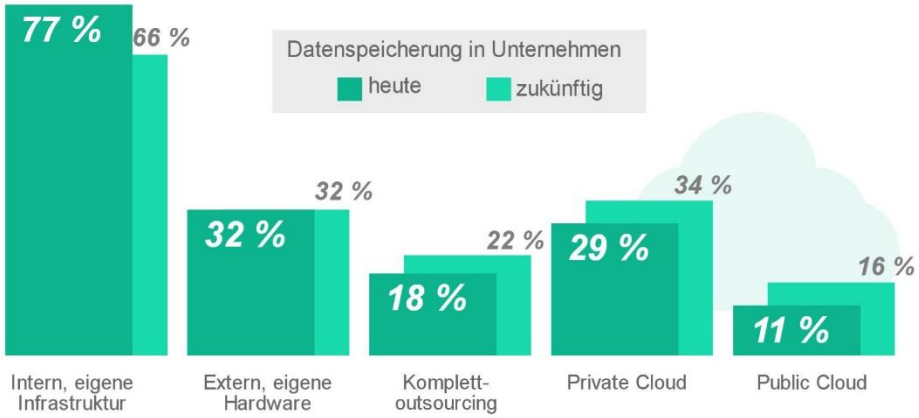
Der Fokus dieser Studie liegt in den Herausforderungen rund um den Datenschutz, vor denen die Unternehmen heute und zukünftig stehen. Die Studie zeigt auf, welche Relevanz der Datenschutz in Unternehmen hat, wo die Verantwortlichkeiten liegen, welche Schäden Datenlecks und verlorene Datenträger verursachen und wie die Außerbetriebnahme und Entsorgung ausgedienter Datenträger erfolgt.

Speicherumgebung

Unternehmen nutzen verschiedene Möglichkeiten zur Datenspeicherung. Die Mehrheit, 77 Prozent der befragten Unternehmen, hat ihre Daten innerhalb der unternehmenseigenen Infrastruktur gespeichert. Aus Sicht der Befragten ist dies nach wie vor die sicherste Speicherart im Hinblick auf Speicherort und Compliance-Anforderungen. Ihre unternehmenseigene Hardware an einen externen Dienstleister auszulagern, dazu haben sich 32 Prozent der Unternehmen entschieden.

Darüber hinaus verwendet schon jedes zweite Unternehmen zur Datenspeicherung eine Cloud-Lösung. Während 29 Prozent die aus ihrer Sicht sicherere Variante der Private Cloud präferieren, lagern derzeit 11 Prozent der Unternehmen ihre Daten in einer Public Cloud. 18 Prozent der Unternehmen haben ihre Speicherumgebung komplett ausgelagert.

In den nächsten zwei Jahren werden sich deutlich mehr Unternehmen für die Datenspeicherung in der Private Cloud oder Public Cloud entscheiden. Innerhalb der Unternehmensgrößen werden überdurchschnittlich viele Unternehmen mit 1000 bis 2000 Mitarbeitern den Weg in die Cloud gehen.



Durch das Speichern „außer Haus“ wird die Verantwortung für den Datenschutz an die externen Partner und Dienstleiter übertragen. Die Unternehmen sollten

daher prüfen, ob ihre Dienstleister auch gemäß den vorgeschriebenen Datenschutzbestimmungen handeln. Insbesondere bei der Auslagerung von Rechenzentren oder der Migration in die Public Cloud, kann es problematisch werden, wenn sich das Rechenzentrum des jeweiligen Dienstleisters außerhalb Deutschlands befindet. Um dem entgegenzuwirken, soll mit der neuen EU-Datenschutzverordnung ab 2018 für alle Dienstleister in allen EU-Mitgliedstaaten derselbe Standard in Bezug auf den Datenschutz gewährleistet werden. Prinzipiell wären somit alle Rechenzentren auf EU-Boden als Standort für Cloud-Lösungen geeignet.

Relevanz von Datenschutz und Verantwortlichkeiten

Definition Datenschutz

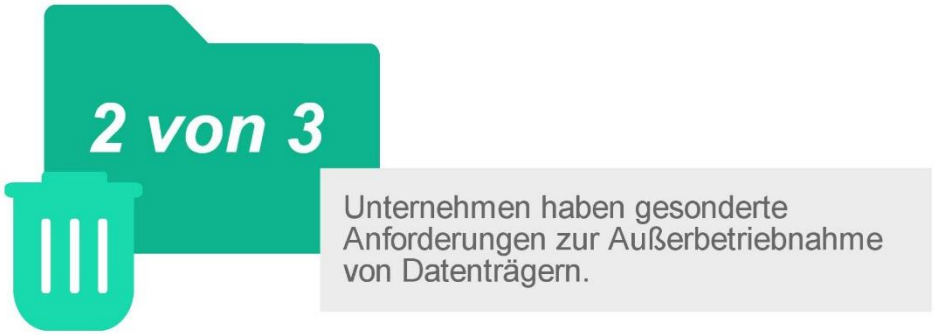
Der Datenschutz befasst sich nicht nur explizit mit dem Schutz der Daten im Allgemeinen, sondern in erster Linie auch mit dem Schutz der Personen, die hinter den Datensätzen stecken. Das Bundesdatenschutzgesetz definiert den Datenschutz so, dass der Zweck dieser Maßnahmen dazu dient, den Einzelnen davor zu schützen, dass der Umgang mit seinen personenbezogenen Daten sein Persönlichkeitsrecht beeinträchtigt (§ 1 Abs. 1 BDSG).

Sind Datenträger defekt oder müssen aus anderen Gründen außer Betrieb genommen werden, sind die Daten vor dem Entsorgen sicher zu entfernen. 76 Prozent der Unternehmen haben Prozesse definiert, wie Datenträger außer Betrieb zu nehmen sind, um eine sichere Datenlöschung zu garantieren.

24 Prozent haben dafür keine konkreten Prozesse vorgeschrieben. Dies birgt Gefahren, denn das Risiko des Datenmissbrauchs ist stark zunehmend. Der wachsende Anteil des mobilen Arbeitens und der mobilen Kommunikation via Tablets und Smartphones lässt die Sicherheitsrisiken steigen. 42 Prozent der Unternehmen haben private Endgeräte in ihrem Unternehmensnetzwerk eingebunden. Die Informationstechnologie ist schnelllebig und dynamisch. Eine täglich wachsende Datenflut ist zu managen. Auch die Lebenszyklen der Datenträger werden immer kürzer, definierte Prozesse zur sichereren Datenlöschung sind dafür unabdingbar.

61 Prozent der Unternehmen haben Hardwarekomponenten im Einsatz, die aufgrund Speicherung sensitiver Daten nach einem Defekt das Unternehmen nicht verlassen dürfen, auch nicht zu Reparaturzwecken.

Werden Datenträger über Service-Provider bezogen, sollte darauf geachtet werden, dass die Möglichkeit besteht, defekte Datenträger im Unternehmen einzubehalten. Explizite Anforderungen an den Datenschutz restriktive gesetzliche Datenschutzbestimmungen zur Außerbetriebnahme von Datenträgern gibt es bei zwei Dritteln der Unternehmen.



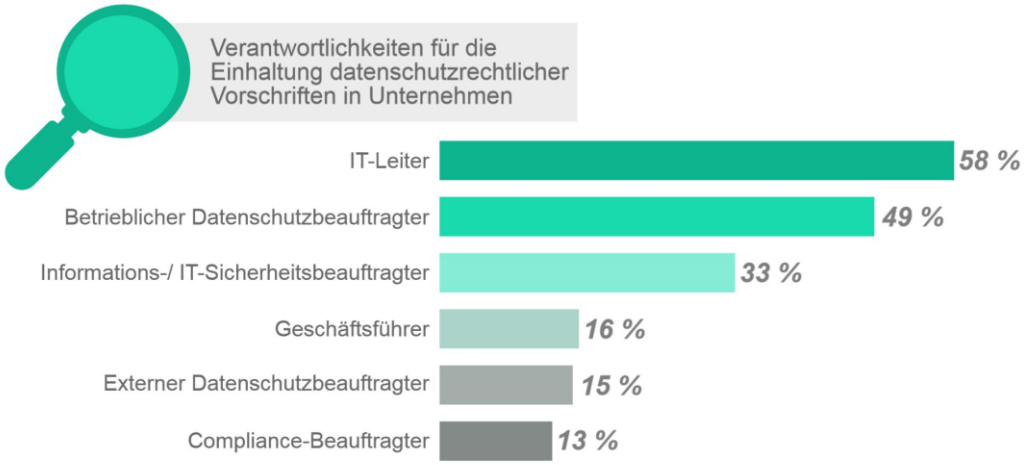
Verantwortung für datenschutzrechtliche Vorschriften

Ab 2018 wird die Ende 2015 beschlossene EU-Datenschutzgrundverordnung für alle EU-Staaten in Kraft treten. Diese soll den Datenschutz innerhalb der EU vereinheitlichen. Dabei wird im Prinzip das sehr strenge deutsche Datenschutzgesetz auf europäisches Niveau gehoben und für alle in der EU operierenden Unternehmen verpflichtend umgesetzt. Auch Unternehmen, welche in den USA ansässig sind, müssen sich künftig an die EU-Gesetze halten, wollen diese am europäischen Markt ihre Dienste anbieten. Für die Unternehmen wird es wichtig sein, sich bis dahin umfassend mit den neuen Compliance-Vorschriften zu befassen.

Viele Unternehmen sind dazu verpflichtet, vordefinierten Richtlinien bezüglich des Datenschutzes zu entsprechen. Dabei geben 64 Prozent der Unternehmen an, sich nach den Vorgaben der ISO 27001 zu richten, welche die Forderungen für die Einführung, Umsetzung, Überwachung und Verbesserung der Informationssicherheit auf internationaler Basis definiert. Durch eine Zertifizierung wird nachgewiesen, dass in einen IT-Verbund die Standardsicherheitsmaßnahmen nach IT-Grundschutz umgesetzt wurden. Für 46 Prozent ist der BSIT-Grundschutz bindend. Dieses Zertifikat soll einen mittleren, angemessenen und ausreichenden Schutz der IT-Systeme garantieren. Dabei wird die IT-Struktur analysiert, Schutzbedarfe festgestellt und anhand einer Modellierung die IT-Grundschutzmaßnahmen umgesetzt. 14 Prozent sind der Meinung keinen IT-Datenschutzrichtlinien entsprechen zu müssen.

Laut Bundesdatenschutzgesetz ist ein interner oder externer Datenschutzbeauftragter für Unternehmen ab 20 Mitarbeiter vorgesehen. Dieser kennt sich mit der komplexen rechtlichen Situation in Deutschland aus, prüft ob die entsprechenden Richtlinien eingehalten werden und unterstützt die bestehenden Datenschutzprozesse. Die Studienergebnisse zeigen, dass die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften eine Angelegenheit der IT-Abteilung (58 Prozent) in Zusammenarbeit mit dem Datenschutzbeauftragten ist. Diese gibt es in fast jedem Unternehmen ab 250 Mitarbeitern. 49 Prozent der Betriebe haben einen internen Datenschutzbeauftragten, 15 arbeiten mit einem externen Datenschutzbeauftragten zusammen. Ein weiteres Drittel der Unternehmen gab an, die Verantwortung einem Informations- und

Sicherheitsbeauftragten zu übertragen. Diesem Personenkreis obliegt die Aufgabe der Beratung, Schulung und Kontrolle der Einhaltung der Datenschutzvorschriften. Innerhalb der Größenklassen leisten sich interne Datenschutzbeauftragte vor allem größere Unternehmen. Unternehmen bis 1000 Mitarbeiter nehmen dagegen eher die Leistungen eines externen Datenschutzbeauftragten in Anspruch.



Außerbetriebnahme von Datenträgern

Eingesetzte Speichermedien

Klassische magnetische Festplatten (HDD) sind aufgrund ihrer vorherrschenden Stellung im Storage-Bereich und ihres relativ guten Preises noch immer das priorisierte Speichermedium und finden in 83 Prozent der Unternehmen ihren Einsatz. Allerdings zeigen die Studienergebnisse, dass bereits heute etwa die Hälfte der befragten Unternehmen neben herkömmlichen Speichermedien auf Flash-Speicher-Technologien setzt. Vor allem Unternehmen mit 1000 bis 1999 Mitarbeitern zeigen sich flash-affin, hier liegt der Einsatzgrad von Flash-Arrays bei 66 Prozent. Eine in 2015 durchgeführte Studie zu Flash-Arrays hat gezeigt, dass Unternehmen zukünftig vermehrt hybride Flash-Speicherlösungen einsetzen werden. Die für Nearline/Backup-Funktionen bewährten und günstigen Magnetbänder sind derzeit in rund einem Viertel der Unternehmen zu finden.

Werden die Speichermedien defekt oder haben sie ausgedient, müssen die Daten zuvor vom Speichermedium entfernt werden. Hierfür gibt es je nach Speichermedium unterschiedliche Methoden.

Nicht konsequent vernichtete Daten lassen sich ohne große Schwierigkeiten wiederherstellen. Damit die Daten dauerhaft und unwiederbringlich verschwinden, müssen sie „physikalisch“ gelöscht bzw. vernichtet werden.

42% der befragten Unternehmen sehen die Datensicherheit auf defekten oder ausgetauschten Datenträgern als kritisch an. Das spricht für einen Bedarf an sicheren Lösungen zur Datenzerstörung. Die Unternehmen greifen dafür auf unterschiedliche Methoden zurück. Generell müssen Unternehmen berücksichtigen, dass Daten nicht nur explizit auf Festplatten vorhanden sind, sondern auch auf Wechseldatenträgern, internen Hardwarekomponenten, wie Mainboards, Speicherriegeln, oder auch in Geräten wie Druckern lagern.

Methoden zur Entsorgung ausgedienter Datenträger

Gemäß dem Bundesamt für Sicherheit und Informationstechnik (BSI) sollte für die Initiierung und Umsetzung der Vernichtung von Daten sowohl der IT-Sicherheitsbeauftragte als auch der Leiter der IT des Unternehmens verantwortlich sein. Zur Löschung von Datenträgern stehen verschiedene Methoden zur Verfügung. Welche Methode gewählt wird, hängt von der Art des Datenträgers und vom Schutzbedarf der zu löschenden Daten ab.

Lagerung von Datenträgern

42 Prozent der befragten Unternehmen lagern ihre ausrangierten Datenträger zunächst im Rechenzentrum oder anderen Räumlichkeiten. Dies ist besonders dann notwendig, wenn auf den Datenträgern vertrauliche oder geheime Dateien gespeichert sind und das Unternehmen selbst mit erhöhten Datenschutzbestimmungen belegt ist, wie es in Behörden, Regierungen sowie Unternehmen aus dem Finanz oder Gesundheitssektor üblich ist. In einem solchen Fall kann der Datenträger aufgrund von Aufbewahrungspflichten nicht sofort zerstört werden.

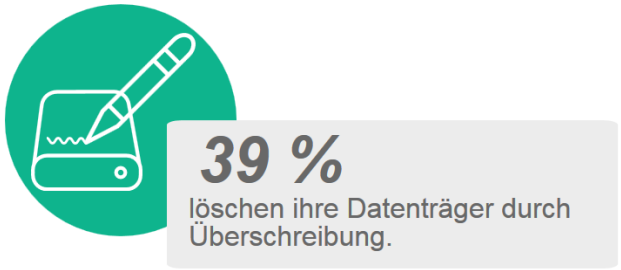
Schreddern

Eine Methode zur Datenvernichtung stellt das Zerstören des Datenträgers, das sogenannte „Schreddern“, dar. Magnetische Datenträger, die nicht weiterverwendet werden, werden mit geeigneten Geräten vernichtet. 42 Prozent der Unternehmen gaben an, zur Zerstörung der Datenträger „Schredder-Services“ zu nutzen. Die Geräte zur Vernichtung von Datenträgern sind häufig groß, komplex in der Bedienung und teuer. Dennoch „schreddern“ 58 Prozent die Datenträger vor Ort im eigenen Unternehmen, die sie ihre Datenträger auf Grund

sensitiver Daten nicht aus dem Haus geben dürfen. Die übrigen 42 Prozent nehmen hierfür die Leistungen eines Dienstleisters in Anspruch.

Das zuverlässige Vernichten der Daten ist die eine Seite, der rechtliche Aspekt die andere. Wichtig ist, dass entsprechende Zertifizierungen vorhanden sind und eingehalten werden. Der Entsorgungsdienstleister muss einen Sicherheitsprozess haben, der garantiert, dass die zu vernichtenden Datenträger zuverlässig unlesbar gemacht werden und Unbefugte keine Informationen daraus gewinnen können. Der Dienstleister muss daher nach einem aktuellen und nachvollziehbaren Datenschutz- und Sicherheitskonzept handeln. Die Unternehmen müssen mit dem Dienstleister entsprechende Regelungen gemäß den jeweils geltenden gesetzlichen Bestimmungen treffen und bei der Vertragsgestaltung darauf achten, dass die Sammelstellen, der Transport und die Vernichtung beim Dienstleister angemessen abgesichert sind.

Datenlöschung

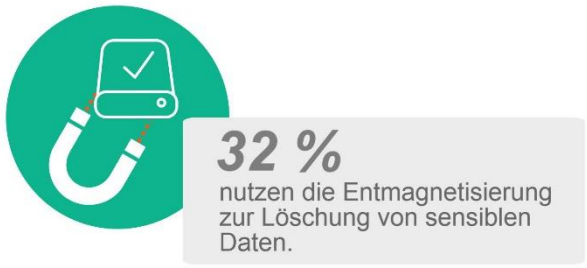


Eine relativ einfache Möglichkeit, Daten dauerhaft zu löschen, ist der Einsatz einer speziellen Software. 39 Prozent lassen die Datenträger nach standardisierten Verfahren überschreiben. Bei dieser Methode werden die Datenträger mit unterschiedlichen Algorithmen überschrieben. Dabei sind Verfahren und Mechanismen notwendig, die über die Standardlöschverfahren hinausgehen und Daten mit hohem Schutzbedarf so löschen, dass sie nicht wiederhergestellt werden können. Um zu gewährleisten, dass keine Reste des ursprünglichen magnetischen Musters übrigbleiben, muss mehrfach überschrieben werden. Es gilt: Je öfter der Datenträger überschrieben wird, umso sicherer kann man sein, dass die Daten auch definitiv nicht mehr durch Unbefugte wiederhergestellt werden können. Laut BSI-Richtlinien ist vorgeschrieben, wie oft zu überschreiben ist.

Für den normalen Schutzbedarf ist ein einmaliges Überschreiben ausreichend. Vertrauliche Daten sind zweimal zu überschreiben. Hewlett Packard Enterprise bietet mit Data Privacy Services eine Software an, deren Überschreibungspro-

zedur bereits standardmäßig dreimal erfolgt, so dass eine sichere Löschung garantiert wird. Es ist es wichtig, dass die eingesetzte Softwarelösung auf dem neuesten Stand der Technologie ist. Zudem muss die Software richtig bedient und konfiguriert werden. Falsche Bedienung führt dazu, dass der Datenträger gar nicht oder nur teilweise überschrieben wird und ein Auslesen durch Dritte noch möglich ist. Der Einsatz von Experten für die korrekte Löschung von Datenträgern ist bei fehlendem in-house Know-how unabdingbar. Was das Speichermedium betrifft, so gibt es keine Einschränkungen, SSDs können mit entsprechenden Softwarelösungen, wie sie HPE anbietet, ebenso gelöscht werden wie Festplatten.

Entmagnetisierung (Degaussing)



Eine weitere Alternative, insbesondere zur Löschung von SSDs und hybriden Festplatten, ist die Entmagnetisierung. Durch Degausser werden magnetische Datenträger irreversibel gelöscht. Dabei werden die Magnetstrukturen auf dem Datenträger – egal ob Festplatte, Diskette oder Backup-Band – zerstört. Alle Informationen, die als Bits und Bytes in der Form 1 oder 0 auf dem Speichermedium hinterlegt sind, werden in eine Richtung gebracht, sodass nur noch entweder Einsen oder Nullen vorhanden sind. Bei der Entmagnetisierung werden auch die Servo- und Wartungsinformationen mit vernichtet, so dass die Datenträger nach der Entmagnetisierung nicht mehr zu gebrauchen sind.

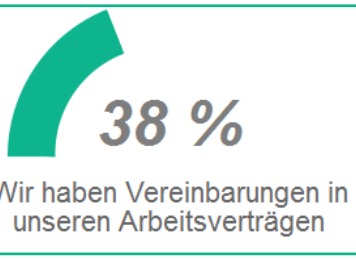
Was tun bei Datenverlust?

Trotz höchster Vorsicht bei all den genannten Methoden, kommt es dennoch vor, dass Daten verloren gehen. Diesbezüglich handeln die Unternehmen unterschiedlich:

66 Prozent der Unternehmen haben definiert, welche Personen innerhalb des Unternehmens über den Datenverlust zu informieren sind. Die entsprechenden Stellen oder Personen, meist die IT-Leitung, wenn vorhanden Datenschutzbeauftragte oder die Geschäftsführung, können auf den Verlust schnell reagieren und Maßnahmen einleiten.

Den Datenverlust an externe Stellen, wie der Polizei oder entsprechenden Datenschutzaufsichtsbehörden, melden knapp 49 Prozent der Unternehmen. Mit der neuen EU-Verordnung muss prinzipiell jeder Datenverlust gegenüber dem Betroffenen und der Meldebehörde zur Kenntnis gebracht werden, sofern das Risiko besteht, dass Dritte die Daten verwenden können, es sei denn die Daten sind durch Verschlüsselungsmaßnahmen geschützt.

Einzuleitende Maßnahmen, wie zum Beispiel die genaue Feststellung und Dokumentation des Verlustes, werden von 47 Prozent der Unternehmen definiert. Eine detaillierte Aufbereitung des Vorfalls kann dazu genutzt werden, zukünftig besser gegen Datenverluste geschützt zu sein.



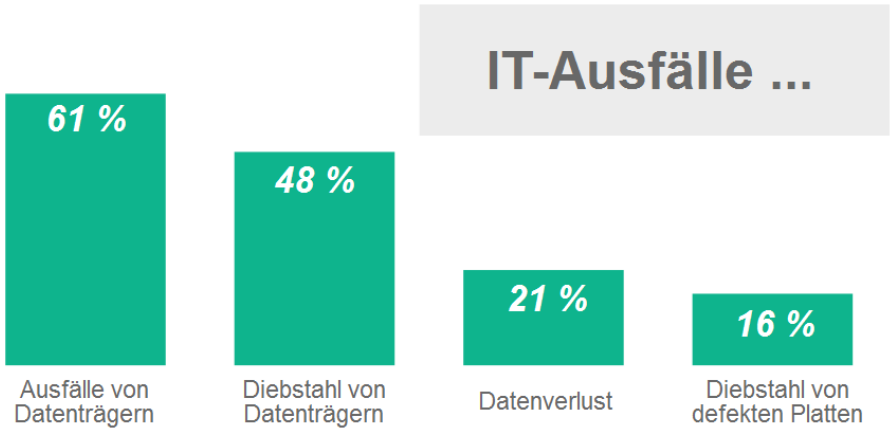
38 Prozent der Unternehmen haben Vereinbarungen bezüglich des Datenschutzes in Arbeitsverträgen, sowie in Dienst- und Betriebsvereinbarungen festgehalten.

Verlust von Datenträgern und deren Folgen

Die Studienergebnisse zeigen: Trotz aller Maßnahmen kam es im letzten Jahr immer wieder zu unangenehmen Zwischenfällen und „Datenlecks“. Ausfälle von Datenträgern beklagten 61 Prozent der befragten Unternehmen, 33 Prozent sogar mehrfach im Jahr.

47 Prozent der Unternehmen haben Daten verloren. Es zeigt, dass die Unternehmen nicht genügend Sorgfalt walten lassen. In 22 Prozent der Unternehmen kam es zum Diebstahl der Datenträger. In 16 Prozent wurden defekte Festplatten gestohlen.

Die Ergebnisse zeigen, generell sind größere Unternehmen gefährdeter als kleinere.



Die Datenausfälle bleiben nicht ohne Folgen. Für viele Unternehmen wurde es teuer. Auf 55 Prozent der Unternehmen kamen zusätzliche interne Kosten zu. Weitere 39 Prozent mussten außerplanmäßig Gelder für externe Dienstleister aufbringen. In jedem zweiten Unternehmen kam es zu Arbeitsunterbrechungen und -ausfällen. Jedes fünfte Unternehmen litt unter einer beeinträchtigten Produktivität und jedes vierte Unternehmen beklagt den Verlust von Informationen.

Zukünftige Herausforderungen

Der mobile Zugang auf Geschäftsdaten wird zukünftig noch weiter an Bedeutung gewinnen. Aktuell haben 42 Prozent der Unternehmen private Endgeräte in das Unternehmensnetzwerk eingebunden. Mobilität führt dazu, dass die Sicherheit der Daten immer mehr Risiken ausgesetzt ist. 44 Prozent der befragten Unternehmen prognostizieren einen Anstieg von sensiblen Daten. 62 Prozent der Unternehmen sehen daher die Gewährleistung des mobilen Zugangs auf Geschäftsdaten als große Herausforderung in Bezug auf Datensicherheit im Unternehmen.

Mit dem weiteren Wachstum von virtuellen Umgebungen und Cloud-Infrastrukturen werden die Sicherheitsrisiken und Angriffsbedrohungen in Unternehmen zunehmen und neue Formen annehmen. 61 Prozent der Befragten nutzen derzeit Cloud-Anwendungen in ihren Unternehmen. Nahezu jedes Unternehmen, welches Cloud-Dienste bezieht, hat explizit technische, organisatorische und rechtliche Maßnahmen ergriffen, um Cloud-Anwendungen, -Plattformen und -Infrastrukturen abzu-

sichern. 63 Prozent der Unternehmen haben eine dedizierte Cloud-Absicherung, vor allem große Unternehmen ab 1000 Mitarbeitern treffen auf diesem Weg Vorsorge. Bei 33 Prozent erfolgt die Absicherung im Rahmen der allgemeinen IT- und Informationssicherheit. Nur 4 Prozent verlassen sich darauf, dass der Cloud-Anbieter für die Sicherheit sorgt.

61 Prozent der Unternehmen sehen auch die wachsenden Anforderungen an die Compliance als große Herausforderung. Insbesondere mit der neuen EU-Verordnung müssen die Unternehmen ihre gesamte IT-Sicherheit auf den Prüfstand stellen, um nicht dagegen zu verstoßen. Bußgelder von bis zu 4 Prozent vom Jahresumsatz können bei Nichteinhaltung der Gesetze zu schweren finanziellen Schäden führen.

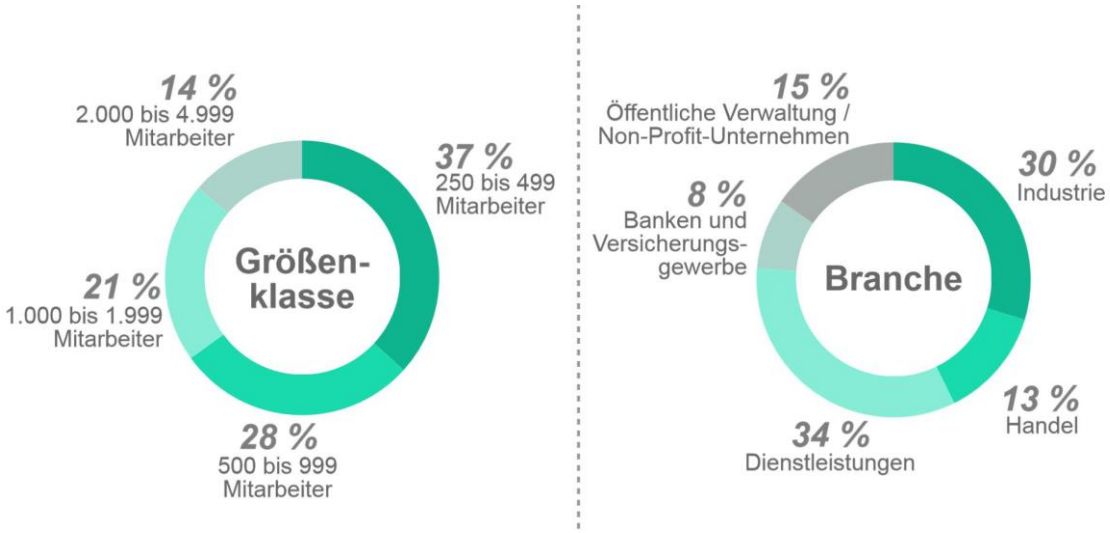
Fazit

In Zukunft wird sowohl die steigende Nachfrage nach mobilem Zugriff auf Geschäftsdaten sowie die generelle Zunahme von sensiblen und kritischen Daten Unternehmen vor immer größere Herausforderungen im Hinblick auf die Wahrung der Datensicherheit stellen. Verschärft wird die Situation durch immer strenger werdende Compliance-Anforderungen und die ab 2018 in Kraft tretende EU-Datenschutzverordnung.

Der Datenschutz ist und bleibt ein absolut wichtiges Thema für die Unternehmen. Viele Unternehmen nutzen entsprechende Methoden zur Datenlöschung und Datenvernichtung. Doch nicht alle tun es in dem Maße, wie es notwendig wäre, denn es treten immer noch zu viele Ausfälle und Datenlecks auf. Die Studienergebnisse zeigen deutlich, dass fahrlässiger Umgang mit Datenträgern und Nachlässigkeit bei der Vernichtung oder Entsorgung ausgedienter Datenträger in den Unternehmen keine Seltenheit ist und noch immer zu Problemen und beachtlichen Schäden führt, die es zu vermeiden gilt. Oftmals ist die interne IT überfordert. Unternehmen sollten daher neben Datenschutzbeauftragten auch mit zertifizierten Dienstleistern kooperieren, die in der Lage sind, defekte und ausgediente Datenträger vorschriftsmäßig gemäß den Datenbestimmungen zu löschen, zu entsorgen oder zu recyceln, um einen Zugriff Unbefugter zu unterbinden und Schaden abzuwenden.

Studiendesign und Stichprobe

Die Studie „Data Privacy Security“ wurde von der techconsult GmbH im Auftrag von Hewlett Packard Enterprise konzipiert und durchgeführt. Im Februar 2016 wurden 300 Unternehmen der Größenklasse 250 bis 4999 Mitarbeiter zum Thema Datenschutz und sichere Datenträger-Entsorgung befragt. Die Stichprobe verteilt sich über alle Branchen. Ansprechpartner waren in erster Linie IT-Leiter, Leiter für Datenschutz und Datensicherheit sowie Geschäftsführer.



Verena Bunk
Senior Analyst

techconsult GmbH

Baunsbergstr. 37
D-34131 Kassel

E-Mail: verena.bunk@techconsult.de
Tel.: +49-561-8109-141
Fax: +49-561-8109-101
Web: www.techconsult.de

Über techconsult GmbH

Die tech**consult** GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt tech**consult** über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht. Die tech**consult** GmbH wird vom geschäftsführenden Gesellschafter und Gründer Peter Burghardt am Standort Kassel mit einer Niederlassung in München geleitet und ist Teil der Heise Medien Gruppe.

Über Hewlett Packard Enterprise

Hewlett Packard Enterprise ist ein branchenführendes IT-Unternehmen, das Kunden hilft, sich schneller weiterzuentwickeln. Mit dem umfassendsten Technologie- und Service-Portfolio der IT-Branche – von der Cloud über das Rechenzentrum bis hin zur Arbeitsplatzanwendung – unterstützen wir unsere Kunden weltweit dabei, ihre IT effizienter, produktiver und sicherer zu machen.

Weiter Informationen unter hpe.com/de