Datenschutz

„Die Verantwortung lässt sich nicht delegieren“

Die Vernichtung vertraulicher Daten ist zu einem komplexen Prozess geworden. Strukturieren soll ihn die neue DIN 66399, nach der papierhafte und digitale Datenträger sicher und umweltgerecht entsorgt werden sollen. Denn Negativbeispiele zeigen immer wieder, wie schnell Informationen über Kunden oder Mitarbeiter in falsche Hände geraten können. Mit Hilfe der aktuellen Sicherheitsvorschriften lassen sich die Gefahren des Verlusts vertraulicher Daten begrenzen und sensible Informationen zuverlässig vernichten. „Banken+Partner“ sprach mit Branchenexperten über Anforderungen und Herausforderungen im Datenschutz.

Seit Oktober 2012 gilt die neue DIN 66399 zur Datenträgervernichtung. Was hat sich konkret mit der neuen Norm verändert?

Ernst: Die Vorgängernorm konzentrierte sich sehr stark auf Papiermedien. Verschiedene Arten digitaler Datenträger fanden kaum Berücksichtigung. In der neuen DIN-Norm werden aber beide Punkte behandelt. Konkret ist bei der Vernichtung von Datenträgern sicherlich die Frage nach dem Schutzbedarf und die Einteilung der einzelnen Schutzklassen die größte Veränderung, die wir derzeit erleben. Diese Faktoren wurden in der alten Norm komplett außen vor gelassen. Hinzu kommen noch die verschiedenen Materialklassifizierungen. Allerdings waren diese Veränderungen in der Informations- und Datensicherheit zwingend erforderlich. Was man darüber hinaus nicht vergessen darf: Der Umweltschutz spielt dabei eine immer größere Rolle. Auch darauf müssen wir uns einstellen. Wir brauchen daher geeignete, aber auch wirtschaftlich vertretbare Verfahren für die sichere Vernichtung von Datenträgern.

Stein: Konkret sieht die neue DIN drei Schutzklassen bei der Datenträgervernichtung vor. Die Herausforderung für jedes Unternehmen besteht darin, diese Schutzklassen in die eigenen Unternehmensstrukturen einzubinden. Im Übrigen ist das papierhafte Zeitalter zwar noch längst nicht vorbei, allerdings sind in den vergangenen Jahren noch andere Datenträger hinzugekommen. Mussten wir früher ganz klassisch lediglich Papier in definierten Stufen zerkleinern, existieren mittlerweile sechs Materialklassifizierungen und für diese wiederum jeweils sieben Zerkleinerungsstufen. Erschwerend kommt hinzu, dass digitale Datenträger wie Festplatten oder USB-Sticks meist eine wesentlich höhere Datendichte haben als ein Stück Papier. Damit ändert sich auch die erforderliche Partikelgröße. Und natürlich bedeutet die neue DIN auch organisatorischen und personellen Aufwand. Heutzutage müssen hochsensible Daten in der Regel unter Aufsicht des Unternehmens vernichtet werden, vorzugsweise vor Ort und nicht erst auf dem Entsorgungshof. Diesen Anforderungen an Qualität und Quantität Rechnung zu tragen, stellt jedes Unternehmen vor eine große Aufgabe.

Inwieweit können Sie Ihre Dienstleister wirklich beaufsichtigen?

Hilderink: Selbstverständlich überwachen wir mit einem mehrköpfigen Team unsere Dienstleister, wenn sie bei uns vor Ort die Datenträger – in der Mehrzahl ist das Papier – vernichten. Eine Begleitung des geschredderten Materials bis zum Recycling-Hof ist aus unser Sicht angesichts des Vernichtungsgrades nicht erforderlich. Dies wäre auch logistisch nicht einfach – zumal es ja auch sein kann, dass der Dienstleister nachdem er bei uns war, zu einem anderen Unternehmen weiterfährt und auch dort Datenträger vernichtet, ehe er zum Recyclinghof zurückfährt.

Ernst: Ein zertifizierter Vernichtungs-Dienstleister muss in seinen Prozessen allerdings genau definieren, was mit dem geschredderten Material – seien es nun Reste von Papier oder elektronischen Datenträgern – passiert. Das gibt uns die Sicherheit, dass die Datenträger tatsäch-

Gesprächsteilnehmer Ernst, Stein, Hilderink (v.l.): *Datenschutz hat viele Facetten, die von den Kreditinstituten und deren Dienstleistern berücksichtigt werden müssen.*

lich der Norm entsprechend vernichtet wurden – dazu gehört natürlich auch, dass sie, wenn möglich, recycled und nicht nur verbrannt werden.

Stein: Allerdings stößt auch das Recycling an seine Grenzen – und zwar dann, wenn eine besonders hohe Zerkleinerungsstufe gewählt wird. Papierfasern im Millimeterbereich lassen sich nicht mehr wiederverwerten. Was mir derzeit noch Sorge bereitet ist Folgendes: Vielen Kunden ist noch nicht bewusst, dass sie zwar den Recyclingprozess delegieren können, die Verantwortung für die sichere Datenvernichtung aber nach wie vor tragen. Gehen dann wirklich hochsensible Daten verloren, wird nicht der Dienstleister, sondern immer der Auftraggeber zur Rechenschaft gezogen.

Weshalb schreddern die Institute ihre Datenträger dann nicht einfach selbst und sparen sich den Dienstleister?

Hilderink: Wir haben ein gestuftes Verfahren: Besonders sensible Daten auf Papier, zu denen insbesondere Informationen über Kunden gehören, schreddern wir vorab mit kleineren Geräten, die in den einzelnen Abteilungen stehen. Das gleiche gilt für besonders sensible Daten auf anderen Datenträgern. Laufwerke werden beispielsweise elektronisch gelöscht und dann mechanisch zerstört. Darüber hinaus gibt es Informationen, deren Vernichtung nicht unmittelbar erforderlich ist, beispielsweise Ausdrucke externer Newsletter, Gesetzesentwürfe, Veröffentlichungen von Behörden und so weiter. Die Anschaffung einer großen Schredderanlage hierfür wäre allerdings nicht rentabel. Für größere Mengen papierhafter sowie digitaler und elektronischer Datenträger greifen wir deshalb auf einen externen Dienstleister zurück, der die Vernichtung mit seiner mobilen Anlage vor Ort durchführt. Zumal wir ja Niederlassungen in ganz Deutschland haben. Die Zentrale ist zwar in Frankfurt, wir haben aber auch Filialen in Berlin, Bielefeld, Hamburg, Düsseldorf, Köln, Stuttgart oder München.

Ernst: Bei uns liegt der Fall ähnlich. Es ist schlichtweg ein Mengenproblem und logistisch nicht zu bewältigen. Deshalb stand eine eigene Anlage für uns auch nie zur Debatte. Ausgenommen ist die Personalabteilung. Deren Büros sind in der Regel mit Tisch-Schreddern ausgestattet, um Personalunterlagen sofort vernichten zu können. Für alle anderen Aufgaben haben wir unsere festen Auftragsunternehmen. Wenn wir Dokumentenarchive im Auftrag unserer Mandanten digitalisieren, dann übernehmen wir Unterlagen oder Aktenordner, die teilweise in meterhohen Regalen lagern. Diese Unterlagen anschließend zu vernichten, könnten wir allein gar nicht leisten. Für uns ist klar, diese Aufgabe muss jemand übernehmen, dessen Kernaufgabe die Datenvernichtung ist. Bei der Auswahl des Dienstleisters achten wir natürlich auf die Zertifizierung nach DIN 66399.

Stein: Tatsächlich müssen sich die Institute drei Fragen stellen, ehe sie sich für oder gegen die Vergabe an einen Dienstleister entscheiden. Erstens: „Haben wir eine dezentrale oder eine zentrale Aktenvernichtung?“ Zweitens: „Mit welcher Datenträgermenge haben

Alfred Ernst
Datenschutz- und IT-Sicherheitsmanagement, DSGF Deutsche Servicegesellschaft für Finanzdienstleister

Dr. Berthold Hilderink
Datenschutzbeauftragter, UBS Deutschland

Harry Stein
Externer Datenschutzbeauftragter (IHK), Key Account Manager Bürotechnik Zentraleuropa, HSM

wir es zu tun?“ Und drittens: „Wie hoch ist der Schutzbedarf, der auf den Trägern vorhandenen Daten?“ Im Tagesgeschäft ist die selbstständige Aktenvernichtung bei den meisten Instituten eher unproblematisch. Mit einem Tisch-Schredder je Arbeitsplatz, oder einem größeren Gerät für eine Abteilung, lässt sich die Menge an Papier, die täglich anfällt, in der Regel problemlos vernichten. Wenn es aber darum geht, einmal jährlich ganze Archive zu leeren, reichen die Kapazitäten eines kleinen Aktenvernichters nicht aus. Vor allem, da viele Unternehmen vergessen, dass es neben den vorgeschriebenen Aufbewahrungspflichten auch die Pflicht zur Aktenvernichtung gibt. Das ist ein extrem wichtiger Aspekt, den viele Unternehmen einfach außer Acht lassen. Wirtschaftlich ist es daher sinnvoll, einen Experten zu Rate zu ziehen. Eine finanzielle Gegenüberstellung von Kosten und Ertrag ist sicherlich der schwierigere Teil. Denn wenn es sich nicht um eine einmalige Entsorgung, sondern um einen regelmäßigen Aufwand handelt, könnte man durchaus über eine Inhouse-Lösung nachdenken. Hier haben wir allerdings wieder das Platzproblem. Kaum ein Architekt hat bei der Planung eines Unternehmensgebäudes Räume für eine Aktenvernichtungsanlage berücksichtigt. Das beginnt bereits bei den einfachen Kopierräumen. Bei der Entscheidung, ob eine Anlage beim Kunden vor Ort installiert wird oder ob er die gesamte Aktenvernichtung auslagert, müssen also zahlreiche Dinge beachtet und abgewogen werden. Das ist die eigentliche Herausforderung.

Wie haben Sie die Aktenvernichtung in ihren Häusern konkret organisiert?

Hilderink: Wir haben auf jeder Etage verschlossene Metallbehälter, in die alles Papier kommt, das in den Büros anfällt und welches nicht bereits unmittelbar in den Abteilungen geschreddert wird. Hierzu gehören Unterlagen, die weniger kritisch sind, weil sie weder Kunden- beziehungsweise Arbeitnehmerdaten noch Betriebs- oder Geschäftsgeheimnisse beinhalten. Abfalleimer gibt es nur für Restmüll. Hochsensible Akten, die einen besonderen Schutz verlangen, werden von den Mitarbeitern im Büro sofort und selbst vernichtet. Dazu zählen zum Beispiel Ausdrucke von Kundenportfolios, Schriftverkehr oder Personalunterlagen. Der gesamte Papiermüll aus den Tonnen und den Büroschreddern wird gesammelt und von unserem Dienstleister dann unter Aufsicht geschreddert. Natürlich erhalten unsere Mitarbeiter von uns eine entsprechende Einweisung oder Schulung, zudem existieren klare Verhaltensregeln.

Ernst: So ähnlich handhaben wir das auch. Wir führen alle Papierabfälle einer datenschutzkonformen Vernichtung zu, um Risiken zu minimieren oder ganz zu vermeiden. Denn wenn die Mitarbeiter selbst entscheiden, welche Papiere sie schreddern lassen und welche nicht, kann es immer zu Fehlern kommen. Zwar sollten Fehlentscheidungen in jedem Unternehmen die Ausnahme sein, aber keines ist davor gefeit. Deswegen spielt bei uns auch das Thema Informationsklassifizierung eine entscheidende Rolle. In einer internen Verordnung haben wir entschieden, welche Dokumente wir welcher Sicherheitsstufe zuordnen. Aus diesem Grund schreddern wir alles, was in den Papierkörben landet, egal ob es sich um Werbematerial oder internen Schriftverkehr handelt. Das geschieht einheitlich und datenschutzkonform. Vernichtungstonnen für mandantenbezogene Unterlagen stehen auf allen Fluren unserer Bürogebäude bereit.

Ist den Mitarbeitern bewusst, wie wichtig die korrekte Vernichtung von Datenträgern ist?

Hilderink: Bei unseren Mitarbeitern in jedem Fall. Unser Personal wird diesbezüglich gezielt geschult. Alle neu eintretenden Mitarbeiter erhalten eine Datenschutzschulung. Zudem erfolgen bundesweit regelmäßige Wiederholungsschulungen durch den betrieblichen Beauftragten für den Datenschutz. Um in der praktischen Umsetzung für die Mitarbeiter die Datenvernichtung noch komfortabler zu machen, sind auch genügend verschlossene Metallbehälter in den einzelnen Abteilungen vorhanden, um die Wege zu verkürzen.

Stein: Wenn wir von Bewusstsein

reden, müssen wir den externen Dienstleister unbedingt mit einbeziehen. Und dieser Bereich beginnt schon beim Reinigungspersonal. Schließlich ist selbst die Gebäudereinigung eine Art Auftragsdatenverarbeitung – wenigstens dann, wenn sie nicht nur die Restmüll-Abfalleimer leert. Deswegen müssen auch diese Mitarbeiter eingewiesen werden und Datenschutz- und Sicherheitsstandards beachten. Sie müssen dafür sensibilisiert werden, Papierkörbe gründlich zu leeren, und mit dem Material vertraulich umzugehen. Entsteht bereits in dieser Kette ein Bruch, nützt auch die schönste Datenschutzverordnung nichts. Dieser Gesichtspunkt darf nicht unterschätzt werden.

Inwieweit sind elektronische Datenträger ein Thema?

Hilderink: Wir halten alle Daten auf unseren Servern. Auf den Arbeitsplatzrechnern können lokal keine Daten gespeichert werden. Auch USB-Sticks existieren bei uns nicht, ebenso wenig können unsere Mitarbeiter CDs brennen oder etwas auf andere mobile Datenträger speichern. Aus diesem Grund fallen bei uns nur sehr wenige elektronische Datenträger an.

Ernst: Auch wir setzen auf eine Thin-Client-basierte IT-Infrastruktur und verzichten dort ganz auf lokale Laufwerke und Speichermedien. Während die klassischen Desktop-PCs früher standardmäßig mit einer enormen Festplattengröße und genügend Speicherplatz ausgestattet waren, ist es damit für unsere Mitarbeiter nicht mehr möglich, Daten lokal abzulegen. Der Vorteil: Die neuen Geräte heute können anders entsorgt werden. Die wenigen Festplatten, die noch existieren, werden bereits bei uns grob vorvernichtet, das heißt, sie werden mechanisch unbrauchbar gemacht. Da diese Methode zur sicheren Datenvernichtung bei weitem nicht ausreicht, übernimmt der externe Dienstleister den Rest des Vernichtungsprozesses entsprechend der DIN-Norm.

Stein: Elektronische Datenträger oder Informationsquellen gehen natürlich weit über Desktop-PCs oder USB-Sticks hinaus. Heutzutage müssen wir zum Beispiel auch die Kopiersysteme als elektronischen Datenträger bezeichnen, denn selbst diese Geräte sind mit einer Festplatte ausgestattet. Deswegen weisen wir unsere Kunden bereits bei einem ersten Gespräch auf dieses Thema hin. Unser Rat ist es, schon bei der Ausschreibung solcher Kopier- oder Multifunktionsgeräte mit dem Lieferanten über die Entsorgung nach Ablauf der Mietzeit zu reden. Es sollte im Vorfeld geklärt werden, ob die darin vorhandenen Datenträger beispielsweise vor Ort ausgebaut und zur eigenen Vernichtung überlassen werden. Solche Fragen geraten schnell in Vergessenheit. Ein anderes Thema ist das Hardware-Reselling – also die Wiederaufbereitung und der Weiterverkauf von Hardware. Manche Dienstleister erwerben von Banken oder Behörden gebrauchte Rechner, bereiten diese auf – indem sie beispielsweise die alten Festplatten austauschen – und verkaufen sie weiter. Die darauf gespeicherten Daten müssen natürlich so vernichtet werden, dass die Inhalte nicht wiederhergestellt werden können. Das funktioniert am besten mit einem Festplattenschredder.

Margaretha Hamm, Anja Töpfer