Destruction physique de porteurs de données

Evitez de vous faire pénaliser!

Le vol d'informations confidentielles (ou espionnage industriel) peut être néfaste pour plus d'une organisation. Dans de mauvaises mains, ces informations pourraient mener des entreprises à la faillite, faire perdre leur emploi à de nombreuses personnes et ruiner actionnaires et familles. Ces mêmes informations peuvent également avoir des conséquences pour les actions en bourse (l'abus d'informations privilégiées est punissable!). D'autre part, l'emploi contrôlé et la sécurisation des données à caractère privé ne cessent de gagner en importance. La protection de la vie privée se voit, en effet, de plus en plus règlementée par le législateur. Et de fortes peines pécuniaires sanctionnent toute entorse à ces règles.

C'est surtout dans les grandes organisations à caractère documentaire ou informatique prononcé que les flux d'informations entrantes/sortantes peuvent atteindre des niveaux fort élevés. Et ceci sous la forme de mémos, de rapports, de comptes rendus, de clés USB, de CD-ROM, de bandes (magnétiques) et autres supports de données. Cette pléthore d'information complique notablement les problèmes de stockage, de transport et de destruction. Le présent article traite principalement des supports de données arrivés en fin de vie et devant être détruits de façon sécurisée.

La norme DIN 66399

Depuis 2010, la DIN 66399 régit les procédures de destruction de supports de données. Il s'agit d'une norme industrielle à caractère général traitant de la destruction de toutes sortes de supports de données. En plus des principes de base et des définitions des différents types de support, la DIN 66399 formule également des exigences techniques pour l'équipement de destruction et donne aussi des directives quant aux procédés de destruction des supports de données (SPEC). La norme DIN 66399 a été rédigée par le DIN (Deutsches Institut für Normung), en collaboration avec l'industrie et autres parties concernées. Elle remplace la très connue DIN 32757. A côté de la DIN 66399, citons aussi la Directive NEN-EN 15713:2009 "Destruction sécurisée de données confidentielles", toujours d'application. Néanmoins, la NEN-EN 15713:2009 n'est pas suffisamment claire sur certains points. La DIN 66399 corrige ces imperfections. La façon la plus avantageuse de détruire les supports de données arrivés en fin de vie est à l'aide d'un destructeur de documents ou 'shredder'. Mais un déchiquetage poussé n'est pas nécessairement fin assez : il importe donc d'attribuer une classification de sécurité à ces

Niveau de sécurité	Données	Reconstitution
1	Données générales	Requiert peu d'efforts
2	Données internes	Requiert un effort spécial
3	Données confidentielles	Requiert un effort considérable
4	Données hautement confidentielles	Requiert un effort exceptionnel
5	Données secrètes	Requiert des méthodes extrêmes
6	Données hautement secrètes	Techniquement impossible
7	Données 'Top Secret'	Impossible

La DIN 66399 distingue sept niveaux de sécurité. Le niveau de sécurité se rapporte aux données et à la reconstitution des documents. Il dépend des cylindres de coupe du destructeur de documents.

Classification du matériau	Information/données	Exemples	Niveaux de sécurité
P	Taille d'origine	Papier, films, plaques d'imprimerie	P-1 à P-7
F	Taille réduite/minimalisée	Microfilms	F-1 à F-7
O	Porteurs optiques	CD, DVD, BluRays	O-1 à O-7
T	Porteurs magnétiques	Bandes, cartes à bande magnétique, diskettes	T-1 à T-7
H	Disques durs	Stations à disques durs	H-1 à H-7
E	Porteurs électroniques	Clés USB, cartes à puce, appareils de communication mobile	E-1 à E-7

La DIN 66399 introduit aussi une classification matérielle pour les supports de données à détruire. Le matériau dont est fait le support de données influence les possibilités de reconstitution. Cette classification normalisée est la suivante

supports, par le biais d'une analyse des risques. Les supports de données classifiées pourront, ensuite, être détruits en conformité avec les normes applicables. Si l'importance des données à détruire croît, le degré de destruction (finesse) doit croître dans la même mesure : ceci réduit les chances de reconstitution de l'information. La DIN 66399 connaît trois classes de protection des données :

1. Protection normale de données internes, dont la divulgation peut avoir un impact négatif sur l'entreprise ou impliquer un risque d'usurpation d'identité de personnes.
2. Protection élevée de données confidentielles, dont la divulgation peut avoir un impact hautement négatif sur l'entreprise ou impliquer un risque d'enfreinte d'obligations légales.
3. Protection très élevée de données confidentielles et Top Secret, dont la divulgation peut mettre en danger l'existence même d'une entreprise ou d'une autorité, ou impliquer un risque de santé, de sécurité ou de liberté personnelle, ou nuire à la position économique ou sociale d'un individu.

La DIN 66399 distingue sept niveaux de sécurité. Le niveau de sécurité se rapporte aux données et à la possibilité de reconstitution des documents. Il dépend des cylindres de coupe du destructeur de documents considéré.

Comme expliqué ci-dessus : la DIN 66399 est une norme industrielle d'application générale qui décrit l'entièreté du processus : de la collecte des documents jusqu'à leur destruction proprement dite, en passant par le transport et le stockage. Les sujets suivants y sont traités : organisation, personnel, collecte/stockage/transport, destruction. Ainsi, le personnel ayant accès au local où se trouvent les 'shredders' doit signer une déclaration de conformité. Les personnes extérieures visitant un tel local doivent être accompagnées par un membre du personnel organique et porter un badge 'visiteurs'. L'espace où sont entreposés les documents à détruire doit être pourvu d'une alarme d'effraction, reliée à un centre de télésurveillance, et la DIN 66399 prévoit aussi des caméras de surveillance. Des exigences particulières pour le transport sont également prévues dans la norme. Ainsi, les véhicules doivent être équipés d'un tracking GPS passif et/ou avoir au moins deux personnes à bord. On fera, en outre, appel à des véhicules à superstructure fermée et fixe. Finalement, les machines employées à la destruction doivent aussi satisfaire à la norme DIN 66399-1. Bref, la DIN 66399 a vraiment tout prévu. Vous lirez davantage à ce sujet dans la norme DMS 2008, plus loin.

European Association for **Data Media Security ©**

La European Association for Data Media Security, EA DMS en abrégé, réunit un nombre d'entreprises spécialisées qui s'occupent de la destruction de porteurs de données numériques/informatiques.

EA DMS

La European Association for Data Media Security, EA DMS en abrégé, réunit un nombre d'entreprises spécialisées qui s'occupent de la destruction de porteurs de données numériques/informatiques. Ce sont des entreprises d'Allemagne, de Belgique et des Pays-Bas. L'EA DMS a mis au point sa propre certification de branche dont le point de départ est « qu'il s'agit d'une méthode simple mais sûre pour la sélection et le contrôle du standard de sécurité requis, celui-ci étant d'un emploi aisé pour tout le monde, sans aides techniques ni connaissances exceptionnelles.» C'est cette philosophie qui est à la base de la DMS 2008.

La DMS 2008 donne des directives claires et transparentes pour l'élimination sécurisée de disques durs (HDD). Contrairement à la DIN 66399, la DMS 2008 décrit exclusivement les exigences relatives à l'élimination de disques durs. C'est pourquoi la DMS 2008 convient particulièrement à la certification de déchiqueteuses et/ou presses. Elle distingue cinq classes de sécurité : A, B, C, D et E.

Les entreprises certifiées DMS 2008 se déplacent généralement avec des minibus contenant un 'shredder' mobile. Si vous avez des disques durs à détruire, ces firmes viennent sur place et se garent devant votre porte, pour ainsi dire. La destruction se ▶▶

Classes de sécurité	Méthode	Possibilités de reconstitution	But
A	Le disque dur est débité en bandes d'env. 50 mm.	100%	Convient pour usage privé
B	Le disque dur est débité en bandes d'env. 30 mm.	70-80%	Convient pour organisations commerciales
C	Le disque dur est déchiqueté en particules d'env. 300 mm².	30-35%	Convient pour organisations commerciales et pouvoirs publics
D	Le disque dur est déchiqueté en particules d'env. 30 mm².	15-20%	Convient pour données ultra confidentielles chez les pouvoirs publics, etc.
E	Le disque dur est déchiqueté en particules d'env. 10 mm².	0-5%	Convient pour les données les plus confidentielles (classifiées) chez les pouvoirs publics

La DMS 2008 distingue cinq classes de sécurité : A, B, C, D et E

fait sur site, mais les particules vous sont restituées. Les disques durs et leurs débris restent donc sous votre responsabilité et sous votre régime sécuritaire.

NAID AAA

La National Association for Information Destruction, NAID en abrégé, est l'association internationale regroupant les prestataires de services en matière de destruction d'archives, de documents en papier et de disques durs. Les prestataires qui répondent à cette certification exclusive - et fort sévère - peuvent obtenir le certificat NAID AAA. La certification NAID AAA pose des exigences au personnel, aux bâtiments et aux moyens/équipements. Mais elle formule aussi des règles pour la destruction de médias en papier ou imprimés, de microfilms, de disques durs et d'autres porteurs de données que le papier. La NAID pousse la perfection à tel point qu'elle exige le renseignement des numéros de série des disques durs détruits, par exemple, et elle formule aussi des exigences quant à la protection antieffraction et la surveillance par caméras à l'intérieur et autour des bâtiments employés pour la logistique et les opérations de destruction. Et même les véhicules n'échappent pas à la réglementation. Une entreprise qui veut obtenir la certification NAID doit donc satisfaire à toute une batterie d'exigences.

La NAID prescrit une batterie d'exigences et de mesures de sécurité pour l'obtention de la certification.

Destructeurs de documents

Pour la pratique journalière, on a le choix entre différents types de 'shredders'. La plupart des firmes, et de nombreux particuliers aussi, disposent d'un ou de plusieurs destructeurs de documents 'papier' (la destruction de disques durs se fait encore par/dans des firmes spécialisées). Voici les points à considérer lors de l'achat d'un destructeur de documents :

- La machine répond-elle à la norme DIN 66399 ?
- Quelles sont les quantités de papier à détruire ?
- Vous faut-il une machine rapide ou efficace ?
- Combien de déchets aurez-vous à la fin ?
- De combien d'argent disposez-vous ?
- Quel est le niveau de sécurité de la machine ?
- Dimensions de coupe; coupe croisée (particules) ou en bandes ?
- Largeur de coupe de la machine ?
- Capacité de la machine ?

En pratique, on constate plus d'une fois qu'il y a un manque d'accord entre l'analyse des risques et la machine achetée. Les destructeurs de documents sont régulièrement la cause de problèmes divers : nuisances sonores, poussière, manque de capacité. Bien souvent aussi, il faut enlever agrafes et trombones avant de passer les feuilles dans la machine.

Sous-traitance

Votre organisation peut, si vous le voulez, sous-traiter la collecte et la destruction d'anciens papiers à des firmes spécialisées. La collecte et le tri se font sur site, par exemple à l'aide de conteneurs fermés dans lesquels on peut déposer, via une ouverture style 'boîte aux lettres' les documents à détruire. Ces conteneurs sont régulièrement vidés. Les firmes spécialisées offrant ces services sont certifiées par la Federatie Nederlandse OudpapierIndustrie (FNOI), aux Pays-Bas du moins. La FNOI est l'association professionnelle de l'industrie de recyclage du papier et est en

Après avoir passé l'audit avec succès, la firme en question est en droit d'employer le logo CA+.

Classe de protection et taille max. des particules pour données P, F, O, T et H													
		P papier	Max (mm2)	F Flim	Max (mm2)	O (optique)	Max (mm2)	T (magnétique)	Max (mm2)	H (HHD)	MAX (mm2)	E (électronique	Max (mm2)
Classe 1		P-1	2000	F-1	160	O-1	2000	T-1	hors d'état de fonctionner	H-1	hors d'état de fonctionner	E-1	hors d'état de fonctionner
		P-2	800	F-2	30	O-2	800	T-2	diviser et 2000	H-2	endommagé	E-2	diviser
	Classe 2	P-3	320	F-3	10	O-3	160	T-3	320	H-3	déformer	E-3	160
		P-4	160	F-4	2,5	O-4	30	T-4	160	H-4	2000	E-4	30
	Classe 3	P-5	30	F-5	1	O-5	10	T-5	30	H-5	320	E-5	10
		P-6	10	F-6	0,5	O-6	5	T-6	10	H-6	10	E-6	1
		P-7	5	F-7	0,2	O-7	0,2	T-7	2,5	H-7	5	E-7	0,5
si mélangé et en ballots d'au moins 1000kg, le niveau de sécurité monte d'1 unité													

droit d'accorder les certifications CA+.

Cette réglementation inclut des normes et procédures objectives devant assurer la confidentialité des données à détruire et la sécurité du processus. Elle garantit un processus de destruction adéquat, efficace et bouclé. La certification CA+ répond aux normes reconnues en matière de destruction d'archives, telles que la DIN 66399 allemande et la NAID AAA Certification américaine.

Le Certificat CA+ est accordé après audit du processus complet, de la collecte et du transport jusqu'à la destruction des documents confidentiels. Le schéma de certification couvre les aspects suivants : procédures de proposition/exigences pour moyens de collecte, sécurisation du transport, déchargement/transfert, exigences pour locaux de destruction, procédures/instructions/directives de travail, screening du personnel. Après avoir passé l'audit avec succès, la firme en question est en droit d'employer le logo CA+.

Conclusion

Les cadres et collaborateurs d'une organisation doivent être conscients du fait que le cycle de vie des porteurs de données est limité. Ils doivent disposer de procédures claires quant à leur destruction sécurisée. Cet article décrit en grandes lignes les systèmes de certification concernés, tant en Belgique qu'aux Pays-Bas.

Avant de passer à l'achat d'un équipement de destruction ou d'envisager une sous-traitance, il faut procéder à un inventaire des risques. Toute entreprise ou organisation doit également introduire un système de classification de l'information. Il s'agit ici de pouvoir déterminer le degré de sécurisation correspondant à chaque type d'information, en fonction de son degré de sensibilité ou de confidentialité. Cette classification a un impact sur le cycle de vie de l'information et sur la façon d'y mettre fin dans un cadre règlementé.

L'introduction d'un tel système de classification n'est pas une sinécure : elle peut prendre plusieurs mois. Bien sûr, cette introduction se base sur un modèle de croissance, qui commence à la source même de l'information.

Il faut que les personnes qui créent l'information sachent qu'elles doivent en déterminer et maintenir la classification, bien sûr dans les limites de la politique d'entreprise relative à leur destruction, entre autres. Bref : la destruction de données doit faire partie intégrante de la politique d'entreprise en matière de sécurisation de l'information.

(Par Ronald Eygendaal)

www.eygendaals.nl