Fysieke vernietiging van gegevensdragers

Voorkom boetes

Diefstal van gevoelige informatie (= bedrijfsspionage) kan zeer schadelijk zijn voor organisaties. Informatie die in verkeerde handen terechtkomt kan het faillissement betekenen voor organisaties, mensen werkloos maken en aandeelhouders en families verwoesten. Ook kan informatie beursgevoelig zijn (voorkennis is strafbaar!). Maar ook het veilig gebruik en de opslag van persoonsgegevens worden steeds belangrijker. De privacy van burgers wordt meer en meer omkaderd door de wet en regelgeving. Op het uitlekken van privacygevoelige informatie staan hoge boetes.

In vooral de wat grotere document- en kennisintensieve organisaties gaan grote hoeveelheden informatiestromen heen en weer. Dit in de vorm van memo's, verslagen, rapporten, USB-sticks, cd-roms, tapes en andere gegevensdragers. Hierdoor worden de beveiliging van opslag, transport en vernietiging van gegevens steeds belangrijker. Dit artikel gaat voornamelijk over gegevensdragers die hun levenscyclus hebben doorlopen en moeten worden vernietigd.

De DIN 66399

De DIN 66399 is sinds 2010 de norm voor vernietiging van gegevensdragers. Het is een allesomvattende industrienorm voor het shredderen en/of vernietigen van alle soorten gegevensdragers. DIN 66399 beschrijft naast de principes en definities van gegevensdragers ook de vereisten voor apparatuur voor de vernietiging van gegevensdragers en geeft richtlijnen en regels voor het proces van het vernietigen van gegevensdragers. DIN 66399 is ontwikkeld door het DIN (Deutsches Institut für Normung) in samenwerking met industrie en stakeholders. De DIN 66399 is de opvolger van de alom bekende DIN 32757. Naast de DIN66399 is de Praktijkrichtlijn NEN-EN 15713:2009 “Zekere vernietiging van vertrouwelijk materiaal” nog steeds van toepassing. Echter de NEN-EN 15713:2009 kent een aantal vage bepalingen. De DIN 66399 verduidelijkt deze vaagheden. Zo kunnen gegevensdragers die aan het einde van hun levenscyclus zijn, het beste worden vernietigd met een vernietiger, ook wel shredder genoemd. Fijn is vaak niet fijn genoeg, daarom is het belangrijk dat met behulp van een risico-inventarisatie de veiligheidsfactor van de gegevensdragers wordt bepaald. Geclassificeerde gegevensdragers dienen volgens voorgeschreven normen vernietigd

Veiligheidsniveau	Data	Reproduceren
1	Algemene data	Verlangt eenvoudige inspanning
2	Interne data	Verlangt speciale inspanning
3	Gevoelige data	Verlangt aanmerkelijke inspanning
4	Hoogst gevoelige data	Verlangt uitzonderlijke inspanning
5	Geheime data	Verlangt verregaande methodes
6	Hoogst geheime data	Is technisch onmogelijk
7	Top secret data	Is onmogelijk

DIN 66399 kent zeven veiligheidsniveaus. Het veiligheidsniveau zegt iets over de data en de reproduceerbaarheid. Het veiligheidsniveau, dat een shredder produceert, hangt af van de snijwalsen in de vernietiger.

Materiaalclassificatie	Informatie	Voorbeelden	Veiligheidsniveaus
P	Originele grootte	Papier, Films, Drukplaten	P-1 tot P-7
F	Gereduceerd/ geminimaliseerd	Microfilms	F-1 tot F-7
O	Optische Datadragers	Cd's, dvd's, BluRays	O-1 tot O-7
T	Magnetische Datadragers	Tapes, ID Cards, Floppy Disks	T-1 tot T-7
H	Hard Disk Drives	Hard Disk Drives	H-1 tot H-7
E	Elektronische Datadragers	USB-sticks, Chip Cards, Mobiele communicatie apparaten	E-1 tot E-7

De 66399 kent materiaalclassificaties ten aanzien van de te vernietigen gegevensdrager. Het materiaal waarvan de gegevensdrager is gemaakt is immers van invloed op de reproduceerbaarheid. De DIN 66399 kent de volgende materiaalclassificatie van gegevensdragers.

te worden. Naarmate de inhoud van de te vernietigen gegevensdragers belangrijker wordt, moet ook de output na vernietiging kleiner zijn. Hierdoor neemt de tijd voor reproduceerbaarheid af. De DIN 66399 kent een drietal beschermingsklassen:

1. Is voor normale bescherming van interne data waarbij openbaring een negatieve invloed zou hebben op een bedrijf of een risico op identiteitsfraude bij een persoon.
2. Is voor hogere bescherming van vertrouwelijke gegevens waarbij openbaring een aanzienlijk negatieve invloed zou hebben op een bedrijf, schending van een wettelijke verplichting of een risico.
3. Is voor zeer hoge beveiliging voor vertrouwelijke en Top Secret gegevens waarbij openbaring gevolgen kan hebben op het voortbestaan van een bedrijf of overheid, of een risico op het gebied van gezondheid, veiligheid of persoonlijke vrijheid van een persoon op een nadelige sociale of financiële status van een individu kan opleveren.

DIN 66399 kent zeven veiligheidsniveaus. Het veiligheidsniveau zegt iets over de data en de reproduceerbaarheid. Het veiligheidsniveau, dat een shredder produceert, hangt af van de snijwalsen in de vernietiger.

De 66399 kent materiaalclassificaties ten aanzien van de te vernietigen gegevensdrager. Het materiaal waarvan de gegevensdrager is gemaakt is immers van invloed op de reproduceerbaarheid. De DIN 66399 kent de volgende materiaalclassificatie van gegevensdragers.
Zoals eerder beschreven: de DIN 66399 is een allesomvattende industrienorm en beschrijft de hele procesketen, van de inzamelcontainer, het transport en de opslag tot en met de daadwerkelijke vernietiging. In het procesdeel komen de volgende onderwerpen aan bod: organisatie, personeel, inzameling/ opslag/ transport, transport, vernietiging.

Zo dienen alle medewerkers die toegang hebben tot de shredderruimte een geheimhoudingsverklaring te hebben ondertekend en moeten bezoekers tijdens het verblijf in de shredderruimte worden begeleid door een medewerker. Uiteraard krijgen de bezoekers een bezoekerspas. Ook dient de ruimte waar de nog te vernietigen materialen liggen, voorzien te zijn van inbraakalarm met doormelding naar een alarmcentrale en ook cameratoezicht is voorgeschreven van de DIN 66399. Met betrekking tot het vervoer zijn specifieke eisen vastgelegd in de DIN 66399.

European Association for **Data Media Security ©**

De branchevereniging European Association for Data Media Security, kortweg EA DMS, verenigt een aantal gespecialiseerde bedrijven dat zich bezighoudt met vernietiging van digitale datadragers.

Zo moeten voertuigen uitgerust zijn met een passief GPS tracking systeem en/of dienen ze bemand te worden met minimaal twee medewerkers. Ook dient men gebruik te maken van voertuigen met een gesloten en vaste opbouw. Tenslotte dienen ook de machines die gebruikt worden voor de vernietiging te voldoen aan de DIN 66399-1. Kortom aan alles is gedacht en beschreven in de DIN 66399 anders dan in de DMS 2008 standaard daarover later meer.

EA DMS

De branchevereniging European Association for Data Media Security, kortweg EA DMS, verenigt een aantal gespecialiseerde bedrijven dat zich bezighoudt met vernietiging van digitale datadragers. Daarbij moet men denken aan bedrijven uit Duitsland, België en Nederland.

De EA DMS heeft zijn eigen branchecertificering ontwikkeld met als uitgangspunt dat het "om een eenvoudige veilige methode voor de selectie en controle van de gekozen veiligheidsstandaard gaat- waarbij zonder technische hulpmiddelen of uitzonderlijke kennis - deze gewoon voor eenieder goed te gebruiken is." Vanuit dit uitgangspunt is de DMS 2008 ontstaan.

De DMS 2008 geeft duidelijke en transparante richtlijnen voor de veilige afvoer van harddisks (HDD's). In tegenstelling tot de DIN 66399 beschrijft de DMS 2008 uitsluitend de eisen voor een veilige afvoer van harddisks. Daarom is de DMS 2008 ▶▶

Veiligheidsklasse	Methode	Recover mogelijkheid	Doel
A	De harde schijf wordt vernietigd in circa 50 mm stroken.	100%	Geschikt voor privé personen
B	De harde schijf wordt vernietigd in circa 30 mm stroken.	70-80%	Geschikt voor commerciële organisaties
C	De harde schijf wordt vernietigd in deeltjes van circa 300 mm².	30-35%	Geschikt voor commerciële- en overheidsorganisaties
D	De harde schijf wordt vernietigd in deeltjes van circa 30 mm².	15-20%	Geschikt voor hoog gevoelige data bij overheid, etc
E	De harde schijf wordt vernietigd in deeltjes van circa 10 mm².	0-5%	Geschikt voor de meest hooggevoelige (geclassificeerde) data bij overheid

De DMS 2008 kent vijf veiligheidsklassen: A, B, C, D en E.

uitstekend geschikt om de snijmachines en/of persen te certificeren. De DMS 2008 kent vijf veiligheidsklassen: A, B, C, D en E.

De conform DMS 2008 gecertificeerde bedrijven rijden veelal rond met transportbusjes met daarin een mobile shredder. In het geval dat u harddisks ter vernietiging heeft komen zij naar u toe en parkeren hun transportbusje bij u voor de deur. Ter plaatsen shredderen zij uw harddisks, waarna u de vernietigde en verpulverde retour krijgt. De harddisk en het restmateriaal blijven dus onder uw toezicht en beveiligingsregiem.

NAID AAA

De National Association for Information Destruction of kortweg de NAID, is de internationale overkoepelende vereniging van dienstverleners op het gebied van archiefvernietiging, papiervernietiging en harde schijf vernietiging.

Dienstverleners die aan de exclusieve en strenge certificeringsregeling voldoen, kunnen het NAID AAA-certificaat verkrijgen. Zo stelt de NAID AAA eisen aan het personeel, de gebouwen en middelen. Maar ook stelt de NAID regels ten aanzien van de vernietiging van papier en geprinte media, microfilms, harde schijven en overige niet papieren media. De NAID gaat zelfs zover dat de serienummers van bijvoorbeeld de te vernietigen harde schijven moeten worden bijgehouden. Ook stelt de NAID eisen met betrekking tot inbraakdetectie en cameratoezicht in en rond de gebouwen die gebruikt worden voor de logistiek en vernietiging. Maar ook de voertuigen dienen aan regels te voldoen. Kortom de NAID schrijft een heel stelsel van eisen en beveiligingsmaatregelen voor, wanneer een bedrijf de certificering wil behalen.

De NAID schrijft een heel stelsel van eisen en beveiligingsmaatregelen voor met het oog op het behalen van de certificering.

Papiervernietigers

In de dagelijks praktijk komen we verschillende shredders tegen. Veel bedrijven, maar tegenwoordig ook veel particulieren hebben papiervernietigers staan. (Het vernietigingen van harde schijven gebeurt echter nog steeds bij daartoe gespecialiseerde bedrijven.) Omdat bedrijven vaak zelf papier- vernietigers aanschaffen zijn er de volgende overwegingen die kunnen worden gebruikt bij de keuzen van papiervernietigers:

- Voldoet de shredder aan de DIN 66399?
- Om welke hoeveelheden te vernietigen materiaal gaat het?
- Is er een snelle of een grondig versnipperaar nodig?
- Hoeveel afval ontstaat er?
- Hoeveel geld is er beschikbaar?
- Het veiligheidsniveau van de machine?
- De versnipperingsmaat; cross-cut (snippers) of stroken.
- De verwerkingsbreedte van de machine?
- De capaciteit van de machine?

In de praktijk zien we vaak een mismatch tussen de risico-inventarisatie en de aangeschafte shredder. In de dagelijkse praktijk geven papiervernietigers nogal eens wat problemen. De apparaten veroorzaken veel herrie en stof en vaak is de capaciteit beperkt. Vaak dienen paperclips, nietjes en dergelijke verwijderd te worden voordat het papier de shredder in kan.

Uitbesteden

Als organisatie kunt u het verzamelen en vernietigen van papier uitbesteden aan

Na een geslaagde audit mogen gespecialiseerde bedrijven het CA+ logo gebruiken.

Beschermingsklasse en max snippergrootte voor P, F,O,T, H en E gegevens													
			P papier	Max (mm2)	F Flim	Max (mm2)	O (optisch)	Max (mm2)	T (magnetisch)	Max (mm2)	H (HHD)	MAX (mm2)	E (Elektronsich	Max (mm2)
klasse 1			P-1	2000	F-1	160	O-1	2000	T-1	onbruikbaar	H-1	onbruikbaar	E-1	onbruikbaar
			P-2	800	F-2	30	O-2	800	T-2	splijten en 2000	H-2	beschadigd	E-2	splijten
	klasse 2		P-3	320	F-3	10	O-3	160	T-3	320	H-3	vervormen	E-3	160
		klasse 3	P-4	160	F-4	2,5	O-4	30	T-4	160	H-4	2000	E-4	30
			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
Bij vermengen en balen van min. 100 KG één veiligheidsniveau omhoog.														

daartoe gespecialiseerde bedrijven. Zij doen dit door inzameling en sortering van papier binnen uw organisatie. Hierbij kan worden gedacht aan het plaatsen van geheel afgesloten containers waar men het papier via een brievenbussleuf in kan gooien. Deze afgesloten containers worden regelmatig geleegd en de inhoud wordt afgevoerd en vernietigd. De gespecialiseerde bedrijven die deze dienstverlening aanbieden zijn gecertificeerd door de Federatie Nederlandse OudpapierIndustrie (FNOI). De FNOI is de brancheorganisatie voor de oud papier industrie en is de eigenaar van de CA+ certificeringsregeling.

De regeling bevat objectieve normen en procedures om de vertrouwelijkheid van het te vernietigen materiaal en de veiligheid van de procedures te waarborgen. De regeling waarborgt tevens een adequaat, efficiënt en gesloten vernietigingsproces. De certificeringregeling CA+ sluit aan op erkende normeringen voor archiefvernietiging, zoals de Duitse DIN 66399 en de Amerikaanse NAID AAA Certification.

Het Certificaat CA+ wordt afgegeven na een geslaagde audit, indien het hele proces van inzameling/transport tot en met vernietiging van het vertrouwelijk materiaal voldoet aan de eisen van de regeling. Het certificatieschema kent de volgende toetsingsonderdelen: procedures aanbieden/eisen inzamelmiddelen, beveiliging transport, lossen/overdracht, eisen archiefvernietigingsruimte, procedures/instructies/werkvoorschriften, screening personeel. Na een geslaagde audit mogen gespecialiseerde bedrijven het CA+ logo gebruiken.

Conclusie

Medewerkers en directieleden van een organisatie moeten zich bewust worden van de levenscyclus van gegevensdragers. Zo moeten er duidelijke procedures zijn over hoe om te gaan met informatie die aan het einde van zijn levenscyclus is gekomen. Dit artikel beschrijft in grote lijnen de meest gebruikte types van certificering voor vernietiging van gegevensdragers binnen België en Nederland.
Voorafgaande aan de aanschaf of bij het uitbesteden van papiervernietiging of de vernietiging van gegevensdragers moet een risico-inventarisatie worden gemaakt. Daarnaast zal de organisatie een informatieclassificatiesysteem moeten invoeren. Het gaat daarbij immers om de juiste mate van beveiliging, die past bij de risico's die de informatie loopt. Classificatie van informatie geeft een inschatting van de gevoeligheid en het belang van de informatie en de daarbij horende graad van beveiliging. Classificatie levert zodoende een bijdrage aan de levenscyclus van informatie en de vorm van beveiliging van deze informatie.
Het invoeren van een informatieclassificatiesysteem is geen sinecure en kost een organisatie een aantal maanden. Uiteraard is de invoering een groeimodel, dat begint bij de bron van informatie.

Mensen die informatie creëren moeten zich bewust worden van het feit dat zij de classificatie bepalen en handhaven, uiteraard binnen de daartoe uitgezette beleidsrichtlijnen ook ten aanzien van vernietiging. Kortom: gegevensvernietiging hoort een integraal onderdeel te zijn van het bedrijfsbeleid en het informatiebeveiligingsbeleid in het bijzonder.

(Door Ronald Eygendaal)

www.eygendaals.nl