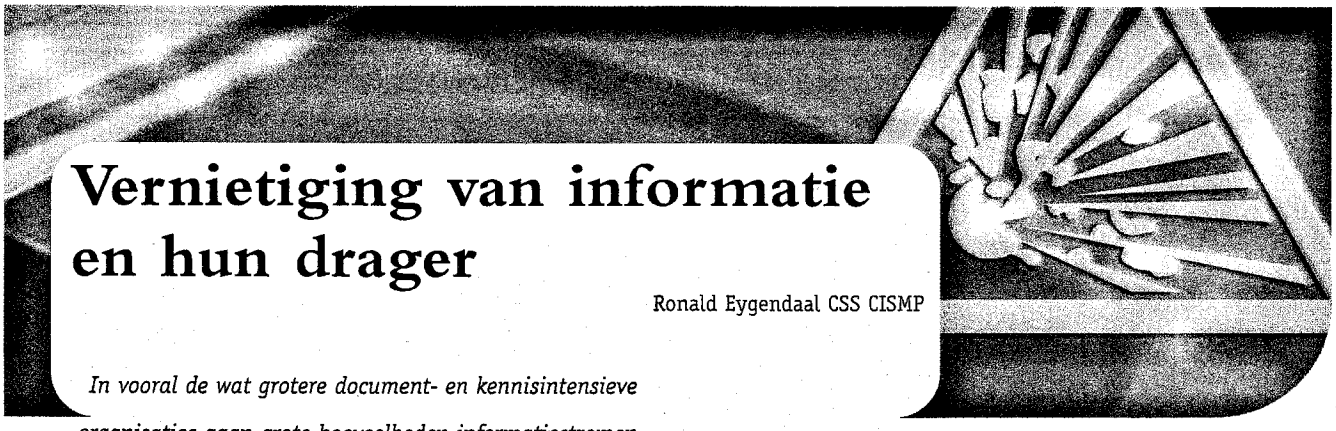
involving a system of internal controls and encourages the deployment of an internal audit function. BS 7799 Part 2 requires (a) a risk assessment process to be in place (Plan Phase); (b) a system of internal ISMS controls to be in place to manage the applicable risks (Do Phase); (c) a management review process to be employed to verify effectiveness of these controls (Check Phase) and (d) a process to implement any necessary actions to improve the system of controls (Act Phase). Information security and any information security management system (ISMS) should naturally form an integrated part of the Corporate Governance risk management process and procedures.

2002 Editing Group

The editing and development group for the newly revised BS 7799 Part 2 includes representatives from the International User Group (IUG) and the following organisations and the following individuals:

Adacel (Australia)	KPMG (UK)
Angelika Plate, AEXIS Security Consultants (Germany)	William List (UK)
Articsoft (UK)	LCH (UK)
Rune Ask (Norway)	Logica UK Ltd (UK)
British Telecom (UK)	LRQA Ltd (UK)
BSI Management Systems (UK)	NSAI (Ireland)
DNV (Norway)	PCCW (Hong Kong)
DTI (UK)	PNP (Korea)
EDS (UK)	PSB Certification (Singapore)
Ariosto Farias Jr (Brazil)	QinetiQ (UK)
Gamma Secure Systems Ltd (UK)	S Cube (Korea)
ING Bank (Netherlands)	SIS (Sweden)
JQA (Japan)	Swedac (Sweden)
KDDI (Japan)	Validation AB (Sweden)
	XiSEC Consultants Ltd (UK)



Vernietiging van informatie en hun drager

Ronald Eygendaal CSS CISMP

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, diskettes, cd-roms, tapes en andere informatiedragers.

Diefstal van gevoelige informatie (een vorm van bedrijfsspionage) kan zeer schadelijk zijn voor organisaties. Informatie die in de verkeerde handen valt kan organisaties failliet laten gaan, mensen werkloos maken en aandeelhouders en families verwoesten. Ook kan informatie beursgevoelig zijn (voorkennis is strafbaar).

Beveiliging van opslag, transport en vernietiging van informatie is dus belangrijk. Dit artikel gaat voornamelijk over informatie die zijn levenscyclus heeft doorlopen en moet worden vernietigd

<Over de auteur> Ronald Eygendaal is werkzaam als Senior consultant voor Aranea, heeft meer dan 10 jaar ervaring in beveiliging en informatiebeveiliging in het bijzonder; is voorzitter van de vakgroep ICT beveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN); lid van het International Advisory Board van de International Foundation for Protection Officers (IFPO), is Certified Security Supervisor (CSS) en Certificate in Information Security Management Principles (CISMP).

Dumpster Diving

Naast de bekende scenario's, waaronder de fysieke diefstal van informatiedragers door derden valt, is er een minder bekende techniek genaamd Dumpster Diving. Dumpster Diving is een techniek om informatie over een bepaalde organisatie te verzamelen. In feite is Dumpster Diving het doorzoeken van het afval van een bepaalde organisatie om zodoende waardevolle informatie te verzamelen. Het gaat dus om fysieke informatiedragers zoals papier, diskettes, cd-roms, tapes en videobanden welke ongeautoriseerd zijn weggegooid.

Een methode om een organisatie te beveiligen tegen Dumpster Diving is de informatiestroom binnen een organisatie goed te regelen. Vaak wordt dit gedaan via de zogenaamde informatie classificatie. Informatie krijgt dus een kenmerk dat iets weergeeft over de omgang met desbetreffende informatie.

Wat vaak wordt vergeten is hoe een organisatie moet omgaan met informatiedragers die hun levenscyclus hebben doorlopen. Informatie die bijvoorbeeld op papier staat, mag niet zomaar in de prullenbak of oud papier bak worden gedaan. Maar ook de oude videobanden van het CCTV-systeem mogen niet zomaar weggegooid worden. Er kunnen immers nog beelden opstaan die personen of organisaties schade kunnen toebrengen. Als we de controle op de informatiedragers verliezen dan kunnen we slachtoffer worden van Dumpster Diving.

Papiervernietigers

Kleine hoeveelheden papieren informatie die aan het einde van hun levenscyclus zijn, kunnen het beste worden vernietigd met een papiervernietiger, 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 papieren informatie wordt bepaald. Geclassificeerde papieren informatie dient volgens voorgeschreven normen vernietigd te worden. Naarmate de inhoud van de te vernietigen papieren belangrijker wordt, moet ook de output na vernietiging kleiner zijn. Output van papiervernietigers varieert van stroken tot snippers in diverse maten.
Het gebruik van papiervernietigers met stroken brengt risico's met zich mee. Als de output van de vernietiger in de vorm van stroken is, moeten de documenten altijd haaks op de leesrichting vernietigd worden.

Hoe hoger de vertrouwelijkheid des te kleiner dient de snipper of strook te zijn. Naast de snippergrootte en de oppervlakte is het soort gegevensdrager van belang. Naast papier zijn er ook andere bedrukte gegevensdragers zoals film, microfilm en kunststof.

Deutsches Institut Normung

Het Deutsches Institut für Normung (DIN) in Berlijn, heeft een norm vastgesteld waarbij de veiligheid van vernietigd materiaal geclassificeerd wordt. Deze norm, de DIN 32757, wordt internationaal erkend en gehanteerd. In 1995 is de norm aangepast en is de oppervlakte van de snipper en/of strook mede bepalend voor de veiligheidsfactor. Dit is aangegeven in de DIN 32 757-1:1995-01. Naast papier gaat de DIN 32757 uit van film, microfilms en kunststof, waarbij bij de laatste gedacht moet worden aan ID-kaarten.

Overeenkomstig DIN 32757-1 bestaat deze 'kwaliteit' in 5 verschillende veiligheidsfactoren:

				
veiligheidsfactor 1	**veiligheidsfactor 2**	**veiligheidsfactor 3**	**veiligheidsfactor 4**	**veiligheidsfactor 5**
stroken 10,5 mm snippers 10,5x40-80 mm	stroken 3,9-5,8 mm	stroken 1,9 mm snippers 3,9x30-50 mm	snippers 1,9x15 mm	snippers 0,78X11 mm
maximale oppervlakte van de snipper cq strook 1000mm²	maximale oppervlakte van de strook 400mm²	maximale oppervlakte van de snipper cq strook 1mm²	maximale oppervlakte van de snipper 0,5mm²	maximale oppervlakte van de snipper 0,2mm²
toepassing: papier film	toepassing: papier film	toepassing: papier film microfilm kunststof	toepassing: papier film microfilm kunststof	toepassing: papier film microfilm kunststof

Europese banken hanteren veiligheidsfactor van 3 of hoger. Ook voor het vernietigen van persoonsgegevens wordt veiligheidsfactor van 3 of hoger gehanteerd. Deze werkwijze is op grond van de Wet Bescherming Persoonsgegevens goedgekeurd door het College Bescherming Persoonsgegevens in Den Haag.

Aanschaf papiervernietiger

Bij de keuze van een papiervernietiger moeten de volgende overwegingen worden gemaakt:

- Om welke hoeveelheden papier gaat het?
- Is er een snelle of juist een grondige versnipperaar nodig?
- Hoeveel afval ontstaat er?
- Hoeveel geld is er beschikbaar?
- Wat is het veiligheidsniveau van de machine?
- De versnipperingsmaat, cross-cut (snippers) of stroken.
- De verwerkingsbreedte van de machine?
- De capaciteit van de machine

Magnetische gegevensdragers

Ook via diskettes, datatapes, videobanden en andere magnetische gegevensdragers kan informatie 'lekken'. Wanneer deze gegevensdragers aan het eind van hun levenscyclus zijn, is een van de mogelijke alternatieven het demagnetiseren van de magnetische gegevensdragers. Uit onderzoek is bekend dat het zelfs mogelijk is om hardschijven met aluminium behuizing te demagnetiseren. Het demagnetiseren gebeurd met een degausser.

Retentivity en Coercivity

Magnetische gegevensdragers hebben een aantal eigenschappen. De belangrijkste eigenschappen voor het proces van informatievernietiging zijn Retentivity en Coercivity.

Onder Retentivity wordt de capaciteit om magnetisme te bewaren nadat de externe magnetische kracht verwijderd is verstaan. De hoeveelheid energie die nodig is om een opgenomen signaal volledig te wissen wordt Coercivity genoemd. Hoe hoger de Coercivity hoe beter want dit heeft een positieve invloed op de Retentivity, zou men zeggen. Op zich is dat juist maar bij informatievernietigingsprocessen is dit een nadeel. Het zal duidelijk zijn dat elke magnetische gegevensdrager zijn eigen Coercivity heeft en men dus ook anders moet degaussen.

Typical Media Coercivity Figures

Medium	Coercivity
5.25" 360K floppy disk	300 Oersteds
5.25" 1.2M floppy disk	675 Oersteds
3.5" 720K floppy disk	300 Oersteds
3.5" 1.44M floppy disk	700 Oersteds
3.5" 2.88M floppy disk	750 Oersteds
3.5" 21M floptical disk	750 Oersteds
Older (1980's) hard disks	900-1400 Oersteds
Newer (1990's) hard disks	1400-2200 Oersteds
1/2" magnetic tape	300 Oersteds
1/4" QIC tape	550 Oersteds
8 mm metallic particle tape	1500 Oersteds
DAT metallic particle tape	1500 Oersteds

De hoeveelheid energie die nodig is om magnetische informatie te (her)schrijven of te wissen, wordt uitgedrukt in Oersted. Voor het degaussen van een magnetische gegevensdrager is een drie tot vier keer zo groot magneetveld nodig (in Oersteds) als de maximum Coërciviteitswaarde van de magnetische gegevensdrager.

SEAP, DIN & DOD

Het Security Equipment Assessment Panel (SEAP) is, als Britse overheidsorganisatie, verantwoordelijk voor de beveiliging van overheidseigendommen. In 1997 heeft het SEAP een Britse overheidsstandaard gepubliceerd voor het veilig wissen en vernietigingen van informatie en data bewaard op magnetische gegevensdragers. Deze Britse overheidsstandaard de SEAP 8500 Specification Degaussers beschrijft een viertal wis- en vernietigingsklasse.

Ook op dit gebied heeft het Deutsches Institut für Normung (DIN) in Berlijn een norm vastgesteld. Het gaat dan om Norm DIN 33858 Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern.

Het Amerikaanse ministerie van Defensie (DOD) heeft in de zeventiger jaren de DOD-Manual 5200.28M uitgegeven. Hierin heeft men een indeling gemaakt waarbij het degauslevel en het type tape beschreven staan. Andere Amerikaanse normen zoals de Air Force Regulation AFSSI-5020 en Army Regulation 380/19 zijn hier van afgeleid.

Computerbestanden

Het verwijderen van computerbestanden lijkt zo gemakkelijk, je sleept het bestand naar de prullenbak en weg is het. Schijn bedriegt. Met wat recovery tools, in ruime mate op internet verkrijgbaar, is de kans groot dat informatie geheel of gedeeltelijk te achterhalen is. Eigenlijk worden we door Microsoft voor de gek gehouden: weg, informatie is niet weg!

File Allocation Table

De index van een schijf wordt bijgehouden in de FAT (File Allocation Table), ofwel Bestands Toewijzingstabel. Dit is een speciaal gegevensbestand op een schijf (diskette, cd-rom of harde schijf) met de naam, omvang, datum en locatie van alle bestanden op die schijf. Bij het openen van een bestand, kijkt het besturingssysteem in die toewijzingstabel waar het bestand is opgeslagen. Wanneer dan een bestand wordt gewist, dan wordt deze uit de FAT verwijderd. Echter; de plaats waar het werkelijke bestand staat, blijft ongewijzigd en dus benaderbaar, ook zonder FAT.

Bestands Recovery

Door allerlei invloeden zoals mechanische afwijkingen en temperatuurverschillen, schrijft de kop van een harde schijf niet altijd op precies dezelfde plaats op de disk. Hierdoor kan het gebeuren dat bij het wissen van een bestand

de disk-kop een klein beetje naast het originele spoor (of track) schrijft, waardoor het midden van het spoor wel wordt overschreven, maar de rand niet. Met de originele disk-kop zal die rand niet te lezen zijn, maar met een speciale disk-kop is dit geen moeite. Ongeacht hoe vaak een track door de originele disk-kop wordt overgeschreven, het bijna onmogelijk op die rand track komen. Bij diskettes is dit nog moeilijker, omdat deze er op gemaakt zijn om door verschillende disk-koppen te worden beschreven.

Theoretisch is te bepalen hoe vaak (passages) een bestand moet worden overschreven zodat het terughalen van een bestand zo goed als onmogelijk is. Overigens verschillen de deskundigen hierover van mening.

Standaarden

De Gutmann-standaard gaat uit van 35 keer overschrijven, met bepaalde karakters. De meest gebruikte normen is DOD 5220.22M van het Amerikaanse ministerie van Defensie (DOD) en de normen van de NAVO. Volgens de DOD-norm is een procedure met drie overschrijvingen vereist, soms zijn zeven overschrijvingen vereist. Een aantal landen heeft zijn eigen standaarden ontwikkeld. Het gaat binnen dit artikel te ver om al deze standaarden uitgebreid te bespreken. Vandaar een kort overzicht.

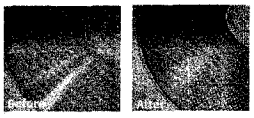
National data destruction standards		
German	VSITR	
Russian	GOST p50739-95.	
American	DoD 5220.22-M	
NAVO	NAVSO P-5239-26 (RLL)	7 of 3 passages
NAVO	NAVSO P-5239-26 (MFM)	

Tapes, diskettes en cd-roms

Er zijn diverse manieren om cd-roms, dvd's, diskettes, dat-tapes en andere gegevensdragers te vernietigingen. In het geval van fysieke vernietigingen moet worden gedacht aan machines die sterk lijken op de traditionele papiervernietiger. De verschillen zitten vooral in de techniek. Hierbij moet worden gedachte aan hardere messen en afwijkende invoermechanisme. De machines die geschikt zijn om cd-roms, dvd's, diskettes, dat-tapes te vernietigen, voldoen over het algemeen aan DIN 32757

Het is een bekend gegeven dat het degaussen van dat-tapes een moeilijk proces is. Dit wordt hoofdzakelijk veroorzaakt door de hoge Coercivity en het gegeven dat voor degaussen een drie tot vier keer hogere waarde nodig is. De fysieke vernietiging van een dat-tape moet dus worden gezien als een serieuze mogelijkheid.

Voor het vernietigingen van cd-roms en dvd's is apparatuur in de handel waarmee de toplaag van de cd-rom en de dvd wordt afgeschuurd. Hierdoor is het met een gewone cd-rom- of dvd-lezer niet meer mogelijk om de vernietigde cd-rom of dvd te lezen.



Alera Technologies

Conclusie

Dumpster Diving is in Nederland een niet verboden bezigheid die kwaadwillenden de mogelijkheid geeft eenvoudig aan informatie over een organisatie te komen.

Medewerkers en directieleden van een organisatie moeten bewust worden van de levenscyclus van informatiedragers. Er moeten duidelijke procedures zijn over hoe om te gaan met informatie die aan het eind van zijn levenscyclus is gekomen. Denk bijvoorbeeld aan het risico van een papiervernietiger die met stroken werkt. Vergeet ook oude videobanden van het CCTV-systeem niet.

Voordat een papiervernietiger, degausser of een ander informatievernietigingsmiddel aangeschaft wordt, moet een risico-inventarisatie worden gemaakt. Ook zal de organisatie een informatieclassificatiesysteem moeten invoeren. Dat invoeren is geen sinecure en het kost een organisatie een paar maanden tijd. Uiteraard is de invoering een groeimodel dat begint 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. Vanuit deze basis is een verdere inbedding van de classificatie nodig in de informatiesystemen, kaartenbakken en eventuele kluizen.

Uiteraard moeten we ook naar de milieuaspecten van de aan te schaffen middelen kijken. Hierbij spelen vragen als: wordt het restafval gescheiden?, is het restafval van een cd-rom chemische afval?

Kortom

informatievernietiging behoort een integraal onderdeel te zijn van het informatiebeveiligingsbeleid.

Http:

www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
www.tno.nl/instit/fel/refs/pub97/afvoer.html
www.aleratec.com/
www.dss.mil/isec/nispom.htm