JOOST MAG HET WETEN

Ronald Eygendaal CSSM CISMP

Op 7 juni 2004 heeft de Amsterdamse officier van justitie Joost Tonino een computer vol vertrouwelijke informatie voor de deur van zijn huis op straat bij het grofvuil gezet. Een passerende taxichauffeur nam de computer mee naar huis en wist het ding moeiteloos aan de praat te krijgen. Vervolgens verkreeg de misdaadverslaggever Peter R. de Vries de computer en printte twee vuistdikke ordners vol vertrouwelijke informatie uit. Het blijkt om zowel justitiële informatie als om privé-informatie te gaan. In een televisie uitzending van 5 mei 2005 blijken de privé-bestanden op de computer van deze (voormalig) officier van justitie Joost Tonino kinderporno te bevatten. Beide onthullingen leidde tot avonden spraakmakende televisie, grote krantenkoppen, Kamervragen en een grote blamage voor Justitie. Dit artikel beschrijft wat Joost en u moeten weten om dit soort knulligheden te voorkomen.

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, zoals in ruime mate op internet verkrijgbaar zijn, is de kans groot dat de informatie geheel of gedeeltelijk te achterhalen is. Eigenlijk worden we door Microsoft voor de gek gehouden, de informatie is dus niet weg!! 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 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. Een beetje software doet de rest.

ECHT WISSEN

Door allerlei invloeden, zoals mechanische afwijkingen en temperatuurverschillen, schrijft de kop van een harde schijf niet altijd op precies dezelfde plaats op de disk. (Hoge temperaturen kunnen schadelijk zijn voor harde schijven.) Hierdoor kan bij het wissen van een bestand gebeuren dat de diskkop 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 diskkop zal die rand niet te lezen zijn, maar met een speciale diskkop is dit geen moeite. Ongeacht hoe vaak een track door de originele diskkop wordt overschreven, het is bijna onmogelijk om op die 'rand track' komen. Bij diskettes is dit nog moeilijker, omdat deze gemaakt zijn om door verschillende diskkoppen 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. Zo gaat de Gutmannstandaard uit van 35 keer overschrijven, met bepaalde karakters. De meest gebruikte normen zijn DOD 5220.22M van het Amerikaanse ministerie van Defensie (DOD) en van de NAVO. Volgens de DOD-norm is

een procedure met drie overschrijvingen vereist, soms zijn zeven overschrijvingen vereist. Een aantal landen heeft hun eigen standaarden ontwikkeld. Het gaat in het kader van dit artikel te ver om al deze standaarden uitgebreid te bespreken. Vandaar een kort overzicht.

National data destruction standards		
German	VSITR	Wisselend overschrijven met 0x00 en 0xFF
Russian	GOST p50739-95.	4 x over schrijven met 0x00
American	DoD 5220.22-M	1 x overschrijven met voorgeschreven waarde 1 x overschrijven met random waarde 1x overschrijven met de waarde uit het eerste spoor
NAVO	NAVSO P-5239-26 (RLL)	7 of 3 x overschrijven
NAVO	NAVSO P-5239-26 (MFM)	7 of 3 x overschrijven

MAGNETISCHE GEGEVENSDRAGERS

Ook via diskettes, datatapes, videobanden en andere magnetische gegevensdragers kan informatie 'lekken'. Wanneer deze gegevensdragers aan het einde 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 gebeurt met een 'degausser'. Het demagnetiseren wordt 'degaussen' genoemd.

RETENTIVITY EN COERCIVITY

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

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

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.

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

Bij magnetische gegevensdragers is het 'degaussen' met een vier keer zo groot magneetveld nodig om alle gegevens echt te verwijderen. Hoog geclassificeerde data wordt op deze wijze hoog geclassificeerd vernietigd.

SEAP, DIN & DOD

Het Security Equipment Assessment Panel (SEAP) is als Britse overheidsorganisatie verantwoordelijk voor de beveiliging van overheidseigendommen. In 1997 heeft de 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 vernietigingsklassen.

Op dit gebied heeft het Deutsches Institut für Normung (DIN) in Berlijn ook 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.

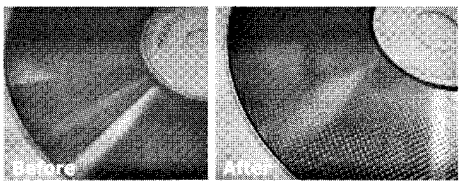
TAPES, DISKETTES EN CD ROMS

Er zijn diverse manieren om CD-ROM's, DVD's, diskettes, DAT-tapes en andere gegevensdragers te vernietigingen. In het geval van fysieke vernietigingen moet worden gedacht aan machines welke sterk lijken op de traditionele papiervernietiger. De verschillen zitten vooral in de techniek. Hierbij moet worden gedacht aan hardere messen en afwijkende invoermechanismen. De machines, welke geschikt zijn om om CD-ROM's, 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-ROM en DVD's is apparatuur in de handel waarmee de toplaag van de CD-ROM en DVD's wordt afgeschuurd. Hierdoor is het met een gewone CD-ROM / DVD-lezer niet meer mogelijk om de vernietigde CD-ROM / DVD te lezen.



Alera Technologies

PAPIERVERNIETIGERS

Kleine hoeveelheden papieren informatie, die aan het einde van zijn levenscyclus is, 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 risicoinventarisatie 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. Bij het vernietigen van teksten, waarbij de output van de vernietiger stroken zijn, 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 welke waardevolle informatie kunnen bevatten.

DEUTSCHES INSTITUT FÜR 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 sindsdien is 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 gedachte moet worden aan ID-kaarten.

In de volksmond is er nog een DIN 32757 level 6 hiermee bedoeld men de Amerikaanse richtlijn NSA/CSS 02-01 ook wel level High Security genoemd. Deze versnippert tot stukjes van 1 x 4 mm. NSA/CSS 02-01 gebruikt men voor het vernietigen van hoog geclassificeerde documenten.

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, aanbevolen door het College Bescherming Persoonsgegevens in Den Haag.

Aanschaf papiervernietiger

Bij de keuzen van papiervernietigers moeten de volgende overwegingen worden gemaakt:

- Om welke hoeveelheden papier gaat het?
- Is er een snelle of een grondige 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

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

veiligheidsfactor 1
stroken 10,5 mm
snippers 10,5X40-80 mm

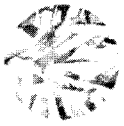
Toepassing
Papier
Film

veiligheidsfactor 2
stroken 3,9-5,8 mm breed

Toepassing
Papier
Film

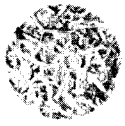
veiligheidsfactor 3
stroken 1,9 mm
snippers 3,9X30-50 mm

Toepassing
Papier
Film
Microfilm
Kunststof



veiligheidsfactor 4
snippers 1,9X15 mm

Toepassing
Papier
Film
Microfilm
Kunststof



veiligheidsfactor 5
snippers 0,78X11 mm

Toepassing
Papier
Film
Microfilm
Kunststof

Dumpster Diving

Dumpster Diving is een techniek om informatie over een bepaalde organisatie of persoon te verzamelen. In feite is 'Dumpster Diving' het doorzoeken van het afval van een bepaalde organisatie en of persoon om zodoende waardevolle informatie te verzamelen (zoals in het geval bij de Amsterdamse officier van justitie Joost Tonino). Het gaat dus om fysieke informatiedragers zoals papier, diskettes, CD-ROM's, tapes, videobanden en zelfs computers welke ongeautoriseerd zijn weggegooid.

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

Want vaak wordt in een organisatie vergeten hoe men om moet gaan met informatiedragers die hun levenscyclus hebben doorlopen. Informatie, welke bijvoorbeeld op papier staat, mag niet zo maar in de prullenbak of oud papierbak 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. Volgende de Wet bescherming persoonsgegevens zijn we zelfs verplicht persoonsgebonden informatie deugdelijk te vernietigen.

Als we de controle op de informatiedragers verliezen dan kunnen we slachtoffers worden van 'Dumpster Diving' en Joost Tonino weet daar alles van.

Conclusie

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

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

Voorafgaande aan de aanschaf van papiervernietigers, degaussers of andere informatievernietigingsmiddelen moet een risicoinventarisatie worden gemaakt. Ook zal de organisatie een informatieclassificatiesysteem moeten invoeren. Het invoeren van een informatieclassificatiesysteem is geen sinecure en kost een organisatie een aantal maanden. Uiteraard is de invoering een groeimodel wat 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. 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 zoals, wordt het restafval gescheiden en is restafval van een CD-ROM chemische afval?

Kortom, informatievernietiging behoort een integraal onderdeel te zijn van het informatiebeveiligingsbeleid.

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