Joost mag het weten

Auteur: Ronald Eygendaal CSSM CISMP > Eygendaal is werkzaam als Senior Security & Fraud Consultant en heeft meer dan 12 jaar ervaring in beveiliging, fraude onderzoeken en informatiebeveiliging in het bijzonder; Eygendaal is voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN); e-mail: ronaldeygendaal@protectioncompany.com.

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 misdaadverslaggever Peter R. De Vries de computer en hij 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 privébestanden op de computer van deze (voormalig) Officier van Justitie kinderporno te bevatten. Beide onthullingen leidden tot avonden spraakmakende televisie, vette krantenkoppen, Kamervragen en een grote blamage voor Justitie. Dit artikel beschrijft wat Joost Tonino en u moeten weten om dit soort zaken 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 deze 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 die we denken te hebben weggegooid, is niet weg, maar wordt bijgehouden in de index van een schijf, 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 nu een bestand wordt gewist,wordt dit uit de FAT verwijderd. Echter de plaats waar het werkelijke bestand staat, blijft ongewijzigd en dus benaderbaar, ook zonder FAT.

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 het 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. Ongeachte hoe vaak een track door de originele diskkop wordt overschreven, het is bijna onmogelijk op die 'rand track' komen. Bij diskettes is dit nog moeilijker, omdat deze gemaakt zijn om door verschillende diskkoppen te worden beschreven.

Bestanden veilig vernietigen

Theoretisch is te bepalen hoe vaak (passages) een bestand moet worden overschreven zodat het terughalen ervan zo goed als onmogelijk is. Overigens verschillen de deskundigen hierover van mening. Zo gaat de Gutmann standaard uit van 35 keer overschrijven, met bepaalde karakters (het aantal overschrijving hangt onder andere af van de karakterpatronen en de volgorde van deze patronen welke voor de overschrijvingen worden gebruikt). De meest gebruikte normen zijn DOD 5220.22M van het Amerikaanse ministerie van Defensie, Department of Defense (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 haar 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	
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)	

Een andere mogelijkheid waarmee het terughalen van bestanden niet eenvoudig uit te voeren is, is het op een degelijke manier versleutelen van bestanden. De zwaktes zitten dan in het key management en zeker zoals bij gebruik van computers in de thuisomgeving.

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 harde schijven met aluminium behuizing te demagnetiseren. Het demagnetiseren gebeurt 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 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. Hoe hoger de Coercivity hoe beter, want dit heeft een positieve invloed op de Retentivity zou men zeggen. Op zich is dit juist, maar in het kader van informatievernietigingsprocessen is dit een nadeel. Het zal duidelijk zijn dat elke magnetische gegevensdrager zijn eigen Coercivity heeft en men dus ook anders moet demagnetiseren (of 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
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.

Ook het Deutsches Institut für Normung (DIN) in Berlijn heeft op dit gebied 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 van de vorige eeuw 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 hiervan afgeleid.

Tapes, diskettes en CD ROMs

Er zijn diverse manieren om CD-ROM's, DVD's, diskettes, DAT tapes en andere gegevensdragers te vernietigen. In het geval van fysieke vernietiging 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 CD-ROM's, DVD's, diskettes en 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's en DVD's is apparatuur in de handel waarmee de toplaag van de CD-ROM's 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 hun levenscyclus zijn, kunnen het best 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. Bij het vernietigen van teksten, waarbij de output van de vernietiger stroken zijn, moeten de documenten altijd haaks op de leesrichting vernietigd worden (hierdoor ontstaat een hogere reconstructietijd).

Hoe hoger de vertrouwelijkheid des te kleiner dient de snipper of strook te zijn. Naast de snippergrootte en het -oppervlak 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 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.

>>

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 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

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 een veiligheidsfactor van 3 of hoger. Ook voor het vernietigen van persoonsgegevens wordt veiligheidsfactor 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 keuze voor een papiervernietiger 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

Uitbesteden

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 e.d. verwijderd te worden alvorens het papier de vernietiger in kan.

Als organisatie kunt u de het verzamelen en vernietigen van papier uitbesteden aan daartoe gespecialiseerde bedrijven. Zij doen dit door reguliere 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 Certificeringsregeling Archief en Datavernietiging. Deze regeling kent 2 Certificaten namelijk: het CA+ certificaat en het CA certificaat.

Het Certificaat CA+ wordt afgegeven na een geslaagde audit, indien het gehele 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

Certificaat CA

Het Certificaat CA wordt afgegeven na een geslaagde audit waarbij volgens vastgelegde normen de volgende onderdelen worden getoetst: de overdracht van het materiaal, de opslag en vernietiging van het vertrouwelijk materiaal. Inzameling en transport naar de vernietigingslocatie worden niet getoetst.

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 van 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 enorme hoeveelheid informatie binnen een organisatie goed te regelen. Vaak wordt dit gedaan via zogenaamde informatieclassificatie. Informatie krijgt dus een kenmerk dat iets weergeeft over de manier van omgaan met de betreffende informatie.

Wat vaak wordt vergeten hoe een organisatie om moet gaan met informatiedragers die hun levenscyclus hebben doorlopen. Informatie die bijvoorbeeld op papier staat, mag niet zomaar 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 slachtoffer worden van Dumpster Diving - Joost weet daar alles van.

Conclusie

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

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

Voorafgaande aan de aanschaf van papiervernietigers, degaussers of andere informatie vernietigingsmiddelen, moet een risico inventarisatie worden gemaakt. Ook zal de organisatie een informatieclassificatiesysteem moeten invoeren. Het invoeren van een informatieclassificatiesysteem is geen sinecure en koste een organisatie geruime tijd. Uiteraard is de invoeringen 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. 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 geschieden en is restafval van CD-ROM's chemische afval?

Kortom informatievernietiging behoort intergraal 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

Over deze rubriek > InZicht geeft een overzicht van recent verschenen en te verschijnen boeken en whitepapers in binnen- en buitenland, geselecteerd door de redactie. Onze bronnen voor de toelichting bestaan uit persberichten en internet, niet gegarandeerd onafhankelijke informatie. Actualiteit staat bij de inhoud van deze rubriek voorop.

Silence on the Wire
A Field Guide to Passive Reconnaissance and Indirect Attacks
Auteur: Michal Zalewski
ISBN: 1-59327-046-1
Uitgeverij: No Starch Press
Vorm: Paperback, 312 pag.
Druk: 1e druk, april 2005

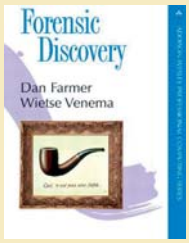
Er zijn vele manieren waarop een potentiële aanvaller informatie kan onderscheppen of meer van de zender kan leren tijdens informatiestromen over een netwerk. Silence on the Wire onthult deze stille aanvallen zodat Administrators zichzelf hiertegen kunnen beschermen en tegelijkertijd monitoring beter zullen doorgronden.
Silence on the Wire ontleedt verschillende unieke en fascinerende security en privacy problemen, welke zijn verbonden met de alledaagse protocollen en technologie zoals we die gebruiken. Deze kennis kan vervolgens ter verdediging ingezet worden.

Whitepaper
Phishing, viruses, bot-nets and more: How to prevent the "Perfect Storm" from devastating your email
Auteur: Postini
Datum: 3 February, 2005
URL: http://www.postini.com/white-papers/?WPID=26

The convergence of newly evolving email attacks is creating a "perfect storm" that threatens to devastate your email systems. This white paper explains these email threats and how you can protect your email system from the impending "perfect storm" in 2005.

Digital Identity
Auteur: Phil Windley
ISBN: 0-596-00878-3
Uitgeverij: O'Reilly
Vorm: Paperback, 264 pag.
Druk: 1e druk, Augustus 2005

De manier waarop zakendoen geschied, is de afgelopen tien jaar drastisch gewijzigd, echter niet altijd ten goede. Het aanbieden van diensten, het uitvoeren van transacties en het on line publiceren van data biedt vele nieuwe kansen. De meeste CTO's en CIO's maken zich echter vooral zorgen, zorgen om de risico's. Hieruit volgt meestal een minder soepel lopende commercie. Sommige bedrijven herzien gelukkig de manier waarop beveiliging wordt aangeboden, zodat interactie met klanten, prospects, werknemers, partners en toeleveranciers zowel rijker als flexibeler wordt. Digital Identity maakt duidelijk hoe hiermee om te gaan. Het concept van Identity Management Architecture (IMA) wordt in detail beschreven. IMA is een coherente en bedrijfsbrede verzameling van standaarden, policies, certificaten en beheeractiviteiten waarmee digitale identiteiten effectief en veilig beheerd kunnen worden.



Forensic Discovery
Auteurs: Dan Farmer, Wietse Venema
ISBN: 020163497X
Uitgeverij: Addison Wesley Professional
Vorm: Paperback, 240 pag.
Druk: 1e druk, december 2004

Uw vingerafdrukken zitten nu overal op de omslag van dit boek, alleen even oppakken is voldoende! Iedere keer wanneer u uw PC gebruikt laat u sporen achter van het formaat olifant, zelfs mensen met verkeerde bedoelingen wissen zelden alle sporen. Dit boek gaat feitelijk over computer archeologie. Het gaat over hetgeen wellicht is geweest, gebaseerd op hetgeen achtergelaten. De auteurs hebben door hun wetenschappelijke en grondige benadering met deze titel het 'guesswork' uit een zeer moeilijk onderwerp weten te halen.