Beleidslijn informatieveiligheid en privacy

Wissen van elektronische informatiedragers

(BLD ERASE)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

In dit document worden de verantwoordelijkheden beschreven van een organisatie inzake het wissen van magnetische (zoals harde schijven of magnetische banden) en niet-magnetische (zoals USB-sticks, CD, DVD of SD-kaarten) informatiedragers waarop professionele, vertrouwelijke of gevoelige informatie zou kunnen staan.

2. Wissen van informatiedragers

Elke organisatie onderschrijft de volgende beleidslijn van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

1. Vercijfering is de preventieve basismaatregel in geval van diefstal, misbruik of verlies van de informatiedrager en is een essentieel element in het bemoeilijken van het eventueel decoderen van de gegevens na het wissen van de drager. Tijdens de levensduur van de informatiedrager, en in het bijzonder voor mobiele informatiedragers, wordt altijd een lokale vercijfering van alle gegevens uitgevoerd aan de hand van een erkend product en met een correct beheer van de encryptiesleutels. De encryptiesleutels mogen nooit aanwezig zijn in een duidelijke vorm op de drager zelf. Deze vercijfering moet betrekking hebben op logische volumes in hun geheel (in plaats van op bestanden of individuele repertoria). Deze vercijfering dient als aanvulling op de toepasbare organisatorische en procedurele maatregelen die er op gericht zijn om misbruiken tegen te gaan.
2. Bij hergebruik wordt de informatiedrager opnieuw gebruikt in een minstens vergelijkbaar data classificatieniveau.
3. Om de gepaste methode[1] te bepalen voor het wissen van een informatiedrager is het noodzakelijk een risico-beoordeling uit te voeren.
4. Wanneer het residuele risico[2] van het terugvinden van de gegevens na het wissen voor de organisatie niet aanvaardbaar is, dan moet de informatiedrager fysiek vernietigd worden, zelfs als het residuele risico hypothetisch is.
5. Wanneer de organisatie informatiedragers gebruikt die geen eigendom zijn (bijvoorbeeld in het kader van leasing of disaster recovery), dan moeten de gepaste maatregelen voor het wissen van gegevens contractueel vastgelegd zijn. Dit geldt ook wanneer de organisatie de technologie niet beheerst voor toegang tot alle niveaus van de informatiedrager (bijvoorbeeld in het kader van cloud computing).

[1] Zie bijlage D

[2] de waarschijnlijkheid dat een negatieve impact zich zal voordoen, ondanks de maatregelen die genomen worden om het (inherent) risico te beïnvloeden (beperken)

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2011		V2011	Eerste versie	21/12/2011	01/01/2012
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISO, “ISO/IEC 27040: 2015 Security techniques – storage security”, januari 2015, 111 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- NIST, “guidelines for media sanitization”, December 2014, 64 blz.

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- http://www.iso.org/iso/iso27001
- https://www.iso.org/standard/54534.html
- https://www.iso.org/standard/54533.html
- https://www.iso.org/standard/44404.html
- https://dban.org/
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- http://www.ccb.belgium.be/nl/documents
- http://www.isaca.org/cobit
- https://www.safeonweb.be/nl
- https://www.cybersimpel.be/nl

Bijlage C: Problematiek van gegevens wissen

De problematiek van het hergebruik van dragers die gevoelige informatie bevatten, is een bijzonder complex onderwerp. Behalve de fysieke vernietiging garandeert geen enkele technische oplossing dat de gegevens volledig gewist zullen worden op een magnetische of andersoortige drager. De werkwijze voor het “wissen” van gegevens bestaat erin op de elektronische dragers één of meerdere reeksen bepaalde of willekeurige karakters te schrijven zodat het achterhalen van de oorspronkelijke gegevens bijzonder moeilijk wordt: de term “overschrijven” is dus geschikter en geeft beter het feit weer dat informatie mogelijk altijd aanwezig is op de drager ten gevolge van de beperkingen van de mechanische schrijfbeveiliging of van het onderliggende algoritme.

In de praktijk is het weinig realistisch te garanderen dat er geen enkel spoor meer gevonden kan worden door laboratoriumonderzoekers met aanzienlijke middelen of met een grondige kennis van hoe dragers werken. Op het vlak van puur magnetisme, buiten het risico op achterblijvende informatiesporen, hebben moderne schijven, die steeds gevarieerder en complexer worden, een groeiend aantal functies (achterhalen van defecte sectoren, maskeren van verdelingen, etc.). Deze dragen ertoe bij dat volledige delen van de schijf niet toegankelijk zijn via standaardcommando’s, terwijl een hacker met kennis van mogelijke specifieke commando’s van de fabrikant of met geschikte hardware de opgeslagen gegevens op de schijf kan achterhalen.

Hoewel de gebruikte technologieën verschillend zijn, heeft het gebruik van een product gebaseerd op een logische overschrijving voor het vernietigen van gegevens op een niet magnetische drager (USB-sticks, geheugenkaarten, Flash-geheugens) strikt genomen dezelfde beperkingen.

De instellingen zouden moeten eisen dat alle gegevens van digitale dragers verwijderd worden vooraleer deze ontmanteld, hergebruikt (intern of extern) of hersteld worden. Jammer genoeg is dit niet altijd mogelijk wanneer het apparaat defect is. Om het even wie met de nodige laboratoriuminstrumenten zou de opgeslagen gegevens kunnen achterhalen. Een risico-beoordeling moet uitgevoerd worden voor elk geval. Bovendien moet er rekening gehouden worden met de waarde van de gegevens en de mogelijke gevolgen van de verspreiding ervan. Als het risico gemiddeld of hoog is, moet de instelling zich ervan vergewissen dat de drager onder haar controle blijft. Anders dient de instelling de drager te vernietigen volgens de goedgekeurde vernietigingsmethodes.

Bijlage D: Methodes voor vercijferen, vernietigen of wissen van informatiedragers

2.1. Vercijfering

De voorafgaande encryptie van de gegevens vermindert aanzienlijk het risico op het compromitteren van professionele, vertrouwelijke en gevoelige gegevens zelfs al is niet alle informatie op de informatiedrager volledig verwijderd. Het is bijgevolg het voornaamste technische middel om de impact van een diefstal, misbruik of verlies te beperken. De overschrijving op het einde van de levenscyclus wordt altijd aanbevolen. De vercijfering kan de bescherming van de gegevens slechts gedurende een bepaalde periode waarborgen ten gevolge van de evoluerende technologieën. Deze oplossingen hebben meestal inherente beperkingen zoals het risico op een zwak wachtwoord/wachtzin dat de sleutel beveiligt, het bestaan van niet vercijferde gegevens in de tijdelijke bestanden van de tools of het besturingssysteem, de aanwezigheid van geheugensleutels.

De efficiëntie van encryptie voor wat de permanente beveiliging van gegevens betreft, berust op drie factoren: de sterkte van het encryptiebeveiligingsschema dat toegepast wordt, de kwaliteit van het beheer van de encryptiesleutel door de gebruiker en het vermijden van hacker incentives. Bij tijd en gelegenheid kan een competente hacker de gegevens terughalen als hij voldoende gemotiveerd is om de nodige inspanningen te leveren. De encryptiemethodes moeten voldoende afraden en ervoor zorgen dat de nodige inspanningen om de gegevens te achterhalen, de waarde van de gegevens in kwestie overtreffen.

2.2. Overschrijven

Via het overschrijven van de informatiedrager, kan informatie verwijderd of gewist worden op basis van drie technieken:

- CLEAR: softwarematig verwijderen van data, door standaard commando's of resetten naar fabrieksinstellingen, dit laatste is dikwijls de aanbevolen methode bij mobiele toestellen en routers/switches.
- PURGE: hierbij worden labotechnieken toegepast op logische wijze (vercijfering technieken) om data te verwijderen van media via gespecialiseerde software of hardware (demagnetisatie)
- INSTALL: bij hergebruik van toestellen is het meestal voldoende om een nieuwe binaire installatie uit te voeren (gegevensbytes "1" en (of) "0" in alle opslagzones type Ghost, Bare Metal) aangezien deze installatie bestaande gegevens op destructieve wijze overschrijft.

De efficiëntie van deze methode hangt af van het aantal overschrijfcycli (om de remanentie in de randen te beperken), van de competenties en de kennis van de persoon die het proces uitvoert, en van de verificatiefuncties van de overschrijvingssoftware. Deze helpen garanderen dat de gehele toegankelijke opslagruimte van de informatiedrager overschreven wordt.

Norm "Secure Erase": Sinds omstreeks 2001 beantwoorden alle harde schijven ATA (IDE) en SATA aan de "Secure Erase"-norm. Bij dit type harde schijf beschikt de beheerder van de harde schijf over een commando "Secure Erase" waardoor alle datablokken op de schijf, bij activatie van dit commando, gewist worden (door overschrijven). Het belangrijkste voordeel van deze oplossing is dat ze a priori betrouwbaarder is dan een softwareoplossing van een hoger niveau: Hoe dichter de opdracht tot het wissen van de gegevens op de fysieke laag van de harde schijf uitgevoerd worden, hoe meer kansen er bestaan dat deze opdracht met het gewenste gevolg uitgevoerd zal worden. Volgens sommigen is deze "Secure Erase"-oplossing echter niet zeker als men zich het geval inbeeldt waar er aan de hand van niet gedocumenteerde commando's toegang verkregen kan worden tot zogenaamde gewiste gegevens. Hiermee dient rekening gehouden te worden, wetende dat vroeger de mogelijkheid is overwogen om gegevens die vernietigd werden door deze techniek (MFM- Magnetic Force Microscopy), opnieuw te herstellen. Er dient ook opgemerkt te worden dat het Amerikaanse NIST ("National Institute of Standards and Technology") in meerdere gevallen deze wismethode aanbeveelt.

Harde schijven SCSI en Fiber Channel beantwoorden niet aan deze norm en kunnen enkel vernietigd worden met behulp van softwareproducten van derden. Bij voorkeur wordt software gebruikt die aan een onafhankelijke labo-analyse onderworpen werd en die toegang geeft tot elke gekende opslagzone van de schijf.

Gutmann heeft in 1996 aanbevolen om 35 opeenvolgende passes uit te voeren tijdens de overschrijving om elk risico op gegevensherstelling te vermijden. Deze 35 passes hebben als doel rekening te houden met alle coderingstechnieken van de laatste drie decennia. Gutmann erkent dat voor hedendaagse technologieën (die gebruik maken van een magnetisch signaal aan de hand van de "PRML"-techniek – "Partial Response Maximum Likelihood"), enkele overschrijvingen met willekeurige gegevens waarschijnlijk volstaan.

Een drievoudige overschrijving is algemeen aanvaardbaar als methode om alle professionele en vertrouwelijke gegevens te vernietigen. Het drievoudig overschrijven van gegevens volstaat niet als vernietigingsmethode van gegevens op magnetische informatiedragers die gevoelige informatie bevatten. Indien het drievoudig overschrijven echter gecombineerd wordt met andere vernietigingsmethodes zoals de desintegratie of de versnippering van gegevens, biedt deze werkwijze een aanvullende garantie op vernietiging van de gegevens. In dat geval is er geen redelijke mogelijkheid meer om de gegevens te achterhalen.

Wat niet-magnetische informatiedragers betreft, zoals USB-sticks, geheugenkaarten, FLASH-geheugens, bestaan er specifieke schrijfalgoritmes om degradatie tegen te gaan. Dit leidt tot meerdere kopieën zodat de kans op het achterhalen van gegevens na het wissen vergroot. Voor dit type informatiedrager is, voor een maximale beveiliging, niet alleen de encryptie van gegevens essentieel maar ook de fysieke vernietiging van de informatiedrager.

2.3. Demagnetisatie

Demagnetisatie bestaat erin aan de hand van een voldoende krachtig magnetisch veld alle gegevens te wissen op een specifieke magnetische informatiedrager. De efficiëntie van de methode is gekoppeld aan de intensiteit van het

magnetische veld dat opgewekt wordt door het demagnetisatie-apparaat en aan de magnetische eigenschappen van de informatiedrager.

2.4. Fysiek vernietigen

Fysische vernietiging van informatiedragers dient altijd te worden toegepast bij defecte en WORM (write once, read many) media. Dit dient dit te gebeuren door gespecialiseerde firma's. Na vernietiging dient een 'attest van gewaarborgde vernietiging' worden opgevraagd of dient de vernietiging minstens geregistreerd te worden. Bewaartijd van de registratie is minstens 2 jaar.

2.4.1. Vervormen.

Fysieke vervorming bestaat erin instrumenten te gebruiken zoals een hamer, een boormachine, een bankschroef, etc., om een aanzienlijke mechanische schade toe te brengen aan informatiedragers met als doel om elke poging om gegevens te achterhalen door een hacker te vertragen, te verhinderen of af te wenden. In het geval van magnetische schijven is de efficiëntie van deze methode gekoppeld aan hoe erg de schade is die toegebracht werd aan het oppervlak van elke gegevenslaag (inclusief de vervorming van het platte oppervlak) met als doel om elke laboratoriumanalyse haast onmogelijk te maken. Voor optische schijven, kan men een machine gebruiken om druk en warmte uit te oefenen waardoor ze gemakkelijk uitgerekt en verbogen kunnen worden. Het doel bestaat erin de optische groeven van de schijf te vernietigen om zo daadwerkelijk de gegevens te vernietigen.

2.4.2. Versnipperen.

Versnippering is een vorm van vernietiging waarbij de informatiedrager tot kleine en eenvormige stukken gereduceerd wordt. Doorgaans worden er versnipperaars gebruikt voor dunne dragers zoals CD's, DVD's, SSD kaarten.

2.4.3. Desintegratie.

Desintegratie bestaat erin een niet-eenvormig mechanisme te gebruiken voor het versnijden en versnipperen (bijvoorbeeld een roterend mes in een afgesloten behuizing, bepaalde centrifuges, hamermolens, …) die de informatiedrager tot kleine, willekeurige stukken reduceren.

2.4.4. Fijnmalen.

Het fijnmalen bestaat erin apparaten te gebruiken waarmee de laag van een optische schrijf tot fijn stof gereduceerd kan worden, maar waarmee de informatiedrager zelf intact blijft zodat deze hergebruikt of vernietigd kan worden. Men kan deze methode echter niet toepassen op DVD's aangezien de informatielaag op DVD's tussen de beschermlagen zit.

2.4.5. Verbranden

Verbranding bestaat erin de informatiedragers in geschikte verbrandingsinstallaties te vernietigen.

2.4.6. Chemisch vernietigen

Bepaalde chemische stoffen kunnen zelfs informatiedragers binnendringen en ze vernietigen.

Bijlage E: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	**Ja**
Fysieke beveiliging en beveiliging van de omgeving	**Ja**
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

***** EINDE VAN DIT DOCUMENT *****