Beleidslijn informatieveiligheid en privacy

Vercijferen

(BLD CRYPT)

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 van de medewerker beschreven met betrekking tot cryptografie: technieken voor het verbergen of zodanig versleutelen van te verzenden informatie, dat het voor een persoon die toegang heeft tot het kanaal tussen zender en ontvanger (en dus 'mee kan luisteren') onmogelijk is om tegen aanvaardbare inspanning uit de getransporteerde data af te leiden welke informatie er door de zender was verzonden en welke partijen daarbij betrokken waren.

Cryptografie wordt gebruikt om gegevens over te dragen die niet leesbaar mogen zijn door andere partijen. Enkel de zender en ontvanger beschikken over de juiste sleutel om de gegevens terug om te zetten in hun originele vorm.

2. Vercijfering

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

- De organisatie dient een formeel beleid voor het gebruik van cryptografische controles op te zetten, te valideren, te communiceren en te onderhouden.
- De organisatie dient een formeel beleid voor het gebruik, bescherming en levensduur van cryptografische sleutels voor de ganse levenscyclus op te zetten, te valideren, te communiceren en te onderhouden.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2017		V2017	Eerste versie en 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.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- ENISA, “Study on cryptographic protocols”, November 2014, 52 blz.
- ENISA, “Recommended cryptographic measures: securing personal data”, September 2013, 34 blz.

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

- http://www.iso.org/iso/iso27001
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.isaca.org/cobit
- http://www.ccb.belgium.be/nl/documents
- https://www.safeonweb.be/nl
- https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools
- https://www.enisa.europa.eu/publications
- https://www.esat.kuleuven.be/cosic/
- https://uclouvain.be/crypto/
- https://webstore.ansi.org/software/Encryption-Cryptography.aspx

Bijlage C: Richtlijnen rond het gebruik van cryptografische controles

Deze richtlijnen zijn van toepassing voor data en informatiesystemen die gebruik maken van symmetrische en asymmetrische encryptie, passphrases en cryptografische sleutels.

Cryptografische maatregelen moeten bepaald worden op basis van een duidelijke formele risico-analyse waarbij antwoord wordt gegeven op de volgende vragen:

- Hoe wordt omgegaan met data die opgeslagen wordt op verwijderbare media?
- Waar wordt data opgeslagen of verwerkt?
- Hoe wordt de vertrouwelijkheid, integriteit of authenticiteit van de data gewaarborgd?
- Hoe wordt de onweerlegbaarheid van een activiteit gewaarborgd?

Wanneer cryptografie vereist is, moet steeds zo sterk mogelijke cryptografische maatregel gebruikt worden.
De organisatie moet een overzicht bijgehouden waarin terug te vinden is waar cryptografische maatregelen worden toegepast, welke cryptografische maatregelen worden toegepast en wie hiervoor verantwoordelijk is.
De gebruikte cryptografische maatregelen moeten door onafhankelijke betrouwbare deskundige getoetst worden. De ICT veiligheids-verantwoordelijke moet bepalen welke cryptografische maatregelen in welke gevallen toegepast moeten worden, gelet op de huidige goede praktijken.
De toepassing en gepastheid van cryptografische oplossingen en maatregelen moet periodiek beoordeeld worden.
Versleutelde data van derden die binnenkomen op het netwerk van de organisatie moeten eerst gedecrypteerd worden om gescand te worden op virussen en andere malware.

Bijlage D: Richtlijnen rond het sleutelbeheer

De organisatie is verantwoordelijk voor effectief sleutelbeheer. Specifieke processen en procedures gerelateerd aan sleutelbeheer moeten opgesteld, gevalideerd, gecommuniceerd worden aan alle betrokken actoren en ook regelmatig onderhouden worden.

Het sleutelbeheer moet minimaal de volgende thema's omvatten:

- Aanvragen/genereren van sleutels
- Opslag van (privé)sleutels
- Transport van (privé)sleutels
- Gebruik van sleutels
- Vervangen en vernietigen van sleutels
- Archiveren van sleutels
- Omgaan met gecompromitteerde sleutels

De volgende minimale richtlijnen moeten gelden voor het aanvragen/genereren van sleutels:

- Er moet gekozen worden voor de sterkste cryptografische maatregel die in de praktijk werkbaar is.
- Sleutels moeten een activatie- en verloopdatum hebben.
- De geldigheidsduur moet afhankelijk zijn van het beoogde doel en de tijd die het zou kosten om de sleutel te kraken.
- Elke sleutel moet uniek zijn.
- Een sleutel moet alleen voor een specifiek doel en omgeving gegenereerd worden.
- Sleutels moeten door een erkende partij geleverd worden die werkt volgens een goede praktijk.

De volgende minimale richtlijnen moeten gelden voor de opslag van (privé)sleutels:

- Sleutels moeten op zo weinig mogelijk locaties opgeslagen worden.
- Systemen moeten de door het systeem gebruikte sleutels afschermen voor gebruikers.
- Sleutels moeten beschermd worden tegen verlies of wijzigingen (bv. door een kopie bij te houden).

- Toegang tot sleutels moet tot een minimum beperkt zijn (tot de verantwoordelijke van de sleutel).
- Sleutels zijn alleen toegankelijk voor de technische experten
- Bij gevoelige of kritieke data zijn er minimaal twee beheerders.
- Sleutels moeten minimaal even goed beschermd worden als de betrokken data.

De volgende minimale richtlijnen moeten gelden voor het transport van (privé)sleutels:

- Wanneer sleutels leesbaar overgedragen worden, moet dit in persoon gebeuren of via een alternatief betrouwbaar kanaal gebeuren.
- Deze middelen en methodes om sleutels te communiceren moeten eerst goedgekeurd worden door de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO).
- Minimaal de volgende richtlijnen moeten gelden voor het gebruik van sleutels:
    - Elke sleutel moet alleen voor het toegewezen doel en omgeving ingezet worden.
    - Een sleutel die gebruikt wordt in productiesystemen mag niet gebruikt worden in niet productie systemen.
    - Binnen de organisatie is het belangrijkste gebruik van cryptografie van toepassing op:
    - Beveiliging van data op mobiele apparatuur
    - Opslag van wachtwoorden
    - Beveiliging van toepassingen
    - Beveiliging van communicatie van niet-publieke data over publieke netwerken (zoals VPN verbindingen).
    - Opslag en beveiliging van communicatie van kritieke data op het interne netwerk.

De volgende minimale richtlijnen moeten gelden voor het vervangen en vernietigen van sleutels:

- Alle sleutels moeten na de verloopdatum overal waar deze opgeslagen of toegepast werden verwijderd worden.
- Zo nodig moet een nieuwe sleutel met dezelfde eisen gegenereerd worden.

De volgende minimale richtlijnen moeten gelden voor het archiveren van sleutels:

- Sleutels die gebruikt werden door gebruikers die de organisatie verlaten hebben, moeten versleuteld en gearchiveerd worden.

De volgende minimale richtlijnen moeten gelden voor gecompromitteerde sleutels:

- Elke sleutel die gecompromitteerd is of waarvan de verwachting bestaat dat deze gecompromitteerd is, moet direct vervangen worden.
- Er moet een procedure zijn vastgesteld voor elk type maatregel waarin is bepaald hoe gehandeld moet worden wanneer een sleutel mogelijk gecompromitteerd is of wanneer een kwetsbaarheid bekend wordt.
- Een gecompromitteerde sleutel mag geen data verschaffen die gebruikt kan worden om de vervangende sleutel te bepalen.

Voor elke sleutel moet een interne medewerker verantwoordelijk zijn. Er moet een overzicht bijgehouden worden van alle verantwoordelijken voor sleutels.
Er moeten maatregelen toegepast worden om ongeautoriseerde pogingen tot verspreiding, ontcijfering, toegang, gebruik, wijziging of vervanging van sleutels of versleutelde data te detecteren.
In overeenkomsten met leveranciers van cryptografische diensten of producten moeten deze richtlijnen ingesloten zijn.
Er moeten procedures opgesteld worden die bepalen hoe omgegaan moet worden met de aanvragen voor toegang tot versleutelde data (zoals in het geval van een rechtszaak of in geval van een klacht die ingediend is bij de organisatie).
Toegang tot of het gebruik van privésleutels moeten gelogd worden volgens de procedures in het document “BLD Logbeheer”.

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	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

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