Beleidslijn informatieveiligheid en privacy

Gebruik van internet om toegang te krijgen tot het netwerk van de Kruispuntbank van de Sociale Zekerheid in het kader van de verwerking van persoonsgegevens door de actoren van de sociale sector

(BLD KSZ)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methdologie 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).

Het gebruik van het internet als toegangsmiddel tot het netwerk van de Kruispuntbank van de Sociale Zekerheid (KSZ) buiten de Extranet-infrastructuur om vormt een aanzienlijk risico, dat het voorwerp moet uitmaken van een strikt en streng veiligheids- en privacybeleid.

Deze beleidslijn kadert in de veiligheids- en privacystrategie van het netwerk van de sociale zekerheid zoals die uitgestippeld werd in het document 'minimale normen' en goedgekeurd werd door het Algemeen Coördinatiecomité van de Kruispuntbank van de Sociale Zekerheid.

Dit document geeft algemene aanwijzingen over het gebruik van het internet om toegang te krijgen tot het netwerk van de KSZ in het kader van de verwerking van persoonsgegevens door de actoren van de sociale sector. Deze beleidslijn is enkel van toepassing op de actoren van de sociale sector die in het kader van de verwerking van persoonsgegevens niet op het Extranet van de Sociale Zekerheid zijn aangesloten en die kunnen aantonen dat ze zich onmogelijk hierop kunnen aansluiten.

2. Toegang tot het netwerk KSZ via internet

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

2.1. Algemeen

Het gebruik van het internet als toegangsmiddel tot het netwerk van de Kruispuntbank van de Sociale Zekerheid (KSZ) vormt een uitzondering op het algemene principe van de toegang via het Extranet van de Sociale Zekerheid. Hiervoor moet een schriftelijke machtiging en afwijking worden gevraagd aan de leidende ambtenaar van de KSZ.

2.2. Inhoud van de aanvraag

In de machtigings- en afwijkingsaanvraag moeten de redenen worden vermeld waarom het Extranet van de Sociale Zekerheid of de door de KSZ als veilig beschouwde private netwerken, niet kunnen worden gebruikt. In de aanvraag moeten de maatregelen die binnen de instellingen werden genomen om de aan het internetprotocol te wijten veiligheids- en privacy-risico's tot een minimum te beperken ook duidelijk worden vermeld.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2004	JMG	V2004	Eerste versie	16/11/2004	16/11/2004
2005	JMG	V2005	Tweede versie	14/02/2005	14/02/2005
2005	JMG	V2005	Derde versie	28/02/2005	28/02/2005
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.

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

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.ccb.belgium.be/nl/documents
- https://www.ksz-bcss.fgov.be/nl

Bijlage C: Extranet van de Sociale Zekerheid

Het Extranet van de Sociale Zekerheid is een beveiligd IP-netwerk en heeft als doel de verschillende instellingen van sociale zekerheid met elkaar te verbinden en een aantal gemeenschappelijke diensten aan te bieden zoals de beveiligde aansluiting van heterogene netwerken, de terbeschikkingstelling van HTTP/FTP-proxies, de uitwisseling van berichten en informatiegegevens, de antivirusscanning van het HTTP/FTP/SMTP-verkeer, de hosting van websites, het beheer en het onderhoud van domeinnamen en toegang verlenen tot interne gegevens via dial-up of VPN.

De infrastructuur die over twee sites is verspreid en die op een gelaagd veiligheidsmodel is gebaseerd, wordt beschermd door firewalls ter hoogte van elke binnenkomende aansluiting, namelijk tussen de instelling en de backbone enerzijds en tussen de backbone en het internet en tussen de backbone en de private netwerken anderzijds; daar vindt ook een centraal beheer van de antivirus-beveiliging plaats.

Het Extranet van de Sociale Zekerheid werd uitgerust met een IDS-systeem (Intrusion Detection System) dat geconsolideerd wordt door een permanente analyse van de logs door middel van een MSS (Management Security Services).

Op de infrastructuur en de componenten ervan worden periodiek audits uitgevoerd.

Bijlage D: Voorwaarden voor toegang tot het Extranet van de Sociale Zekerheid via internet

Het gebruik van het internet als toegangsmiddel tot het netwerk van de Kruispuntbank van de Sociale Zekerheid (KSZ) is toegelaten op voorwaarde dat de KSZ een uitdrukkelijke en schriftelijke machtiging verleent en dat de volgende voorwaarden strikt worden toegepast :

1. Niveau toegangsmachtiging

- De machtiging wordt nooit globaal verleend; ze heeft enkel betrekking op de in de aanvraag bedoelde transactie of systeem,
- Bij het gebruik van sociale persoonsgegevens moet duidelijk uit de aanvraag blijken of het een raadpleging of mededeling van sociale persoonsgegevens betreft; wanneer het een raadpleging betreft, moet de beoogde doelstelling duidelijk in het aanvraagdossier worden beschreven,
- De transacties of systemen waartoe toegang wordt verleend, moeten door een toegangsmachtigingssysteem door middel van de User Management Ambtenaar Fonctionnaire (UMAF) worden beveiligd wanneer ze sociale persoonsgegevens bevatten,
- De betrokken gebruikers zijn natuurlijke personen die bij naam worden aangeduid door de leidende ambtenaar van de instelling.

Een lokale beheerder die hiertoe is gemandateerd door de leidende ambtenaar van de instelling, beheert deze machtigingen.

2. Niveau identificatie / authenticatie

Bij de identificatie en authenticatie moet het gebruikersreglement dat op de onthaalpagina van het sociale zekerheidsportaal (https://www.socialsecurity.be) vermeld staat zonder voorbehoud worden toegepast.
Het identificatie- en authenticatieproces hangt af van het vertrouwelijkheidsniveau van de door de transactie of het systeem verwerkte gegevens evenals van het kader waarin de mededeling of de raadpleging van de sociale gegevens plaatsvindt.
De toegang tot de transactie of het systeem via het internet wordt geactiveerd na gunstig advies van de KSZ die in haar beraadslaging bepaalt welk identificatie- of authenticatieproces moet worden geïmplementeerd.

In elk geval bestaat dit proces uit minimaal:

- een identificatie door een user ID,

- een authenticatie door het gebruik van een paswoord, de ambtenaar-token of de elektronische identiteitskaart.

In geval van een verbinding via file transfer, kan het gebruik van een certificaat worden geëist. Het soort certificaat wordt in onderling overleg met de KSZ bepaald.

3. Traceerbaarheid

De activatie van de security logs is verplicht en moet in overeenstemming zijn met de desbetreffende beleidslijnen informatieveiligheid en privacy zoals die is vastgelegd door de werkgroep 'Informatieveiligheid'.

4. Beperkingen

- Het gebruik van het internet in het kader van een verbinding van toepassing tot toepassing is verboden,
- De beschikbaarheid van het internet valt niet onder de verantwoordelijkheid van de KSZ,
- Enkel het HTTPS-protocol (inkapseling van het HTTP-protocol in SSL) is toegelaten.

5. Verbinding via file transfer

Op de activatie van de gegevensuitwisseling door file transfer via het internet zijn de volgende voorwaarden van toepassing:

- De uitdrukkelijke machtiging van de KSZ,
- Het gebruik van een transfertprotocol dat door het netwerk van de KSZ als veilig wordt beschouwd,
- Het gebruik van een identificatie- en authenticatie-proces dat door het netwerk van de KSZ als een sterk proces wordt beschouwd.

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	**Ja**
Cryptografie	**Ja**
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	**Ja**
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

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