Beleidslijn informatieveiligheid en privacy

Veilig telewerken

(BLD TELE)

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).

Dit document geeft algemene aanwijzingen over het werken op afstand. De overheid zet sterk in op een innovatieve en flexibele arbeidsorganisatie door initiatieven te nemen om de beschikbaarheid, betrokkenheid en creativiteit van de medewerkers voortdurend te verbeteren. De mogelijkheid om te kunnen telewerken komt daaraan tegemoet. Ten behoeve van de veiligheid en de privacy van informatie binnen de systemen van organisaties, zijn deze beleidslijnen gericht op hoe met telewerken omgegaan moet worden. Het kan ook gaan om informatie van derde partijen, waarvan de organisatie niet de eigenaar is, indien deze via het platform wordt ontsloten en beschikbaar gesteld wordt aan de telewerker.

Bij telewerken wordt gebruik gemaakt van mobiele apparaten zoals smartphones, tablets en laptops. Voor het uitvoeren van werkzaamheden hebben telewerkers toegang tot informatie en informatiesystemen die onder de verantwoordelijkheid vallen van de organisatie waarvoor zij werkzaam zijn. Dit kan ook informatie zijn uit externe bronnen, waarover organisatie beschikt of waar de organisatie rechtstreeks toegang toe heeft. Het ontsluiten van informatie buiten de beheersbare fysieke organisatie leidt tot veiligheids- en privacy-risico's. De organisatie kan deze risico's verkleinen door de nodige maatregelen te treffen. Deze beleidslijnen zijn geschreven om aan te geven dat de organisatie steeds verantwoordelijk blijft voor de informatie.

2. Veilig telewerken

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

1. Elke organisatie moet de gepaste maatregelen treffen, in functie van het toegangsmedium[1], voor de informatieveiligheid van de online-toegang van buiten de organisatie tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie
2. Er worden duidelijk verstaanbare beleidslijnen met gedragsregels en gepaste implementatie van telewerken opgezet, gevalideerd, gecommuniceerd en onderhouden, inclusief de uitwerking van welke systemen niet, en welke systemen wel vanuit de thuiswerkplek of andere apparaten mogen worden geraadpleegd.
3. De telewerk-voorzieningen van de organisatie zijn zo ingericht dat er op de telewerk-plek (thuis, in een satellietkantoor of in een andere locatie) geen informatie van de organisatie wordt opgeslagen op externe toestellen zonder versleuteling en dat mogelijke bedreigingen vanaf de telewerk-plek niet in de IT infrastructuur van de organisatie terechtkomen.

1 Toegangsmedium : vb. internet, gehuurde verbinding, privaat netwerk, draadloos.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2003		V2003	Eerste versie	10/09/2003	01/10/2003
2004		V2004	Tweede versie	11/02/2004	01/12/2004
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.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- NIST, “Guide to enterprise telework, remote access, and BYOD security”, juli 2016, 53 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.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
- http://www.ccb.belgium.be/nl/work
- http://www.cnt-nar.be/CAO-COORD/cao-081.pdf
- https://www.safeonweb.be/nl
- https://www.safeinternetbanking.be
- https://www.cybersimpel.be/nl

Bijlage C: Telewerk bedreigingen en maatregelen

De bedreigingen en maatregelen bij telewerken kan men indelen naar de componenten van de telewerk-keten tussen medewerker en de ICT-infrastructuur van de organisatie:

1. **De telewerklocatie**

Telewerken vindt plaats vanaf een locatie buiten de organisatie. De grootste bedreiging is het onderscheppen en manipuleren van (professionele, vertrouwelijke of gevoelige) informatie. Deze omgeving valt buiten de invloedssfeer van de organisatie, daarom is voor de beveiliging van een telewerkplek een mix van technische, procedurele en organisatorische maatregelen nodig. De organisatie is bevoegd om de nodige eisen te stellen als het een vaste telewerk-locatie betreft, bijvoorbeeld thuis bij de medewerker of in een satelliet kantoor. Indien een medewerker op een openbare locatie telewerkt, bestaat de kans dat een buitenstaander informatie van het scherm leest of een gesprek afluistert. Daarnaast kan het telewerk-apparaat van de telewerker verloren geraken. Door verlies of diefstal van het telewerk-apparaat kan de daarop opgeslagen informatie in handen komt van een buitenstaander.

Gebruikt een telewerker een computer van een andere organisatie of persoon, zoals in een bibliotheek, thuis, luchthavenlounge, of van een vriend of buurman, dan bestaat de mogelijkheid dat de volgende gebruiker van het toestel de (in de cache) opgeslagen informatie van de vorige sessie kan inzien.

Hieronder volgt een overzicht van de belangrijkste risico's met betrekking tot de telewerklocatie en de maatregelen die de organisatie kan nemen om het risico te verlagen.

Risico: Onbevoegden kunnen informatie van het scherm (mee)lezen
Maatregelen:

- Specifiek aandacht in sensibiliseringscampagnes.
- Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden met daarin onder andere:
  a. Op welke locaties de telewerker mag telewerken. De organisatie kan verbieden om vanuit een internetcafé of via een onbeveiligde draadloze verbinding te telewerken.
  b. Clear screen-beleid
- Schermbeveiliging (screensaver) maakt na een periode van maximaal 15 minuten inactiviteit alle informatie op het scherm ontoegankelijk.
- De organisatie kan een privacy-scherm toevoegen. Een privacy-scherm beschermt tegen meekijken op het telewerk-apparaat, de medewerker moet recht voor het beeldscherm zitten om te telewerken.

Risico: Onbevoegden kunnen informatie onderscheppen door gesprekken af te luisteren.
Maatregelen:

- Specifiek aandacht in sensibiliseringscampagnes.
- Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden met daarin onder andere het beperken in openbare locaties van het uitwisselen van informatie via telefoon.

Risico: Informatie in handen van een buitenstaander door verlies of diefstal van papier of mobiele gegevensdragers.
Maatregelen:

- Specifiek aandacht in sensibiliseringscampagnes.
- Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden met daarin onder andere directe meldingsplicht van verlies of diefstal van mobiele gegevensdragers met professionele, vertrouwelijke of gevoelige informatie aan de informatieveiligheidsconsulent (CISO) en/of functionaris van gegevensbescherming (DPO).
- Clear desk-beleid voor papier en verwijderbare opslagmedia:
  a. De medewerker mag geen gevoelige informatie op het bureau laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, lade, bureau of kamer).
  b. Het afdrukken van informatie in externe omgevingen wordt afgeraden, maar als het niet anders kan, dan wordt door de telewerker een risico-beoordeling gemaakt.

2. Het telewerk-apparaat zoals een desktop, laptop, tablet of smartphone

Telewerk-apparaten kunnen eigendom van de telewerker of de organisatie zijn, of van iemand anders. Indien de telewerker een telewerk-apparaat van de organisatie ter beschikking heeft, kan de organisatie autonoom bepalen welke veiligheidsmaatregelen van toepassing zijn. Daarmee kan een organisatie de risico's grotendeels afdekken. Voor een privé-apparaat is dat anders omdat dit niet in beheer is bij de organisatie. De organisatie is wel bevoegd om veiligheidsinstellingen af te dwingen als privé-apparaten zakelijk gebruikt worden ('bring your own device' of BYOD). Dit gaat dan onder meer over controle op wachtwoord/wachtzin, encryptie, aanwezigheid van anti-malware software. Op verzoek van de organisatie dienen medewerkers de installatie van software toe te laten (via 'mobile device management software').

Mogelijke problemen zijn:

- Geen/onvoldoende richtlijnen over welke gegevens op het telewerk-apparaat mogen staan (geen kennis van de data classificatie regels)
- Malware / Ransomware op het telewerk-apparaat
- Klikken op links in e-mail en webpagina's die niet vertrouwd zijn
- Verbinden via onveilige open netwerken, waar men kan worden aangevallen door derden
- "Man in the middle" attack[2]
- Niet vergrendelen van het telewerk-apparaat
- Geen versleuteling, terwijl dat nodig is
- Diefstal van het telewerk-apparaat
- 'Rooten' of 'jailbreaken' van het telewerk-apparaat[3]
- Verlies van het telewerk-apparaat
- Professionele, vertrouwelijke of gevoelige informatie wordt (onversleuteld) op mobiele gegevensdragers opgeslagen
- Ongeautoriseerde toegang tot, of technische storingen op het telewerk-apparaat.
- De telewerker heeft op zijn privé-apparaat alle rechten en kan hierop software installeren
- Ongeautoriseerde, laattijdige, onjuiste of onvolledige update-installaties op het telewerk-apparaat.
- Installatie van kwaadaardige software die gegevens steelt, zichzelf toegang verschaft, maar ook zichzelf verspreidt over andere systemen van de organisatie.
- Onbevoegden lezen, kopiëren, wijzigen en/of vernietigen gegevens.
- Het telewerk-apparaat moet vervangen worden voor een nieuw telewerk-apparaat.
- Onbeperkte toegang tot systemen van de organisatie via het telewerk-apparaat.

Hieronder een overzicht van de belangrijkste risico's en de maatregelen rond telewerk-apparaat en de maatregelen die de organisatie kan nemen om het risico te verlagen.

Risico: Informatie in handen van een buitenstaander (manipulatie van gegevens of onbevoegd inzien).
Maatregelen:

- Specifiek aandacht in sensibiliseringscampagnes.
- Alle apparaten, zowel van de organisatie of privé, met gegevens van de organisatie worden beheerd met een MDM-tool, zodat het veiligheidsbeleid op het telewerk-apparaat technisch kan afgedwongen worden:
    - software op het telewerk-apparaat, inclusief veiligheidssoftware zoals:
        i. Up-to-date virusscanner
        ii. Up-to-date personal firewall
        iii. Up-to-date anti malware tool
        iv. Up-to-date besturingssysteem en toepassingen (zie hiervoor patchmanagement)
    - rechten van de telewerker op het telewerk-apparaat
    - de telewerker moet inloggen met een gebruikersnaam en wachtwoord/wachtzin, eventueel ondersteund door een certificaat.

[2] http://nl.wikipedia.org/wiki/Man-in-the-middle

[3] Jailbreak is het mogelijk maken dat niet goedgekeurde apps op een mobiel apparaat kunnen werken, waardoor ook malware gedraaid kan worden. Rooten is het proces om meer rechten te krijgen op het apparaat waardoor het complete besturingssysteem gewijzigd of vervangen kan worden, en daarmee malware introduceren en veiligheidsinstellingen omzeilen.

- Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden met daarin onder andere:
    - geen professionele, vertrouwelijke of gevoelige informatie op mobiele gegevensdragers opslagen tenzij versleuteld.
    - geen toepassingen installeren zonder toestemming van de organisatie.
    - geen informatie lokaal op het privé-apparaat opslaan om de kans te beperken dat spyware het kan uitlezen.
- Uitzetten van services die niet nodig zijn ("hardening" van het telewerk-apparaat)[4]
- Het telewerk-apparaat slaat geen informatie van de organisatie op. Een alternatief om decentrale opslag van gegevens van de organisatie te vermijden is Virtuele Desktop Infrastructuur (VDI). Door het centrale beheer is het mogelijk om met relatief lage beheerinspanning de medewerker op ieder tijdstip, vanaf iedere willekeurige plek en met een willekeurig telewerk-apparaat inloggen, veilig, flexibel en gecontroleerd toegang te geven tot de persoonlijke werkplek.

Risico: Het telewerk-apparaat kan een malware/ransomware besmetting oplopen en mogelijk de organisatie infecteren. Het telewerk-apparaat wordt door hackers als aanvalsinstrument gebruikt.
Maatregelen:

- Specifiek aandacht in sensibiliseringscampagnes.
- Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden met daarin onder andere
    - geen gebruik maken van onbekende netwerken
    - niet op onbekende links in e-mail en webpagina's klikken
- Bij veiligheidsproblemen wordt het telewerk-apparaat in een quarantainenetwerk geplaatst[5]. Hierdoor krijgt de telewerker enkel toegang tot een beperkt aantal websites, namelijk die van virusscanners, firewalls, enz.
- Uitzetten van services die niet nodig zijn ("hardening" van het telewerk-apparaat)

3. De verbinding tussen het telewerk-apparaat en de ICT-infrastructuur van de organisatie

De grootste bedreiging met betrekking tot de netwerkvoorziening is onbevoegd inzien, kopiëren, vernietigen en wijzigen van gegevens. De netwerkverbinding tussen het telewerk-apparaat en de ICT-infrastructuur van de organisatie kan op verschillende manieren tot stand worden gebracht. Deze netwerkverbindingen kunnen door hackers worden afgeluisterd, waardoor deze inzage kunnen krijgen in de informatie die tussen de telewerker en de organisatie wordt uitgewisseld. Gebruikersnaam en wachtwoord/wachtzin kunnen worden bemachtigd, waardoor een hacker zich toegang kan verschaffen tot de informatie waarvoor de organisatie verantwoordelijk is. Dit kan ook informatie van burgers of derde partijen zijn, waarvan de organisatie niet de eigenaar is.

Het belangrijkste risico voor de verbinding tussen het telewerk-apparaat en de ICT-infrastructuur van de organisatie is informatie die in handen komt van externe partijen (manipulatie van gegevens of onbevoegd inzien).

Maatregelen:

- Specifiek aandacht in sensibiliseringscampagnes.
- Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden met daarin onder andere geen gebruik maken van onbekende netwerken.
- Alle apparaten, zowel van de organisatie of privé, die worden gebruikt om een verbinding met de ICT-infrastructuur van de organisatie op te zetten worden beheerd met een MDM-tool, zodat het veiligheidsbeleid op het telewerk-apparaat technisch kan worden afgedwongen.

[4] Met hardening wordt bedoeld : overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen. Zodanige waarden toekennen aan veiligheidsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat. Het gaat hierbij ook om het verwijderen van niet gebruikte of onnodige medewerkers accounts, en tevens het wijzigen van standaard wachtwoorden die op sommige systemen aanwezig kunnen zijn.

[5] Deze oplossing biedt beveiliging tegen het feit dat 'onbedoeld' configuratie instellingen van het apparaat zijn gewijzigd en deze niet zijn hersteld voordat een verbinding met de ICT-infrastructuur van de organisatie wordt opgezet. Een telewerker kan bijvoorbeeld antivirussoftware uitschakelen, terwijl deze software een vereiste is voor een netwerkverbinding. De computerconfiguraties kunnen worden gecontroleerd en zo nodig worden gecorrigeerd voordat er toegang tot het netwerk wordt verleend. Wanneer de configuratie van het apparaat overeenkomt met het netwerkbeleid van de organisatie, worden de quarantainebeperkingen opgeheven.

- Het telewerk-apparaat dat een verbinding met de ICT-infrastructuur van de organisatie wil opzetten wordt gecontroleerd of deze voorzien is van een up-to-date virusscanner en een firewall. Indien het telewerk-apparaat niet of onvoldoende is beveiligd (bijvoorbeeld virusdefinities niet up-to-date), kan de toegang tot de ICT-infrastructuur van de organisatie worden geweigerd.

4. Gegevensverwerking of -opslag op het telewerk-apparaat vindt plaats op een externe locatie.

Hierdoor staan gegevens bloot aan risico's die samenhangen met de werklocatie en eventuele kwetsbaarheden op het telewerk-apparaat.

Mogelijke problemen zijn:

- De betrouwbaarheid van gegevens op de serveromgeving bedreigd door ongeautoriseerde toegang en Denial of Service-aanvallen (beschikbaarheid). De impact van deze bedreigingen kan groot zijn omdat het veel telewerkers treft.
- Ongeautoriseerde toegang tot de serveromgeving veroorzaakt door hacking of via een niet voldoende beveiligd telewerk-apparaat.
- Telewerkers gaan onzorgvuldig om met hun identificatie- en authenticatiemiddelen of laten derden hun telewerk-apparaat gebruiken.

Het belangrijkste risico van gegevensverwerking of -opslag op het telewerk-apparaat op een externe locatie is ongeautoriseerde toegang tot de serveromgeving, zowel de systemen als de informatie.

Maatregelen:

- Specifiek aandacht in sensibiliseringscampagnes.
- Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden met daarin onder andere
  - geen gebruik maken van onbekende netwerken.
  - niet op onbekende links in e-mail en webpagina's klikken.
- Toegang tot organisatie systemen beschermen door twee-factor authenticatie (met het telewerk-apparaat alleen kan geen toegang worden verkregen).
- Gebruik maken van Role Based Access Control (RBAC)[6].
  - Na authenticatie wordt toegang verleend tot bepaalde toepassingen en informatie voor medewerkers vanaf een telewerkplek. Het is mogelijk om de autorisaties van een medewerker te beperken bij telewerk. De hoeveelheid autorisaties van een telewerker kan gerelateerd worden aan het veiligheidsniveau van het telewerk-apparaat.
  - Extra aandacht voor het tijdig en volledig intrekken van autorisaties bij uitdiensttreding of wijziging van functies van telewerkers.
- Netwerk compartimentering/segmentering met een 'goede' firewall-configuratie en toepassing van een demilitarized zone (DMZ) kan de toegang van de telewerker beperken.
- Extra aandacht is nodig voor logging en monitoring van toegang tot de serveromgeving. Deze controle moet misbruiken, goed beheer en functionering conform de gestelde eisen vaststellen. Minimale te loggen informatie:
  - Welke apparaten zetten een (VPN) netwerkverbinding op en welke pogingen mislukken?
  - Welke toegangsrechten worden gebruikt/misbruikt voor netwerktoegang van de organisatie (foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen)?
  - Welk netwerkverkeer vindt er plaats tussen het telewerk-apparaat en het interne netwerk?

5. Toegang tot informatie

Voor toegang van de telewerker tot de informatie op het netwerk van de organisatie is multi-factor authenticatie noodzakelijk. Multi-factor authenticatie vereist dat de gebruiker kan aantonen dat hij/zij daadwerkelijk degene is door:

[6] https://nl.wikipedia.org/wiki/Role-based_access_control

1. Wat de gebruiker weet (bijvoorbeeld: wachtzin / PIN code)
2. Wat de gebruiker bezit (bijvoorbeeld: token, certificaat of via SMS-authenticatie)
3. Wie de gebruiker is (bijvoorbeeld: biometrisch kenmerk)

Op basis van twee (twee factor authenticatie) of meerdere factoren kan worden aangetoond dat de gebruiker daadwerkelijk is wie de gebruiker zegt dat hij/zij is.

6. De telewerker zelf

De telewerker kan zich niet of onvoldoende bewust zijn van de mogelijke risico's verbonden met telewerken:

- Het telewerk-apparaat wordt onbeheerd achtergelaten in een ruimte waar derden toegang tot hebben.
- De telewerker heeft niet in de gaten dat 'social engineering'[7] aanval wordt uitgevoerd.
- Privé-computers thuis worden niet goed beheerd en zijn besmet geraakt met malware/ransomware.

De medewerker moet weten welke risico's gepaard gaan met telewerken via sensibiliseringscampagnes. Verder moeten duidelijke afspraken gemaakt worden over rechten en plichten van de medewerker, en de mogelijke gevolgen bij overtredingen.

Bijlage D: 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.	**Ja**
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	**Ja**
Cryptografie	
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 *****

[7] Bij social engineering maken hackers gebruik van de goedgelovigheid en de goedwillendheid van medewerkers om het doel te bereiken. Meestal is de betrokken medewerker zich niet bewust dat het gaat om een kwaadwillige aanval. Het is normaal om een onbekende in de gang aan te spreken en te vragen of ze hulp nodig hebben. Toch hebben veel mensen hier moeite mee en gebeurt het (te) weinig. Het is altijd goed om af te vragen met wie men spreekt aan de telefoon en altijd de vraag te stellen 'waarom krijg ik deze vraag?'.