POD MAATSCHAPPELIJKE INTEGRATIE
BETER SAMEN LEVEN
SPP INTÉGRATION SOCIALE
MIEUX VIVRE ENSEMBLE

De coronacrisis heeft aanleiding gegeven tot het oproepen door de verantwoordelijke instanties om zoveel mogelijk over te gaan tot thuiswerk om de verspreiding van het coronavirus COVID-19 tegen te gaan. Ook veel OCMW-medewerkers werken nu (geheel of gedeeltelijk) van thuis uit. Dat is natuurlijk aangewezen opdat alle werkzaamheden en alle dienstverlening vanuit de OCMW's zou kunnen blijven verder lopen.

In de eerste plaats is het uiteraard de bedoeling om hulpvragers zo goed mogelijk verder te helpen. Daar moet de prioriteit liggen, zeker in deze moeilijke omstandigheden.

Daarnaast zijn we er ons ook van bewust dat de lokale besturen en de OCMW's zeer snel hebben moeten ingrijpen en zeer snel zijn moeten overschakelen naar thuiswerk.

Als de maatschappelijk werkers of andere medewerkers die persoonsgegevens hebben, moeten thuiswerken, moeten de nodige veiligheidsmaatregelen genomen worden. Denk maar aan bijv. indien mogelijk, werken in een aparte ruimte dan waar de andere gezinsleden aanwezig zijn, je computer afsluiten of de schermbeveiliging inschakelen als je niet aan je computer werkt, enz. (zie ook lager)

De deontologische code die maatschappelijk werkers hebben, blijft uiteraard gelden.

Ondanks deze moeilijke omstandigheden, blijft het belangrijk te streven naar maximale cyberveiligheid.

Zo zijn de veiligheidsmaatregelen van de KSZ (nog steeds) van toepassing bij het raadplegen van de KSZ-stromen en voor instellingen die identiteitskaartlezers gebruiken.

We zetten de mogelijkheden nog even op een rij:

1. De medewerkers blijven fysiek in de voorzieningen van het OCMW werken. Er stelt zich dan geen enkel veiligheidsprobleem, deze perimeter wordt verondersteld voldoende beveiligd te zijn volgens de instructies van de KSZ en de POD MI.
2. De medewerkers hebben een PC (desktop of laptop) van hun werkgever. Deze laptop moet normaal geconfigureerd zijn en in overeenstemming zijn met de minimale veiligheidsnormen van de KSZ (zie bijlage 1 op het einde van het document).
3. De medewerkers hebben een privé-PC en willen hiermee, van thuis uit werken. Deze oplossing is om veiligheidsredenen enkel toegelaten onder bepaalde strikte voorwaarden (zie de kwetsbaarheden in bijlage 2), behalve wanneer zij werken met een geïnstalleerde virtuele desktop-oplossing (bv Citrix, Awingu, BeSecure,…)CITRIX of AWINGU. Wanneer men wil werken vanuit een privé-PC, zonder virtuele desktop technologie, dan moeten de volgende criteria worden nageleefd:
    a. Het wachtwoord moet 12 karakters bevatten, inclusief hoofdletter, kleine letter, cijfers en een speciaal teken. Bovendien moet er gebruik worden gemaakt van 2FA (2 factors authorization : https://www.safeonweb.be/nl/gebruik-sterke-wachtwoorden).

b. Tijdens het werk mogen er geen andere opzoekingen gebeuren op het internet via de browser.

c. De werksessie/consultatie/… moet gesloten worden wanneer het werk beëindigd is of tijdens een pauze.

d. Buiten de medewerker mag niemand anders de inhoud van de sessies zien;

e. De firewall van het OCMW legt zoveel mogelijk beperkingen op aan de externe verbindingen. Bijvoorbeeld beperkingen aan de regio vanaf waar er een verbinding kan gemaakt worden, en aan de tijd (enkel tijdens de normale kantooruren, niet tijdens het weekend ...).

Opgelet: als er te veel externe verbindingen worden gemaakt, kan het netwerk verzadigd geraken en vertragen.

Wie u hiermee kan helpen?

Wel, rekening houdend met de hierboven vermelde verplichtingen:

- De informaticus van het OCMW of van de gemeente of uw informaticaleverancier kan helpen om de verschillende beveiligingsmaatregelen in geval van telewerk uit te voeren, ofwel:
  - door een tool te installeren die de controle op afstand overneemt van uw werk-computer in het OCMW. Bijvoorbeeld: VPN-verbinding + gebruik van de tool “toegang bureau op afstand” (**enkel** voor de installatie of herstelling; dit en deze tool zal vervolgens worden gesloten);
  - door voor u een PC (desktop of laptop) van het OCMW klaar te maken die hij u ter beschikking stelt om bij u te installeren en eenvoudiger te werken, waarbij de PC **enkel** zal gebruikt worden voor de ‘OCMW-taken’;
  - door een ‘thin client’ voor te bereiden (of via Citrix) wanneer het OCMW met deze technologie werkt;
  - door u een specifieke executable te laten downloaden die automatisch wordt geïnstalleerd in het geval van de terminal - serverlicentie.

- Benadruk ook dat gebruikers hun scherm moeten vergrendelen als ze hun computer verlaten en dat iedereen die aan telewerk doet, dit moet doen in een omgeving die de noodzakelijke privacy en bescherming van persoonsgegevens van cliënten en collega’s garandeert. Dit geldt zowel bij toepassingen die gebruik maken van de KSZ, als voor andere dossierbehandeling – ook als dit gebeurt met telefonisch, spraak-/chat- en video-overleg.
- Er worden in principe thuis geen afdrukken gemaakt; indien dit om een gegronde reden toch noodzakelijk is moet ervoor gezorgd worden dat deze niet toegankelijk zijn voor andere personen, de afdrukken veilig worden bewaard en nadien naar het OCMW worden gebracht óf zo snel mogelijk op een degelijke manier worden vernietigd.

- Let op, voor maatschappelijk werkers of andere medewerkers die op afstand verbinding moeten maken met de KSZ zijn de volgende tools verplicht, anders zal er een technische blokkering optreden:
  - De verbinding moet gemaakt worden via een VPN of Explore of Publiwin ;
  - Men moet een elektronische identiteitskaartlezer hebben om zich te identificeren op het portaal van de sociale zekerheid (via een aparte lezer ofwel geïntegreerd in het toetsenbord).

- Men moet een gebruikersbeleid uitgeschreven hebben dat door de Functionaris voor GegevensBescherming (FGB)/Data Protection Officer (DPO) en/of jurist is opgesteld en waarin een geheimhoudingsclausule is opgenomen, met inbegrip van de volgende beperkingen:
  - Men mag geen toegang geven (bewust of onbewust) tot zijn werksessies, aan iemand buiten het OCMW
  - Men mag geen toegang geven (bewust of onbewust) tot zijn PC (desktop of laptop) die toebehoort aan het OCMW, aan iemand buiten het OCMW;
  - Men mag geen wachtwoorden meedelen (het spreekt voor zich dat de informaticus administratorrechten heeft);
  - Men mag geen websites raadplegen voor persoonlijk gebruik tegelijk met zijn VPN-sessie met het OCMW (sluit de VPN-sessie en open de browsersessie indien nodig).

Proximus, Telenet, Infrax, Cipal Schaubroeck (onder anderen…) bieden betrouwbare VPN-oplossingen met RDP (remote deskstop protocol) vanaf de PC of zonder Microsoft RDC (Remote Deskstop Connection) licenties (terminal server CAL gebruikerslicentie).

Het spreekt voor zich dat uw informaticus of informaticaleverancier u eveneens kan helpen. Let er wel op dat deze niet van deze gelegenheid gebruik maken om méér installatierechten, connectierechten of ondersteuningsrechten te bekomen die niet toelaatbaar zijn volgens de vereisten van de AVG en de KSZ-richtlijnen.

Aarzel niet om in geval van vragen en/of problemen contact op te nemen met Gilles Kempens, veiligheidsconsulent van de POD MI. Zijn contactgegevens zijn de volgende:
gilles.kempgens@mi-is.be en mi.dpo@mi-is.be of 0473.85.26.24.

Bijlage 1

Herhaling van de veiligheidsmaatregelen die moeten worden nageleefd op PC's (laptops en deskstops):

1. De eindgebruiker heeft geen administratorrechten;

2. De PC bevat geen persoonlijke gegevens, maar als dat wel het geval is, moeten de gegevens op de interne harde schijf/SSD worden gecodeerd (Bitlocker is een gratis Microsoft-tool als u een Microsoft Business- of Enterprise-versie hebt; er zijn ook andere goede encryptietools (vraag: moet het niet 'encryptietools' zijn?) beschikbaar, enkele ervan zijn gratis);

3. De verbinding gebeurt via een VPN die vanaf de PC verbinding maakt met het netwerk van het OCMW;

4. Bij verbinding via VPN zal een GPO (Group Policy Object dat intern, op de firewall of op de Network Access Control wordt ontwikkeld) controleren of de antivirus en het besturingssysteem up-to-date zijn voordat de verbinding wordt toegelaten en zo niet, zal de GPO de updates forceren voordat de verbinding wordt toegelaten;

5. Het GPO zal elk gebruik van een browser om op het internet te gaan verbieden zolang de gebruiker verbonden is met het netwerk van het OCMW via VPN (voorbeelden van browsers: Internet Explorer, Edge, Mozilla, Chrome). Merk op dat het mogelijk is om via VPN op het internet te gaan, maar dit is alleen aan te raden voor professionele raadplegingen;

6. De verbindingen worden gemaakt in het remote desktop-protocol, d.w.z. op afstand zonder gegevens te bewaren, maar met alle bedrijfsapplicaties, terwijl de verbinding rechtstreeks van de PC naar de servers en de databases wordt gemaakt.

Opgelet: bij een te groot aantal verbindingen op afstand dreigt de bandbreedte snel verzadigd te geraken.

Bijlage 2

Lijst van enkele <u>kwetsbaarheden</u> wanneer u via een privé-PC werkt:

1. de eigenaar/gebruiker van de PC deelt zijn PC met de familie;

2. men werkt nog met oude versies van het besturingssysteem zoals Windows 7 (dat niet betrouwbaar is);

3. het is niet zeker dat een oude PC een VPN zal ondersteunen;

4. de naleving van de minimale normen vereist 3 wachtwoorden (een admin-wachtwoord, een gebruikerswachtwoord voor de sessie van de medewerker en een VPN-wachtwoord);

5. de PC moet in orde zijn met de antivirus en het is niet zeker dat een ouder toestel de actuele degelijke antivirus- en antimalware-programma's aankan;

6. het gebruik van een privé-PC veronderstelt dat de eigenaar-gebruiker zijn VPN afsluit voordat hij/zij op het internet gaat voor eigen gebruik en vice versa.