Politique de sécurité de l'information et vie privée

Télétravail sécurisé

(BLD TELE)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie relative à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, aux sous-traitants de données, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

Le présent document contient des instructions générales relatives au travail à distance. Les pouvoirs publics investissent avec force dans une organisation du travail souple et innovatrice en prenant des initiatives pour augmenter la disponibilité, l'engagement et la créativité des collaborateurs. La possibilité de faire du télétravail y répond. Pour la sécurité et la protection des informations au sein des systèmes des organisations, les présentes instructions précisent comment il y a lieu d'organiser le télétravail. Il peut également s'agir d'informations de tiers dont l'organisation n'est pas le propriétaire, si celles-ci sont mises à la disposition du télétravailleur via la plateforme.

Lors du télétravail, il est fait usage d'appareils mobiles tels les smartphones, les tablettes et les ordinateurs portables. Pour l'exécution des travaux, les télétravailleurs ont accès aux informations et aux systèmes d'informations tombant sous la responsabilité de l'organisation pour laquelle ils travaillent. Cela peut également concerner des informations provenant de sources externes dont l'organisation dispose ou auxquelles l'organisation a directement accès. Le fait de rendre les informations accessibles en dehors de l'organisation physique gérable donne lieu à des risques au niveau de la sécurité et de la protection de la vie privée. L'organisation peut réduire ces risques en prenant les mesures utiles. Ces directives ont pour but d'indiquer que l'organisation demeure responsable pour les informations.

2. Télétravail sécurisé

Toute organisation souscrit la politique suivante relative à la sécurité de l'information et à la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation:

1. Toute organisation doit prendre les mesures adéquates, en fonction du moyen d'accès[1], afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de l'organisation aux données sensibles, confidentielles et professionnelles de l'organisation.
2. Des instructions claires et précises contenant des règles de bonne conduite ainsi qu'une mise en œuvre appropriée du télétravail sont mises au point, validées, communiquées et tenues à jour. Ces instructions doivent aussi préciser quels systèmes peuvent et quels systèmes ne peuvent pas être consultés au départ du lieu de travail à domicile ou d'autres appareils.
3. Les dispositifs de télétravail de l'organisation sont organisés de la sorte que sur le lieu du télétravail (à domicile, dans un bureau satellite ou à un autre endroit) aucune information relative à l'organisation ne soit enregistrée sur des appareils externes sans chiffrement et qu'aucune menace potentielle ne puisse atteindre l'infrastructure informatique de l'organisation au départ du lieu de télétravail.

1 Moyen d'accès: p.ex. Internet, ligne louée, réseau privé, réseau sans fil.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
2003		V2003	Première version	10/09/2003	1/10/2003
2004		V2004	Deuxième version	11/02/2004	1/12/2004
2017		V2017	Intégration UE GDPR	07/03/2017	7/03/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 p.
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 p.
- NIST, "Guide to enterprise telework, remote access, and BYOD security", juli 2016, 53 blz.

Ci-dessous figurent les références aux sites web qui ont servi de source d'inspiration pour le présent document:

- https://www.iso.org/fr/isoiec-27001-information-security.html
- https://www.iso.org/fr/standard/54534.html
- https://www.iso.org/fr/standard/54533.html
- http://www.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
- http://www.ccb.belgium.be/fr/work
- http://www.cnt-nar.be/CAO-COORD/cao-081.pdf
- https://www.safeonweb.be/fr
- https://www.safeinternetbanking.be/fr
- https://www.cybersimpel.be/fr

Annexe C: Télétravail menaces et mesures

Les menaces et mesures en cas de télétravail peuvent être réparties en fonction des éléments de la chaîne de télétravail entre le collaborateur et l'infrastructure TIC de l'organisation:

1. Localisation du télétravail

Le télétravail a lieu à un endroit en dehors de l'organisation. La principale menace est l'interception et la manipulation d'informations (professionnelles, confidentielles ou sensibles). Cet environnement tombe en dehors de la sphère d'influence de l'organisation. C'est pourquoi un ensemble de mesures organisationnelles, procédurales et techniques s'impose pour la protection du lieu de télétravail. L'organisation est compétente pour la fixation des exigences requises en cas de télétravail à un endroit fixe, par exemple au domicile du collaborateur ou dans un bureau satellite. Si un collaborateur fait du télétravail dans un endroit public, le risque existe qu'une personne externe lise des informations sur l'écran ou écoute une conversation. Par ailleurs, l'appareil de télétravail du télétravailleur peut se perdre. Suite à la perte ou au vol de l'appareil de télétravail, les informations enregistrées sur cet appareil sont susceptibles de tomber dans les mains d'un étranger.

Si le télétravailleur utilise un ordinateur d'une autre institution ou personne, par exemple dans une bibliothèque, à domicile, dans le hall d'un aéroport, ou d'un ami ou voisin, le risque existe que l'utilisateur suivant de l'appareil puisse voir (consulter) les informations enregistrées dans la mémoire tampon.

Ci-après figure un aperçu des principaux risques relatifs à la localisation du télétravail et des mesures que l'organisation peut prendre pour réduire le risque.

Risque: Des personnes étrangères sont en mesure de lire les informations à l'écran
Mesures:

- Attention spécifique dans des campagnes de sensibilisation.
- Définir, valider, communiquer et tenir à jour les conditions relatives au télétravail, notamment:
  a. Les endroits autorisés pour le télétravail. L'organisation peut interdire le télétravail dans un café Internet ou par le biais d'une connexion sans fil non sécurisée.
  b. Politique du « clear screen » (écran vide)
- Le dispositif de protection de l'écran (screensaver) permet de rendre les informations à l'écran inaccessibles après maximum 15 minutes d'inactivité.
- L'organisation peut ajouter un filtre de protection de la vie privée qui permet d'éviter des regards indiscrets sur l'écran de l'appareil destiné au télétravail. En effet, le collaborateur doit être installé directement face à l'écran lors du télétravail.

Risque: Des personnes étrangères sont en mesure d'intercepter des informations en écoutant les conversations.
Mesures:

- Attention spécifique dans des campagnes de sensibilisation.
- Définir, valider, communiquer et tenir à jour les conditions relatives au télétravail, comprenant notamment l'obligation de limiter les échanges d'informations par téléphone dans des endroits publics.

Risque: Des informations entrent dans les mains d'une personne étrangère suite à la perte ou au vol de supports de données
Mesures:

- Attention spécifique dans des campagnes de sensibilisation.
- Définir, valider, communiquer et tenir à jour les conditions relatives au télétravail comprenant notamment l'obligation de signaler immédiatement la perte ou le vol de supports de données mobiles contenant des informations professionnelles, confidentielles ou sensibles au conseiller en sécurité de l'information (CISO) et/ou au délégué à la protection des données (DPO).
- La politique du bureau vide pour les supports d'informations sur papier et amovibles:
  a. Le collaborateur ne peut pas faire traîner des informations sensibles sur le bureau. Ces informations doivent toujours être conservées dans un endroit qui peut être fermé à clé (armoire, tiroir, bureau ou pièce).

b. Il est déconseillé d'imprimer des informations dans des environnements externes. Toutefois, si cela n'est pas possible autrement, le télétravailleur doit évaluer les risques.

2. L'appareil réservé au télétravail tel un ordinateur fixe, une tablette ou un smartphone

Les appareils réservés au télétravail peuvent être la propriété du télétravailleur ou de l'organisation ou d'une personne étrangère. Si le télétravailleur dispose d'un appareil réservé au télétravail qui est mis à la disposition par l'organisation, cette dernière peut définir, de manière autonome, quelles sont les mesures de sécurité qui sont applicables. Elle peut ainsi couvrir en grande partie les risques. Pour un appareil privé, ceci est différent vu que celui-ci n'est pas géré par l'organisation. Toutefois, l'organisation est compétente pour imposer des paramètres de sécurité lorsque des appareils privés sont utilisés à des fins professionnelles ('bring your own device' ou BYOD). Il s'agit dans ce cas notamment des paramètres relatifs au mot de passe/à la phrase de passe, au chiffrement, à la présence de logiciels antimalware. Sur demande de l'organisation, les collaborateurs doivent autoriser l'installation de logiciels (via 'mobile device management software').

Les éventuels problèmes sont les suivants:

- L'absence ou le manque de directives concernant les données pouvant être enregistrées sur l'appareil de télétravail (aucune connaissance des règles de classification des données)
- Logiciels malveillants/logiciels d'extorsion sur l'appareil réservé au télétravail
- Cliquer sur des liens dans des e-mails ou sur des pages web auxquels vous ne faites pas confiance
- Connexion par le biais de réseaux ouverts non protégés où des attaques par des tiers sont possibles
- "Man in the middle" attack[2]
- Non-verrouillage de l'appareil réservé au télétravail
- Pas de chiffrement, alors que celui-ci est nécessaire
- Vol de l'appareil réservé au télétravail
- « Rooter » ou « jailbreaker » l'appareil réservé au télétravail[3]
- Perte de l'appareil réservé au télétravail
- Des informations professionnelles, confidentielles ou sensibles, sont enregistrées sur des supports de données mobiles (dans un format non chiffré)
- L'accès non autorisé à l'appareil réservé au télétravail ou des disfonctionnements techniques
- Le télétravailleur dispose de tous les droits sur son appareil privé et peut installer des logiciels sur cet appareil
- Des installations de mise à jour de l'appareil réservé au télétravail non autorisées, tardives, inexactes ou incomplètes
- Installation de logiciels malveillants qui permettent de voler des données, de se conférer un accès, mais qui se propagent aussi parmi d'autres systèmes de l'organisation.
- Des personnes étrangères lisent, copient, modifient et/ou détruisent des données.
- L'appareil réservé au télétravail doit être remplacé par un nouvel appareil réservé au télétravail.
- Un accès illimité aux systèmes de l'organisation au moyen de l'appareil réservé au télétravail.

Ci-après figurent un aperçu des principaux risques et des mesures relatives à l'appareil réservé au télétravail et des mesures que l'organisation peut prendre pour réduire les risques.

Risque: Des informations tombent dans les mains d'une personne étrangère (manipulation de données ou prise de connaissance non autorisée).
Mesures:

- Attention spécifique dans des campagnes de sensibilisation.
- Tous les appareils, tant ceux de l'organisation que les appareils privés, contenant des données de l'organisation sont gérés au moyen d'un outil MDM, de sorte que la politique de sécurité sur l'appareil réservé au télétravail puisse, d'un point de vue technique, être rendue obligatoire:
    - logiciel sur l'appareil réservé au télétravail, en ce compris logiciel de sécurité tel que:

[2] https://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu

[3] Le « jailbreak » consiste à installer et faire fonctionner des applis non approuvées sur des appareils mobiles et donc aussi des logiciels malveillants. Le « rootage » est le processus permettant d'obtenir davantage de droits sur l'appareil, ce qui permet la suppression totale et le remplacement du système d'exploitation. Des logiciels malveillants peuvent ainsi être introduits et des paramètres de sécurité détournés.

i. logiciel de scannage contre les virus à jour
ii. pare-feu personnel à jour
iii. outil de suppression des logiciels malveillants à jour
iv. systèmes d'exploitation et applications à jour (voir à cet effet gestion des patchs)
- droits du télétravailleur sur l'appareil réservé au télétravail
- le télétravailleur doit s'annoncer avec un nom d'utilisateur et un mot/une phrase de passe, éventuellement soutenu par un certificat

- Définir, valider, communiquer et tenir à jour les conditions relatives au télétravail comprenant notamment:
  - l'interdiction d'enregistrer des informations professionnelles, confidentielles ou sensibles, sur des supports d'information mobiles, sauf si ces données sont chiffrées.
  - l'interdiction d'installer des applications sans l'autorisation de l'organisation.
  - l'interdiction de stocker des informations en local sur l'appareil privé afin de réduire le risque de lecture des informations par des logiciels espions.
- Désactivation de services non utiles (« hardening » (durcissement) de l'appareil réservé au télétravail)[4]
- L'appareil réservé au télétravail n'enregistre pas d'informations relatives à l'organisation. Une alternative pour éviter un enregistrement décentralisé des données est la « virtual desktop infrastructure ». La gestion centrale permet d'accorder, moyennant des efforts de gestion relativement limités, au collaborateur, à tout moment, à partir de n'importe quel endroit et après connexion avec un quelconque appareil réservé au télétravail, un accès sécurisé, souple et contrôlé à l'emplacement de travail personnel.

Risque: L'appareil réservé au télétravail risque d'être infecté par un logiciel malveillant/logiciel d'extorsion et d'ainsi infecter l'organisation. L'appareil réservé au télétravail est utilisé par les pirates comme un instrument d'attaque.
Mesures:

- Attention spécifique dans des campagnes de sensibilisation.
- Définir, valider, communiquer et tenir à jour les conditions relatives au télétravail comprenant notamment:
  - l'interdiction d'utiliser des réseaux inconnus
  - l'interdiction de cliquer sur des liens inconnus dans des e-mails et sur des pages web
- En cas de problèmes de sécurité, l'appareil réservé est placé dans un réseau en quarantaine[5]. Le télétravailleur a ainsi uniquement accès à un nombre limité de sites web, à savoir ceux des logiciels de scannage contre les virus, des pare-feu, etc.
- Désactivation de services non utiles (« hardening » (durcissement) de l'appareil réservé au télétravail)

3. La connexion entre l'appareil réservé au télétravail et l'infrastructure informatique de l'organisation

La principale menace pour le dispositif réseau est la consultation, le copiage, la suppression et la modification des données par des tiers. La connexion réseau entre l'appareil réservé au télétravail et l'infrastructure TIC de l'organisation peut avoir lieu de différentes manières. Ces connexions réseau peuvent être écoutées par des pirates qui sont ainsi en mesure de prendre connaissance des informations échangées entre le télétravailleur et l'organisation. Les pirates peuvent ainsi s'emparer du nom d'utilisateur et/ou du mot/de la phrase de passe. Un pirate sait ainsi accéder aux informations pour lesquelles l'organisation est responsable. Cela peut aussi concerner des informations de citoyens ou de tierces parties dont l'organisation n'est pas le propriétaire.

Le principal risque pour la connexion entre l'appareil réservé au télétravail et l'infrastructure TIC de l'organisation est le fait que des informations risquent de passer dans les mains de parties externes (manipulation de données ou consultation par des personnes étrangères).

[4] Par « hardening », on entend la désactivation et/ou la suppression de fonctions superflues dans les systèmes d'exploitation. Attribuer de telles valeurs aux paramètres de sécurité de sorte à réduire les possibilités de compromission d'un système et à garantir une sécurité maximale. Il s'agit à cet égard aussi de la suppression de comptes utilisateurs superflus ou non utilisés et de la modification de mots de passe standard qui sont susceptibles d'être présents sur certains systèmes.

[5] Cette solution offre une protection contre la modification non intentionnelle des paramètres de configuration de l'appareil et le non-rétablissement de ceux-ci avant qu'une connexion n'ait lieu avec l'infrastructure TIC de l'organisation. Un télétravailleur peut par exemple désactiver un logiciel anti-virus, alors que ce logiciel constitue une condition obligatoire pour une connexion avec le réseau. Les configurations de l'ordinateur peuvent être contrôlées et si nécessaire corrigées avant qu'un accès au réseau ne puisse être accordé. Lorsque la configuration de l'appareil correspond à la politique du réseau de l'organisation, les restrictions relatives à la quarantaine sont levées.

Mesures:

- Attention spécifique dans des campagnes de sensibilisation.
- Définir, valider, communiquer et tenir à jour les conditions relatives au télétravail comprenant notamment l'interdiction d'utiliser des réseaux inconnus.
- Tous les appareils, tant ceux de l'organisation que les appareils privés, utilisés pour établir une connexion avec l'infrastructure TIC de l'organisation sont gérés au moyen d'un outil MDM, de sorte que la politique de sécurité sur l'appareil réservé au télétravail puisse, d'un point de vue technique, être rendue obligatoire.
- L'appareil destiné au télétravail qui souhaite établir une connexion avec l'infrastructure TIC de l'organisation est contrôlé quant à la présence d'un logiciel de scannage et d'un pare-feu à jour. Si l'appareil de télétravail n'est pas (suffisamment) protégé (par exemple, les définitions des virus ne sont pas à jour), l'accès à l'infrastructure TIC de l'organisation peut être refusée.

4. Le traitement ou l'enregistrement des données sur l'appareil réservé au télétravail a lieu dans un endroit externe.

Les données sont ainsi exposées à des risques inhérents au lieu de travail et à des vulnérabilités éventuelles sur l'appareil réservé au télétravail.

Les problèmes éventuels sont les suivants:

- La fiabilité des données dans l'environnement serveur est menacée par un accès non autorisé et des attaques par déni de service « Denial of Service » (disponibilité). L'impact de ces menaces peut être important car il concerne de nombreux télétravailleurs.
- Accès non autorisé à l'environnement serveur causé par le piratage ou par un appareil réservé au télétravail non suffisamment sécurisé.
- Les télétravailleurs sont négligents en ce qui concerne leurs moyens d'identification et d'authentification ou laissent des tiers utiliser leur appareil de télétravail.

Le risque majeur du traitement ou de l'enregistrement de données sur l'appareil réservé au télétravail dans un endroit externe est l'accès non autorisé à l'environnement serveur, tant aux systèmes qu'aux informations.

Mesures:

- Attention spécifique dans des campagnes de sensibilisation.
- Définir, valider, communiquer et tenir à jour les conditions relatives au télétravail comprenant notamment:
  - l'interdiction d'utiliser des réseaux inconnus
  - l'interdiction de cliquer sur des liens inconnus dans des e-mails et sur des pages web
- Protéger l'accès aux systèmes de l'organisation par une authentification à deux facteurs (le seul appareil de télétravail ne permet pas d'obtenir un accès).
- Avoir recours au Role Based Access Control (RBAC)[6].
  - Après authentification, l'accès est accordé à certaines applications et informations pour les collaborateurs en télétravail. Il est possible de limiter les autorisations d'un collaborateur en télétravail. Le nombre d'autorisations d'un télétravailleur peut être mis en rapport avec le niveau de sécurité de l'appareil réservé au télétravail.
  - Attention spécifique pour une suppression complète et en temps utile des autorisations en cas de sortie de service ou de modification de fonctions des télétravailleurs.
- Segmentation/compartimentage du réseau avec une « bonne » configuration du pare-feu et mise en place d'une zone démilitarisée (DMZ) permettent de limiter l'accès de l'utilisateur.
- Attention spécifique à la prise de traces et à la surveillance de l'accès à l'environnement serveur. Ce contrôle doit permettre de constater des abus, une bonne gestion et un bon fonctionnement conformément aux exigences définies. Informations minimales à conserver:
  - Quels appareils établissent une connexion réseau (VPN) et quelles tentatives échouent?
  - Quels droits d'accès sont utilisés/abusés pour l'accès au réseau de l'organisation (tentatives de connexion échouées, dépassement des compétences d'autorisation, tentatives d'accès refusées)?

[6] https://fr.wikipedia.org/wiki/Contrôle_d'accès_à_base_de_rôles

- Quels échanges réseau ont lieu entre l'appareil réservé au télétravail et le réseau interne?

5. Accès aux informations

Pour l'accès du télétravailleur aux informations du réseau de l'organisation, une authentification multifacteur s'avère indispensable. L'authentification multifacteur implique que l'utilisateur doit pouvoir prouver qu'il/elle est effectivement celui/celle qu'il/elle prétend être par:

1. Ce que l'utilisateur sait (par exemple: phrase de passe / code PIN)
2. Ce que l'utilisateur possède (par exemple: token, certificat ou via authentification par SMS)
3. Qui l'utilisateur est (par exemple: caractéristique biométrique)

Sur la base de deux (authentification à deux facteurs) ou plusieurs facteurs, il peut être prouvé que l'utilisateur est effectivement celui qu'il prétend être.

6. Le télétravailleur même

Le télétravailleur n'est pas (suffisamment) conscient des risques éventuels inhérents au télétravail:

- L'appareil réservé au télétravail est laissé sans surveillance dans une pièce accessible à des tiers.
- Le télétravailleur ne se rend pas compte qu'une attaque de type « social engineering »[7] est en cours.
- Les ordinateurs privés à domicile ne sont pas bien gérés et sont infectés par des logiciels malveillants/des logiciels d'extorsion.

Le collaborateur doit être informé des risques liés au télétravail par des campagnes de sensibilisation. Par ailleurs, il y a lieu de préciser les droits et obligations du collaborateur et les conséquences éventuelles en cas de manquement aux obligations.

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	**Oui**
Sécurité des ressources humaines	
Gestion des actifs	
Toegangsbeveiliging	**Oui**
Cryptographie	
Sécurité physique et environnementale	**Oui**
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****

[7] Dans le cas du social engineering, les pirates abusent de la crédibilité et de la bonne intention des collaborateurs pour atteindre le but. Le collaborateur concerné n'est généralement pas conscient du fait qu'il s'agit d'une attaque malveillante. Il est normal de s'adresser à un inconnu dans le couloir et de lui demander s'il a besoin de l'aide. Toutefois, de nombreuses personnes éprouvent des difficultés à ce niveau. Par conséquent, on s'adresse (trop) peu à des inconnus. Il est toujours bon de se demander qui on a en ligne et pourquoi on reçoit cette question.