Retranscription à l'identique de la copie remise par la/le candidat·e

MEILLEURE COPIE

Concours interne de **TECHNICIEN·NE TERRITORIAL·E**

Session 2020

Spécialité *Ingénierie, informatique et systèmes d'information*

RAPPORT TECHNIQUE

Commune de Techniville
Direction des Systèmes
d'Information

Le 15 avril 2021

Rapport Technique à l'attention
du Directeur des Systèmes d'information

Objet : Le télétravail et la sécurité informatique

Références : Décret du 11/02/2016 sur le télétravail dans la fonction publique, l'ordonnance du 22/09/2017 sur les conditions de recour au télétravail, le règlement sur le RGPD du 25 mai 2018.

Les entreprises utilisent de plus en plus le télétravail, même si celui-ci a de nombreux avantages, il pose néanmoins le problème de la sécurisation des données accessibles à distance.

Comment avoir recour à ce mode de travail tout en préservant cette sécurité.

Dans une première partie nous étudierons le télétravail et la protection des données, puis dans une deuxième partie la mise en œuvre de la sécurité d'un point de vue technique mais aussi humains.

I) Le télétravail et la protection des données

Depuis 2017, un quart des salariés français se sont mis au télétravail et ce mode de travail ne fait qu'augmenter. En 2018 le RGPD venait réglementer la sécurisation des données et sécuriser celles-ci.

A) Le télétravail

Le télétravail, déjà utilisé par les entreprises depuis plusieurs années, est apparu dans les collectivités depuis le décret du 11/02/2016 et faisant suite à la loi sur la modernisation de la fonction publique de 2012.

Ce mode de travail se définie par l'exercice de son métier, au domicile de l'agent ou à défaut sur un lieu déporté mis à disposition.

L’agent doit être en conformité avec non seulement les conditions du télétravail à son domicile mais aussi sur son métier lui-même. En effet tous les métiers ne sont pas compatibles avec le télétravail.

De plus chaque ministère établie ses règles de conditions de télétravail, avec l’utilisation ou non de matériel personnels par exemple.

L’agent, qu’il soit en télétravail ou sur son lieu de travail est soumis aux mêmes règles et particulièrement à la protection des données professionnelles.

B) Le RGPD

Le règlement général sur la protection des données (RGPD), incite les entreprises à davantage de protection car elles risques de lourdes amendes en cas de manquements.

Le RGPD formalise des mesures spécifiques pour un accès sécurisé aux données professionnelles. L’obligation d’avoir recour à des mot de passe complexes, l’utilisation d’antivirus ou d’antimalwares, la mise en place de pare-feu ou du cryptage des données ne sont que quelques exemples.

Comme la CNIL qui préconise d’édicter des règles de bonne conduite, le RGPD impose la formalisation de processus internes, et de bonnes pratiques qui peuvent conduire à des sanctions si celles-ci ne sont pas respectées.

Bien-sûr ces mesures ne peuvent être appliquées que si une politique de sécurité est mis en place.

Ⅱ) La sécurité informatique et celle des agents

La mise en place du télétravail oblige la DSI à renforcer la sécurisation de ses données.

A) Sécurité informatique

Le télétravail, s’il est mis en place, pose le problème de sécurisation des données utilisées à l’extérieur du lieu de travail habituel.
D’un point de vue technique il faut maîtriser l’utilisation des terminaux mobiles par la mise en place d’un réseau privé virtuel (VPN), c'est à dire l’accès au réseau local d’une entreprise à distance via une connexion internet sécurisée.

L’utilisation d’un webmail et d’outils collaboratif comme l’agenda ou la gestion électronique de documents doit être privilégié à distance et accessible avec une simple connexion internet.

Le mode SAAS, c'est à dire l’utilisation des logiciels en mode hébergé ainsi que le recour au cloud pour l’hébergement des données est à privilégier.

L’agence nationale pour la sécurisation des systèmes d’information (L’ANSSI) met en lumière les risques de fuites ou de pertes de données lors de l’utilisation de périphériques

nomades surtout s'ils sont utilisés dans un lieu public (hôtel, transport en commun, espace de co-working).

Avec l'utilisation de ces terminaux mobiles en télétravail ou en utilisation nomade, les risques de vol ou de perte de données sont plus importants.

C'est pourquoi il est déconseillé d'utilisé des terminaux personnel (le BYOD).
La DSI aura plus de difficultés à contrôler ces terminaux, à les mettres à jour pour les sécuriser.
Il existe néanmoins des solutions de MDM pour pouvoir sécurisé et suivre l'utilisation de terminaux mobiles personnel (smartphone, tablettes, portables).

Le but étant pour la DSI d'avoir la même sécurité en interne qu'en externe.
Les mesures de télétravail doivent donc être définies par la DSI dans son plan sécurité SI (PSSI).

Le télétravail ne peut pas concerner tout le monde, de part leur métier ou l'utilisation de données trop sensible.

B) La formation des agents

Toutes ces mesures techniques ne doivent pas occulter que la collectivité est responsable de ces données.
Elle doit veiller à ce que chaque agent concerné par le télétravail est bien conscience des risques liés aux pertes de données.
Comme le prévoit le RGPE, l'agent manipulant des données, surtout à l'extérieur du lieu de travail doit avoir été sensibilisé et formé à l'utilisation de ces données.
Les accès à celle-ci doivent être protégés (contrôle d'accès, authentification de l'utilisateur).
C'est pourquoi l'agent doit faire partie d'une liste d'utilisateur autorisé au nomadisme.
La DSI doit, en outre avoir une gestion des utilisateurs lors d'un changement d'affectation ou de départ (suppression du compte…).

La charte informatique doit contenir ce mode de travail pour sensibiliser les agents aux risques liée au télétravail.

La mise en place du télétravail est technique mais aussi humain de part les risques que ce mode de travail entraîne.

Le télétravail se met en place pour de plus en plus d'employés, de part le fait de l'utilisation de plus en plus de terminaux mobiles.
Dès lors que ce mode de travail se démocratise, il faut cependant bien veiller à la perte de donnée dont l'utilisateur pourrais se rende coupable afin de préserver la collectivité de ce risque majeur à l'heure du tout numérique.