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 — Le 15 avril 2021

RAPPORT TECHNIQUE
à l'attention de Monsieur le Directeur des systèmes d'information

Objet : Le télétravail et la sécurité informatique

Réfs : Loi n°2012-347 du 12 mars 2012
Décret n°2016-151 du 11 février 2016

En France, un quart des français ont recours au télétravail. En mars 2018, 4,65% des agents de l'Administration Territoriale de l'État pratiquaient le télétravail et 3,5% des agents concernaient l'Administration centrale. Le télétravail est organisé au domicile de l'agent ou dans des locaux professionnels distinct de la collectivité et du lieu d'affectation. Pour les salariés les avantages du télétravail sont un mieux être par le fait qu'ils sont moins dans les transports, moins stressés et le management est plus flexible. Toutefois, très peu d'entreprise propose de réel système de travail à distance qu'il soit à domicile ou nomade. En effet, il n'est pas toujours simple de savoir quels outils utiliser et comment l'encadrer.

Face au recours au télétravail pour les collectivités territoriales, comment garantir la sécurité informatique de celles-ci ?

Le présent rapport expliquera comment s'organise le télétravail dans une collectivité (Ⅰ) tout en évitant de compromettre la sécurité de son système d'information (Ⅱ).

Ⅰ) Comment s'organise le télétravail au sein d'une collectivité

A) La règlementation

La loi n°2012-347 du 12 mars 2012 et le décret n°2016-151 du 11 février 2016 encadrent la possibilité pour les agents civils et magistrats d'exercer leurs fonctions en télétravail.
L'Article 2 du décret précise que le télétravail est organisé au domicile de l'agent ou dans des locaux professionnels distinct de ceux de la collectivité et du lieu d'affectation.
Pour organiser le télétravail, la collectivité doit équiper les agents d'ordinateur portable, d'un téléphone ou d'une tablette et se rapprocher de la direction des systèmes d'information. Du côté des agents, ceux-ci doivent répondre à certaines exigences tel qu'apporté un certificat de conformité de son installation électrique du poste de travail ou une attestation sur

l'honneur. Ils doivent avoir une connexion internet haut-débit, apporter une attestation de conformité des risques incendies ou électrique.
L'agent doit pouvoir revenir en cas de nécessité de service. La collectivité peut demander à l'agent d'envoyer une photo du poste de travail.
Enfin, l'administration prend en charge les coûts du télétravail (logiciels, matériels informatiques, maintenance). Aussi, depuis l'ordonnance dite « Macron » du 22 septembre 2017 les conditions de recours au télétravail ont été assouplies.

B) Les outils du télétravailleur

Pour que l'agent puisse bénéficier de bonnes conditions de travail celui-ci peut avoir accès à plusieurs outils. Il peut être privilégier un accès au réseau local de la collectivité de son domicile : le VPN Virtual Private Network, le réseau privé virtuel. Il peut avec accès au serveur de messagerie à distance (webmail). La collectivité peut développer une messagerie instantannée favorisant les échanges entre les agents. C'est rapide et immédiat. Le service informatique peut développer des outils de communication asynchrones tels que des forums, wifis, blog toujours pour favoriser les échanges. Autre outil existant, le softphone c'est à dire les logiciels de téléphonie, les appels sont gérés depuis l'ordinateur. Les agents peuvent avoir recours au travail collaboratif pour accéder au projet directement en équipe (workflow, agenda partagé, gestion électronique de document).
Ensuite, pour que l'agent puisse accéder au logiciel de chez lui, la collectivité peut migrer les logiciels en mode SaaS. Enfin, pour se retrouver visuellement les agents peuvent organiser des réunions virtuelles via la webconférence.
Ces outils offriront aux agents une meilleure qualité de travail, toutefois, il faut qu'ils bénéficient d'une bonnes connexion à internet.

Le recours au télétravail à de nombreux côtés positifs cependant la collectivité est responsable de la sécurité des données personnelles.

Ⅱ) Comment garantir la sécurité informatique?

A) Identifier les risques pour les réduire

70% des entrepreprises ont enregistré des incidents de sécurité ayant eu des répercutions sur leurs activité (Journal du net, mai 2018).
Le télétravail nomade a lieu dans des lieux où les risques ne peuvent être maîtrisés : un hôtel, dans les transports en communs, salles d'attente, espace de working. Ici les risques sont la perte, ou le vol du matériel, des informations vues sur le matériel volé, un accès illégitime au système d'information et la perte de confidentialité.
Les risques du télétravail sont la fuite des données confidentielles.
La collectivité doit redéfinir les objectifs de sécurité à atteindre.
D'une part définir les métiers éligibles au nomadisme et au télétravail, tenir une liste à jour des utilisateurs, surveiller leur statut et d'autre part catégoriser les utilisateurs nomades en fonction des risques exposés. Enfin, elle doit définir des procédures pour les arrivés, mutation, départs.
Les directeurs des systèmes d'information doivent avoir une visibilité complète des activité de réseau afin de déterminer ce qui est normal ou non.
Enfin, autres risques à gérer le BYOD, c'est le Bring Your Own Device, c'est le fait d'utiliser son équipement personnel pour un usage professionnel.

B) Les outils à développer pour limiter les risques

Tout d'abord, une des recommandations da la CNIL est de sensibiliser les agents et d'édicter les bonnes conduites de la charte informatique.
Il faut assurer un réseau de sécurité et respecter le RGPD (Règlement général de la protection des données). Lui aussi impose de sensibiliser les salariés. Il faut sécurisé les postes informatiques, interdire l'installation manuelle d'application, filtrer la navigation.
Il existe des solution en mode Cloud, le Cloud public est un endroit où sont stockés les fichiers et sont partagés entre plusieurs agents.
Le Cloud présente les meilleurs garanties pour un réseau ouvert et accessible. Il propose des performances intéressantes en matière de sécurité de la data.
L'idéal est d'associer le Cloud à d'autres applications mobiles natives, de postes de travail virtualisé et d'application en mode service.
L'agent bénéficiera d'un accès unique à toutes les l'application de n'imorte quel appareil.
La collectivité peut avoir recours à la prévention de la perte de données (DPL) c'est-à-dire surveiller les activités des terminaux, filtrer les flux des données et surveiller le Cloud pour protéger les données au repos. Enfin des sessions de formations régulières peuvent aider les agent à comprendre les risques et les conséquences.

Pour conclure, le télétravail tend à se généraliser, les administrations ne sont pas en mesures d'empêcher leurs agents de perdre leurs matériels mais elles sont capables de définir des politiques de sécurité.