

SPÉCIALITÉ « INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION »

ÉPREUVE DE RAPPORT TECHNIQUE

NOTE OBTENUE : 15.25 / 20

Direction des Systèmes d'information de la commune de Technville

Rapport à l'attention de Monsieur le Directeur des Systèmes d'Information : le télétravail et la sécurité informatique

En 2017, un quart des salariés déclaraient télétravailler un ou plusieurs jours par mois. Ce chiffre semble aujourd'hui dérisoire face aux profondes adaptations auxquelles nous avons dû faire face depuis 2020, avec les mesures d'urgence mises en place pour lutter contre l'épidémie de la Covid19.

Le télétravail fait désormais partie du quotidien d'une grande partie des salariés. Les collectivités ont dû rapidement mettre en place des mesures. Pourtant la mise en place du télétravail doit être pensée et réfléchie afin d'éviter les risques qui en découlent notamment ceux relevant de la sécurité informatique.

Même s'il a parfois été mise en place dans l'urgence, on peut se demander quelles seraient les bonnes pratiques et les mesures les plus adéquates pour assurer la sécurité du système informatique de la collectivité.

Aussi, dans un premier temps nous allons étudier comment on peut définir des besoins et un cadre pour la mise en place du télétravail. Dans un second temps, nous verrons par quels moyens techniques, le télétravail peut être compatible avec la sécurité et l'intégrité du système d'information de la collectivité.

I. Mise en place du télétravail : définir des besoins et un cadre

Certaines études montrent que le télétravail est un facteur d'augmentation de la productivité des salariés. En effet, moins de temps dans les transports et donc moins de stress et plus de temps pour soi contribue au bien être des salariés et donc à une meilleure efficacité. Cependant, tous les postes ne sont pas forcément transposables en télétravail de par notamment des contraintes techniques.

a. Établissement d'un cadre réglementaire et technique

En amont il est primordial d'effectuer un inventaire des différents postes de la collectivité et d'identifier les missions qui sont télétravaillables. En effet, certaines missions nécessitent un travail dans les locaux et ont un niveau de sensibilité des données ou de l'activité trop élevé. De même il est possible qu'il existe des contraintes réglementaires. Enfin, il peut aussi exister des restrictions liées au métier en lui-même qui nécessite des matériels spécifiques (logiciels lourds par exemple). Une fois cet inventaire effectué, les agents pourront ainsi être soit en mesure de télétravailler, leurs missions étant compatibles, soit partiellement, soit entièrement. Certaines missions s'avèreront totalement non compatibles avec le télétravail.

En ce qui concerne le cadre technique, il faudra avoir à l'esprit l'architecture globale du process télétravail.

Il se compose de 5 entités :

- Le SI interne
- Une passerelle d'interconnexion
- Un canal d'interconnexion
- Un équipement d'accès
- Le télétravailleur

Chacune de ces entités devra mettre en place des mécanismes de protection. Celui qui est en bout de chaîne devra bénéficier d'une information suffisante.

b. Information et sensibilisation des agents

L'erreur humaine est le premier risque auquel est confronté le système d'information. Afin de limiter ce risque, il convient donc en premier lieu de sensibiliser les agents aux différents risques encourus avec le télétravail, par la collectivité. Les agents doivent connaître les risques et les comportements à adopter. La charte d'usages informatiques de la collectivité doit intégrer ces règles liées au télétravail.

Les agents devront suivre des sensibilisations et des formations à la sécurité numérique. Ils seront dès lors à même de connaître les comportements à risque et les comportements à adopter.

Un rappel du Règlement Général sur la Protection des Données (RGPD) est aussi nécessaire. Les données de la collectivité ne sont pas la propriété de l'agent. Aussi celles-ci doivent être manipulées et stockées de façon sécurisée.

Après avoir effectué une évaluation des besoins pour chaque poste, puis une sensibilisation des agents, la mise en place technique du télétravail s'appuie sur des éléments techniques afin d'assurer la sécurité du système d'information.

II. Un déploiement technique du télétravail compatible avec la sécurité informatique de la collectivité

a. Des solutions techniques à la portée de toutes les structures

La première brique du système passe par la mise en place d'un VPN (Réseau Privé Virtuel) qui permet d'accéder au réseau local de l'entreprise à distance. Cette solution permet l'accès au poste informatique de l'agent à distance.

La communication entre agents et hiérarchie est primordiale afin de conserver le lien et des équipes efficaces. La mise en place d'outils de communication est donc primordiale. Le Webmail permet de conserver l'accès à la messagerie d'entreprise. Mais les messageries instantanées permettent moins de formalisme. De même, les forums, blogs, espaces collaboratifs qui permettent une communication synchrone sont utiles. Enfin les outils pour les réunions virtuelles et web conférences permettent de se retrouver et partager en temps réel.

Au-delà de ces outils à mettre à disposition de l'agent, le travail en cloud offre des performances intéressantes en terme de sécurisation. On privilégiera les clouds européens pour éviter la fuite des données vers des pays n'ayant pas de législation stricte.

On peut également se tourner vers l'intelligence artificielle pour surveiller les événements inhabituels.

Du côté de l'utilisateur, on devra veiller à la conformité de son installation électrique. Il devra avoir une couverture contre les risques (assurance) et une connexion internet haut débit. Enfin l'ergonomie du poste de travail à la maison est aussi un élément essentiel.

Le matériel informatique est également un point important. En effet, la maîtrise de l'ensemble des équipements est fortement conseillée. L'utilisation de matériel personnel est donc à proscrire car il est impossible de garantir le niveau de sécurité de l'équipement personnel. La gestion du cycle de vie des applications est également difficile. Enfin, l'interrogation en cas d'incidents est trop complexe.

L'équipement moyen s'élève à environ 1000€ par agent sans compter l'abonnement internet.

b. La sécurité : pierre angulaire du télétravail

Le domicile peut être considéré comme un lieu non maîtrisé.

Les risques peuvent être liés au vol ou perte de matériel, l'accès illégitime au système d'information par des tiers, la perte de confidentialité et d'intégrité.

La gestion des utilisateurs est donc primordiale. Le premier inventaire est à mettre à jour en continu afin de connaître les arrivées, les mutations et les changements de missions, afin d'ajuster les droits d'accès spécifiques.

Le matériel doit être affecté spécifiquement et suivi.

Le télétravail s'est parfois mis en place en marche forcée du fait de la pandémie. Cependant, on devra veiller à ce qui a été mis en place parfois rapidement est en accord avec les règles de sécurité informatique. La sensibilisation des agents n'est pas à négliger. En effet, l'erreur humaine est la principale cause de faille dans les systèmes.

Il est toujours possible d'ajuster ce qui a été mis en place. C'est l'essence même d'un système informatique fiable et sûr : le suivi du matériel mis à disposition des agents d'une part, et l'ajustement en fonction de l'évolution du poste et des missions d'autre part.

Un retour en arrière est peu probable dans les années à venir. Il est donc primordial pour la collectivité d'anticiper cette évolution majeure du mode de travail. C'est aussi pour les collectivités un moyen de se réinventer notamment dans leur former et leur organisation avec peut-être moins d'immobilier mais plus de réactivité.